DERECHO DE PROTECCIÓN DE DATOS PERSONALES Y ANÁLISIS DEL RIESGO: UN ENFOQUE PRÁCTICO

PERSONAL DATA PROTECTION LAW AND RISK ANALYSIS: A PRACTICAL APPROACH

FERNANDO FRANCISCO GARCÍA-SOTOCA BARREDA

Doctorando del Programa de Doctorado en Unión Europea de la UNED.
Responsable de Actuaciones y Proyectos en Protección de Datos del Grupo Tragsa

Resumen: En un entorno social caracterizado por la masiva puesta a disposición de nuestros datos a organizaciones con creciente capacidad para procesarlos y extraer información valiosa, la protección de datos personales no sólo es un derecho reconocido constitucionalmente, sino que posee el carácter de garantía de otros derechos.

La protección de estos derechos, conforme al Reglamento General de Protección de Datos, debe instrumentarse mediante un proceso de gestión del riesgo para el cual existen múltiples propuestas metodo-

lógicas, desde las específicas para la protección de datos personales, desarrolladas por diversas autoridades de control, o la norma ISO 29134; hasta otras de carácter genérico, como la norma ISO 31000; o específicas del campo de la seguridad de la información, como el estándar ISO 27005 o MAGERIT.

El presente artículo explora las particularidades de cada una de esas metodologías y, a partir de diversas entrevistas y del análisis de la normativa interna y del proceso de implantación de un sistema de gestión del riesgo en una organización real, plantea diversas recomendaciones y buenas prácticas para la gestión del riesgo sobre los derechos y libertades de las personas físicas.

Palabras clave: privacidad, RGPD, riesgo, derechos, impacto.

Abstract: In a social environment characterized by the massive availability of our data to organizations with increasing capacity to process them and extract valuable information, the protection of personal data is not only a constitutionally recognized right, but also has the character of a guarantee of other rights.

The protection of these rights, in accordance with the General Data Protection Regulation, must be implemented through a risk management process for which there are multiple methodological proposals, from those specific to the protection of personal data, developed by various control authorities, or the ISO 29134 standard; to others of a generic nature, such as the ISO 31000 standard; or specific to the field of information security, such as the ISO 27005 or MAGERIT standard.

This article explores the particularities of each of these methodologies and, based on various interviews and the analysis of internal regulations and the process of implementing a risk management system in a real organization, proposes various recommendations and good practices for risk management on the rights and freedoms of natural persons.

Key words: privacy, GDPR, risk, rights, impact.

I. DERECHOS Y LIBERTADES ANTE LA NUEVA ECONOMÍA DEL DATO

La definición de la protección de datos como derecho ha evolucionado paralelamente a un importante cambio social. La informatización, la expansión de Internet, la forma de relacionarnos con el entorno, nuestras interacciones en redes sociales, servicios en línea,

de mensajería, *chatbots* y dispositivos conectados (Internet de las Cosas o *IoT*) implican la masiva puesta a disposición de nuestros datos personales a empresas y organizaciones con una creciente capacidad para procesarlos y extraer información valiosa gracias a nuevas tecnologías como el *big data* o la inteligencia artificial.

Todos estos datos que cedemos, en ocasiones como contraprestación más o menos tácita por unos servicios, a su vez suponen la materia prima de «la economía de los datos»[1]: un mercado de información asimétrica en el que grandes plataformas y operadores tienen más información que los titulares de los datos y pequeñas y medianas empresas, lo que les permite imponer condiciones ventajosas en un mercado oligopolístico[2].

Este desequilibrio de poder afecta no solo a nuestras libertades y derechos individuales[3], con repercusiones materiales muy palpables como, por ejemplo, que en base a perfiles generados mediante la interconexión de nuestros rastros digitales se nos conceda o no un crédito, o se tenga acceso a un seguro de salud, sino también a los colectivos. Tanto porque, cuando cedemos nuestros datos genéticos, estamos también dando información sobre nuestros familiares, o porque nuestra agenda telefónica o historial de llamadas facilita información sobre los grupos sociales en los que se integran nuestros conocidos; como porque, por ejemplo, la publicidad personalizada con fines electorales puede llegar a afectar a las normas y principios de funcionamiento democrático en nuestras sociedades[4].

La importancia de los datos ha llevado a la Unión Europea a dotarse de instrumentos jurídicos para fortalecer su desarrollo económico y social, su mercado interno y su competitividad, facilitando el intercambio e incrementando la calidad y disponibilidad de los datos generados en los países miembros mediante la mejor gobernanza del dato, pero protegiendo a la vez los derechos y libertades de sus

---

[1] ONTIVEROS E., LÓPEZ SABATER, V., *Economía de los Datos. Riqueza 4.0,* Fundación Telefónica y Editorial Ariel, Madrid 2017, pág. 23

[2] COMISIÓN EUROPEA, *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una estrategia europea de datos,* Bruselas 2020, pág. 9

[3] GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales: en la Era del Big Data y de la computación ubicua*, Edit. Dykinson , Madrid 2016, págs. 23, 44 y 45

[4] PEREZ LUÑO, A., «La protección de la Intimidad frente a la Informática en la Constitución Española de 1978», *Revista de Estudios Políticos*, n. 9, 1979, pags. 59-72, esp. pags. 67 y sig. y en términos similares COTINO HUESO, L., y OTROS, «Encuesta sobre la protección de datos personales», *Teoría y realidad constitucional*, n. 46, 2020, p*ágs*. 15-118, esp. pág. 83

ciudadanos. Este acervo está integrado principalmente por el Reglamento de datos no personales[5], la Directiva de datos abiertos y reutilización de la información del sector público[6], el Reglamento sobre gobernanza europea del dato[7], el Reglamento de Mercados Digitales[8], el Reglamento de Servicios Digitales[9], el Reglamento Europeo sobre Inteligencia Artificial[10] y por supuesto el Reglamento General de Protección de Datos[11].

El derecho de la protección de datos personales se inicia de la mano de otros conceptos relacionados. Así, el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH) ya en 1953 recogía, en su artículo 8, el derecho al respeto de la vida privada y familiar, el domicilio y la correspondencia de las personas. Posteriormente, en aplicación del Tratado de la Unión Europea (TUE), este derecho era reconocido como principio general y parte del Derecho de la Unión. Más específicamente, el artículo 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea (TFUE), reconocían el derecho a la protección de datos, estableciendo el mandato de adoptar normas que regulasen esta materia. Dicho mandato

[5] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

[6] Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019 relativa a los datos abiertos y la reutilización de la información del sector público

[7] Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos)

[8] Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales)

[9] Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales)

[10] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.o 300/2008, (UE) n.o 167/2013, (UE) n.o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial)

[11] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD)

se cumplió principalmente mediante la ya derogada Directiva 95/46/CE[12] y del actual RGPD, así como otras normas complementarias[13].

A nivel nacional, más allá del artículo 18.4 de la Constitución Española, que conforme a la STC 94/1998, FJ6, reconoce la protección de datos como un derecho fundamental autónomo, el primer desarrollo normativo del derecho a la protección de datos lo encontramos en la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), derogada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). Ésta, a su vez, fue sustituida por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), que según su artículo 1, completa y adapta el RGPD al ordenamiento español.

La interpretación del derecho a la protección de datos en un sentido pasivo, consistente en garantizar el honor y la intimidad del individuo frente a amenazas externas, ha ido evolucionando, distanciándose por un lado del propio concepto de intimidad, dado que su protección abarca incluso datos personales excluidos del ámbito de lo íntimo, como los de carácter público[14], y adoptando otra interpretación activa, alineada con el criterio del Tribunal Constitucional[15],según la cual el individuo debe tener la facultad de controlar y conocer el uso de sus datos, «*habeas data*», incluso en ausencia de ninguna amenaza[16]. Esta facultad se concreta en un haz de derechos recogidos a lo largo del capítulo III del RGPD y de los Títulos III y X de la LO 3/2018 en los conocidos como derecho de información, derechos digitales y, sobre todo, los derechos ARCOPOL (acceso, rectificación, cancela-

[12] 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos

[13] Como la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos

[14] MADRID CONESA, F., *Derecho a la intimidad, informática y estado de derecho*, Universidad de Valencia, Valencia 1984, pág. 45

[15] STC 254/1993, FJ7; STC 290/2000, FJ7; STC 292/2000, FJ6; STC 39/2016, FJ3; o STC 58/2018, FJ5

[16] MARTINEZ DE PISÓN, J., «Vida privada sin intimidad. Una aproximación a los efectos de las intromisiones tecnológicas en el ámbito íntimo», *Derechos y Libertades*, n. 37, 2017, págs. 51-84, esp. pág. 62

ción o supresión, oposición y derecho a no ser objeto de decisiones automatizadas, portabilidad, olvido y limitación del tratamiento).

El derecho fundamental a la protección de datos, como cualquier otro, está limitado por la garantía de otros derechos y bienes constitucionalmente protegidos, como el derecho a la libertad de expresión y de información, libertad de empresa, o el derecho a la vida y a la protección de la salud. La preponderancia de unos derechos sobre otros debe establecerse mediante la ponderación de los intereses en conflicto[17].

Sin embargo, la protección de datos personales también tiene un carácter instrumental, convirtiéndose en garantía de esos mismos derechos. Así, el Grupo de Trabajo del Artículo 29 (GT 29) menciona expresamente la libertad de expresión, la libertad de pensamiento, la libertad de circulación, la prohibición de discriminación, el derecho a la libertad y la libertad de conciencia y de religión como derechos a proteger[18]. A título de ejemplo, un sistema telemático de votación en elecciones sindicales no solo debe garantizar la integridad de un dato personal (el voto) sino que, a través de esta, se respete la legítima representación del trabajador y, por tanto, su libertad sindical.

II. Proactividad, privacidad desde el diseño y por defecto y enfoque al riesgo

El derecho a la protección de datos implica la imposición a los tenedores de dichos datos de determinados deberes jurídicos[19], cuyo núcleo principal son los principios relativos al tratamiento, recogidos en el artículo 5 del RGPD y el Título II de la LOPDGDD: la licitud, lealtad y transparencia del tratamiento; la limitación de la finalidad; el principio de minimización; el de exactitud; delimitación del plazo de conservación; de seguridad; y el principio de responsabilidad activa, proactividad o *accountability*.

Este último implica la necesidad de poder demostrar mediante evidencias la eficacia de unas medidas cuya finalidad es garantizar el cumplimiento del RGPD[20], es decir, exige la diligencia debida del res-

[17] Considerando cuarto, y artículo 23 RGPD, además de REBOLLO DELGADO, L., y SERRANO PÉREZ, M., *Manual de protección de datos*, Dykinson: Universidad Nacional de Educación a Distancia, Madrid 2019, pág. 273

[18] GRUPO «PROTECCIÓN DE DATOS» DEL ARTÍCULO 29, *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679 (WP 248 rev.01)*, 2017, pág. 7

[19] STC 292/2000, FJ6 y STC17/2013, FJ4

[20] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 3/2010 on the principle of accountability (WP173)*, 2010, pág. 9 y ESTEPA MONTERO, M., «El prin-

ponsable del tratamiento, siendo esta obligación, conforme a la STS 188/2022, FD3, no de resultados, es decir, de inexistencia de fallos o brechas, sino de adoptar las medidas que razonablemente puedan considerarse adecuadas y suficientes.

Sin embargo, la adecuación de estas medidas está sujeta a una interpretación subjetiva, siendo el enfoque al riesgo la forma de determinar si se ha cumplido con ese deber de diligencia. Tal como recoge el artículo 32 y los considerandos 74 y 83 del RGPD, así como el artículo 28 de la Ley 3/2018, las medidas a aplicar deben depender de los riesgos para los derechos y libertades de las personas físicas, por lo que deben ser identificadas e implantadas mediante la instauración de un proceso de gestión del riesgo[21] documentado y repetible, precisamente para estar en condiciones de demostrar su eficacia e idoneidad.

Por su parte, el artículo 25 RGPD introduce el concepto de protección de datos desde el diseño y por defecto, en el que se exige un enfoque preventivo y no correctivo frente a las posibles amenazas, y en el que las medidas técnicas y organizativas adecuadas se implanten antes y durante el tratamiento. Esto se logra, según la propia Agencia Española de Protección de datos (AEPD) mediante «*un enfoque orientado a la gestión del riesgo y de responsabilidad proactiva*» [22].

Es decir, los conceptos de responsabilidad proactiva, privacidad desde el diseño, y enfoque al riesgo, están íntimamente ligados entre sí, y son complementarios, siendo la gestión de riesgos la pieza clave que muestra el paso de la reactividad a la proactividad, tal como han puesto de manifiesto diferentes expedientes sancionadores de la AEPD[23].

Pero ¿qué es el riesgo? Dado que el RGPD no proporciona ninguna definición podríamos decir que es la posibilidad, más o menos probable, de que se materialice un daño. Existen definiciones más formales, como la aportada por la norma internacional ISO 31000, según

---

cipio de responsabilidad proactiva o rendición de cuentas como informador del régimen jurídico de la protección de datos de las personas físicas», *Anuario jurídico y económico escurialense*, n. 55, 2022, págs. 67-90, esp. pág. 85

[21] STJUE C-340/21, de 14 de diciembre EU:C:2023:986, apartados 29, 30 y 52

[22] AEPD, *Guía de Privacidad desde el Diseño,* 2019, págs. 6 y 7, en https://www.aepd.es/guias/guia-privacidad-desde-diseno.pdf

[23] AEPD, *Expediente N.º: PS/00677/2022. Procedimiento Sancionador*, 2023, págs. 59, 77, 109 y 110; y *AEPD, Expediente N.º: PS/00059/2022. Procedimiento sancionador,* 2022, pág. *5;* AEPD, *Expediente N.º: PS/00078/2024. Procedimiento sancionador, 2024,* pág 18

la cual el riesgo es el «*efecto de la incertidumbre sobre los objetivos*»[24] o por la ISO 27005, que lo define como «el potencial de las *amenazas para explotar las vulnerabilidades de un activo […] y, por lo tanto, causar daños a una organización*»[25], entendiendo como activo cualquier recurso necesario para la consecución de los objetivos de una organización. El GT 29, a su vez, lo define como «*un escenario que describe un acontecimiento y sus consecuencias, estimado en términos de gravedad y probabilidad*»[26], introduciendo los dos parámetros que definen un riesgo, la probabilidad o dimensión matemática que, en términos relativos o porcentuales mide la posibilidad de que un riesgo se materialice, y la gravedad o impacto, que es la medida del daño en caso de producirse.

Por su parte, la gestión del riesgo es el proceso continuo y sometido a monitorización que incluye todas las acciones realizadas para mitigar los riesgos y que suele clasificarse en tres etapas; identificación de amenazas; evaluación de los riesgos; y tratamiento de estos. Es habitual referirse a las dos primeras etapas con el nombre de análisis de riesgos.

El RGPD en ningún momento menciona expresamente estos conceptos, salvo en el considerando 83, al manifestar que se «*deben evaluar los riesgos*». En cambio, sí regula explícitamente en su artículo 35 la evaluación de impacto relativa a la protección de datos (EIPD), que no deja de ser una herramienta de gestión del riesgo más exhaustiva, ideada para tratamientos de datos de alto riesgo, particularmente aunque no de forma exclusiva, los contemplados en el artículo 35.3 RGPD y la directriz WP 248 del GT29[27].

III. Metodologías para análisis del riesgo

En cuanto a cuestiones metodológicas, el RGPD únicamente establece, en su considerando 76, la exigencia de que el riesgo deba pon-

[24] ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (UNE). COMITE TÉCNICO CTN 307 GESTIÓN DE RIESGOS, *UNE-ISO 31000 Gestión del riesgo — Directrices*, AENOR, Madrid 2018, págs. 7 y 8

[25] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). TECHNICAL COMMITTEE ISO/IEC JTC 1 «INFORMATION TECHNOLOGY», SUBCOMMITTEE SC 27, INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION. *ISO/IEC 27005. Information, security, cybersecurity and privacy protection - Guidance on managing information security risks*, ISO/IEC, Vernier 2022, pág. 2

[26] GRUPO «PROTECCIÓN DE DATOS» DEL ARTÍCULO 29, *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679 (WP 248 rev.01),* 2017, pág. 7

[27] Ibid, pp. 10 y sig.

derarse «*sobre la base de una evaluación objetiva*», si bien la directriz WP248 del GT 29, ofrece un listado de marcos aplicables[28], algunos de los cuales vamos a analizar como metodologías específicas para la protección de datos.

Por otro lado, los análisis de riesgos son herramientas cuyo uso está difundido en múltiples campos, por lo que las propuestas metodológicas disponibles son muy diversas y adaptadas a contextos, incluso temporales, diferentes. Por ello, algunas de las puntualizaciones que se van a realizar no deben entenderse tanto como críticas sino como matices que reflejan particularidades específicas de cada una de ellas.

III.1. Metodologías de la AEPD

La AEPD ha publicado a lo largo de los últimos años tres guías relacionadas con la gestión del riesgo; las dos primeras, del año 2018[29], han sido sustituidas en 2021 por un nuevo documento[30], que refleja la evolución de los criterios de la Autoridad de Control.

En las guías del 2018 se diferenciaba por un lado un análisis básico de riesgos, o análisis simplificado, para las actividades de tratamiento con baja exposición al riesgo, y por otro las evaluaciones de impacto para tratamientos de alto riesgo. Sin embargo, en la guía del 2021, se unifica el proceso de gestión del riesgo, al que debe estar sometido cualquier tratamiento de datos y, solo en caso de determinar que el riesgo es alto o muy alto, se procederá a realizar el juicio de idoneidad, necesidad y proporcionalidad, que exige la evaluación de impacto, conforme a la STC 14/2003, FJ9.

Un aspecto cuestionable de las guías de 2018 eran las tipologías de riesgos contempladas, diferenciando por un lado los asociados a la seguridad de la información y, por otro, los riesgos de incumplimiento normativo como, por ejemplo, la falta de legitimación para el tratamiento, o la falta de derecho de información. De hecho, se proponía

[28] Ibid, pp. 23 y 24

[29] AEPD, *Guía Practica de Análisis de Riesgos en los Tratamientos de Datos Personales Sujetos al RGPD,* 2018, en https://www.aec.es/wp-media/uploads/DPD-00117.AEPD-D-GUI-005-guia-analisis-de-riesgos-rgpd.pdf

[A]EPD, *Guía Practica para las Evaluaciones de Impacto en la Protección de los Datos Sujetas al RGPD*, 2018, en https://www.aec.es/wp-media/uploads/DPD-00116.AEPD-D-GUI-004-guia-evaluaciones-de-impacto-rgpd.pdf

[30] AEPD, *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*, 2021, en https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

un catálogo estandarizado de amenazas que ponía un gran énfasis en estos riesgos de incumplimiento normativo.

En cambio, en el nuevo marco metodológico propuesto por la AEPD en 2021 se diferencia claramente la gestión del riesgo del cumplimiento normativo, siendo este un requisito previo e independiente[31]. En otras palabras, que un tratamiento incumpla el RGPD no debe ser un riesgo a mitigar hasta un nivel aceptable, sino una opción inaceptable que debe corregirse o no llevarse a cabo.

Aún más sorprendente resultaba la inclusión, dentro del catálogo de factores de riesgo de las primeras guías, de algunas amenazas que no tenían impacto en los derechos y libertades de los interesados, sino en la propia organización como, por ejemplo, pérdidas económicas, reputacionales o de clientes. En este sentido el actual criterio de la AEPD es que deben protegerse las personas que están detrás de los datos y deben excluirse «*otra serie de riesgos a los que puede encontrarse sometida la organización y que afecten a su ámbito de negocio*»[32]. No obstante, considera deseable la integración de ambas gestiones, aunque no aclara cómo compaginar la defensa de unos intereses que, en ocasiones, pueden llegar a ser contrapuestos.

El nuevo catálogo de amenazas elaborado por la AEPD en 2021, además de resolver estas contradicciones, es mucho más amplio, meticuloso y detallado, valorando incluso muchos de los factores de riesgo.

Respecto a la valoración del riesgo, la AEPD propone una escala de nivel de riesgo (bajo, medio, alto y muy alto), resultado de combinar los valores de probabilidad e impacto, definidos como variables ordinales conforme a una serie de criterios cualitativos.

En definitiva, esta metodología se constituye como una opción que ha superado sus iniciales incoherencias, consistente y sencilla.

III.2. Otras metodologías específicas para protección de datos

Otra metodología reconocida por el GT 29 es la de la Autoridad Catalana de Protección de Datos[33] (APDCAT), exclusiva para evalua-

[31] Ibid, pp. 17 y sig.

[32] AEPD, *Expediente N.º: PS/00677/2022. Procedimiento Sancionador,* 2023, *pág*. 73

[33] APDCAT, *Evaluación de impacto relativa a la protección de datos,* 2022, en https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Guia-EIPD.pdf

ciones de impacto, y con un alcance, por tanto, limitado a los tratamientos de alto riesgo.

Esta metodología diferencia entre dos tipos de riesgos: los asociados a la seguridad de la información, resultado de una violación de seguridad; y los riesgos inherentes al tratamiento, resultado de la propia concepción o diseño del tratamiento, sin necesidad de que se produzca ningún tipo de error técnico, humano o ataque.

La metodología planteada para estos últimos es similar a la de la AEPD, pero para los riesgos de seguridad se proponen, para el cálculo del impacto, una serie de escenarios (ej.: pérdida de un ordenador, o borrado de un fichero), y se fijan una serie de criterios que incrementarían el riesgo (ej.: tratamiento de datos de carácter especial, monitorización de personas, etc.). A su vez, para el cálculo de la probabilidad establece una lista de control con una serie de cuestiones como; «*¿Alguna parte del tratamiento se hace a través de internet?*», «*¿Puede el personal conectar dispositivos externos al sistema?*», «*¿Se ha externalizado alguna parte del tratamiento a un encargado?*», y en función del número de respuestas afirmativas se determina el nivel de probabilidad.

Se aporta, además, otro listado de medidas mitigadoras y su eficacia para hacer frente a las cuestiones del listado de control antes mencionado. De esta forma, determinando cuales de esas medidas se han implantado se reduce el número de respuestas afirmativas, y por tanto la probabilidad residual.

Otro marco aplicable es el establecido por la Comisión Nacional de la Informática y las Libertades (CNIL), autoridad de control de la República Francesa, entre cuyas publicaciones se encuentran una serie de guías relativas a las evaluaciones de impacto[34] y, por tanto, también limitadas en su alcance a los tratamientos de alto riesgo.

Las amenazas se definen, en este caso, como fuentes de riesgo que aprovechan vulnerabilidades de los activos que dan soporte al tratamiento, lo que implica un concepto de riesgo y un proceso de identificación complejo y cercano a metodologías propias de la seguridad de

[34] CNIL, *Privacy Impact Assessment (PIA). Methodology*, 2018, en https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

[c]NIL, *Privacy Impact Assessment (PIA). Templates*, 2018, en https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf

[c]NIL, *Privacy Impact Assessment (PIA). Knowledge bases*, 2018, en https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

[c]NIL, *Privacy Impact Assessment (PIA). Application to IoT devices*, 2018, en https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-en.pdf

la información. Por ejemplo, una posible amenaza sería un empleado sobornado (la fuente del riesgo), que aprovecha que el sistema de gestión de ficheros permite su manipulación (la vulnerabilidad), para modificar o borrar datos personales. de dichos ficheros (el activo).

Para finalizar, la norma 27701[35], extensión de la norma ISO 27001, tiene como objetivo proteger la privacidad mediante la implantación de un sistema de gestión. Esta norma recoge la necesidad de aplicar un procedimiento de evaluación de riesgos y de realizar evaluaciones de impacto relativas a la protección de datos o PIA (*Privacy Impact Assesment*), cuestión que, a su vez, es desarrollada en la norma ISO 29134[36].

Incluye esta norma un listado de posibles amenazas y activos, a la vez que recomienda que el proceso de análisis sea escalable, es decir, que sea más o menos detallado en función de la gravedad e indica que deben evaluarse las consecuencias no solo para los interesados, sino también para la organización.

III.3. Metodologías no específicas

La norma *ISO 31000* proporciona un enfoque común para gestionar cualquier tipo de riesgo de cualquier organización y su marco es similar a otros específicos de protección de datos, como el propio de la AEPD, a la que claramente inspira. En ella se señala que deben asignarse los recursos apropiados (humanos, materiales y organizativos) a la gestión del riesgo, e introduce la necesidad de tener en cuenta las limitaciones del conocimiento, los sesgos y creencias de las personas involucradas y la confiabilidad de la información.

Dentro del marco de trabajo de la ISO 31000 y como apoyo a esta, la norma 31010[37] describe técnicas concretas para el análisis del ries-

[35] ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (UNE). COMITE TÉCNICO CTN 307 GESTIÓN DE RIESGOS, *UNE-EN ISO/IEC 27701. Técnicas de seguridad. Extensión de las Normas ISO/IEC 27001 e ISO/IEC 27002 para la gestión de privacidad de la información. Requisitos y directrices. (ISO/IEC 27701:2019)*, AENOR, Madrid 2021

[36] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). TECHNICAL COMMITTEE ISO/IEC JTC 1 «INFORMATION TECHNOLOGY, *UNE-EN ISO/IEC 29134:2020. Tecnología de la información. Técnicas de seguridad. Directrices para la evaluación del impacto de la privacidad (ISO/IEC 29134:2017) (Ratificada por la Asociación Española de Normalización en mayo de 2020)*, AENOR, Madrid 2020

[37] GRUPO ESPECÍFICO DE CARÁCTER TEMPORAL AEN/GET13 GESTIÓN DE RIESGOS, *UNE-EN 31010. Gestión del Riesgo. Técnicas de Apreciación del Riesgo*, AENOR, Madrid, 2011

go. Algunas de estas técnicas, habituales por su sencillez y bajo coste, son los catálogos o listados de verificación; los índices o escalas de riesgo para valorar, impacto, probabilidad o nivel de riesgo; o las matrices de consecuencias/probabilidad, que permiten obtener el nivel de los riesgos para compararlos y ordenarlos jerárquicamente.

Otras técnicas fácilmente aplicables son las tormentas de ideas, en las que se debate sin que ninguna idea sea censurada; las entrevistas estructuradas o semiestructuradas, que permiten una mayor reflexión pero requieren más tiempo; la técnica Delphi, en la que un grupo de expertos responde a un cuestionario, ofreciéndoles la posibilidad de cambiar su respuesta sobre aquellas en las que existe diversidad de opiniones y repitiendo el proceso hasta que se logra un consenso suficiente; o la técnica de análisis de la causa primordial o raíz (RCA), que parte de un suceso adverso para identificar las causas subyacentes hasta llegar a la más profunda. Por ejemplo, en un envío erróneo de correos electrónicos, la causa superficial sería el error humano, pero la causa inmediata subyacente sería la realización de una tarea repetitiva y monótona, que a su vez estaría provocada por la falta de automatización del proceso, siendo la causa raíz que el departamento de sistemas no dispone de suficientes recursos para acometer desarrollos nuevos.

Otro grupo de metodologías no específicas para la protección de datos son las concebidas para la gestión de la seguridad de la información, entre las que destaca la metodología MAGERIT y las de la familia de la norma ISO 27001.

El estándar internacional ISO 27001[38] especifica los requisitos para implantar, mantener y mejorar un sistema de gestión de la seguridad de la información, así como para la apreciación y el tratamiento de sus riesgos, cuya implantación a su vez se desarrolla en la norma ISO/IEC 27005[39]. Una de sus aportaciones más novedosas respecto a otras metodologías es que el enfoque ciclico no es solo aplicable a todo el proceso de gestión en su conjunto, sino también y específi-

[38] ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (UNE). COMITÉ TÉCNICO CTN-UNE 320 CIBERSEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES, *UNE-ISO/IEC 27001 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos*, AENOR, Madrid, 2023

[39] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). TECHNICAL COMMITTEE ISO/IEC JTC 1 «INFORMATION TECHNOLOGY», SUBCOMMITTEE SC 27, INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION, *ISO/IEC 27005. Information, security, cybersecurity and privacy protection - Guidance on managing information security risks*, ISO/IEC, Vernier, 2022

camente para las fases de análisis, lo que permite aumentar en cada iteración el nivel de conocimiento sobre los riesgos.

Por otro lado, la norma ISO 27005 sugiere dos tipos de enfoque para la identificación y análisis del riesgo: el basado en eventos o sucesos y el basado en activos. El primero es típicamente un enfoque «de arriba hacia abajo», que no requiere excesivos recursos, focalizándose en los riesgos más críticos y que parte de la identificación de escenarios o posibles sucesos por parte de la dirección o los propietarios de los riesgos de una organización, para a continuación analizar sus consecuencias.

El enfoque basado en activos es «de abajo hacia arriba», requiere la identificación y análisis de los activos de la organización, tanto los principales (información y procesos de valor) como los que les dan soporte (hardware, software, personal...), así como sus interdependencias, sus vulnerabilidades (por ejemplo, falta de mantenimiento, redes desprotegidas, etc.) y las amenazas (deliberadas, accidentales, etc.) que pueden aprovechar esas vulnerabilidades (por ejemplo, falta de mantenimiento o redes desprotegidas).

Por su parte MAGERIT (acrónimo de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) ha sido desarrollada por el CSAE (Consejo Superior de Administración Electrónica). La propia guía de MAGERIT[40] reconoce su complejidad, aconsejando aplicarla mediante una aproximación iterativa y adaptada a cada organización, logrando que en cada repetición se revise el modelo consiguiendo un mayor nivel de detalle, y gestionando en primer lugar los riesgos más graves para posteriormente acercarse a los menos críticos.

Esta metodología adopta un enfoque basado en activos en el que cada amenaza, riesgo y control se asignan a un activo concreto, por lo que la primera acción a realizar será inventariar los activos de la organización y determinar cómo se interrelacionan, para averiguar cómo el fallo de uno de ellos se traslada a los demás, y posteriormente determinar su valor y el coste que supondría su degradación; así, el valor de cada activo no dependerá únicamente de sí mismo, sino también de aquellos otros a los que da servicio. Estas tareas pueden simplificarse estableciendo como base, no activos concretos, sino grupos de ellos o «dominios de seguridad». Una aproximación gradual a esta

[40] DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA, *MAGERIT–versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método*, M. de Hacienda y Adm. Públicas, Madrid 2012, pág. 17

metodología sería establecer unos pocos dominios amplios y posteriormente, según el proceso ganase madurez, tender a desagregarlos.

Finalmente, el Esquema Nacional de Seguridad (ENS)[41] puede definirse como un sistema de gestión de la seguridad de la información, siendo uno de sus principios básicos, regulado en el artículo 7 del RD 311/2022, la «*gestión de la seguridad basada en los riesgos*», y uno de sus requisitos mínimos, incluido en el artículo 12.6.b), el «*análisis y gestión de riesgos*». Tanto los principios básicos como los requisitos mínimos se deben garantizar mediante la aplicación de las medidas de seguridad recogidas en el Anexo II del Real Decreto, una de las cuales, la op.pl.1, es el análisis de riesgos.

El ENS, por tanto, y al igual que el RGPD, exige configurar la seguridad mediante el establecimiento de unas medidas adecuadas a los riesgos. Esta interrelación entre ambas normas queda de manifiesto en los artículos 3.1 y 3.2 del RD 311/2022 según los cuales, cuando los sistemas de información traten datos personales, les será de aplicación el RGPD y deberá realizarse «*un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos*».

Sin embargo, el RD 311/2022 tampoco ofrece una metodología específica para la gestión del riesgo, aunque en la medida op.pl.1, apartado 4.1.1. del Anexo II establece que, en caso de que la categorización del sistema sea básica, baste con un análisis informal en lenguaje natural, si es de categoría media, uno semi-formal, con catálogos de amenazas y uno formal con fundamento matemático, si es de categoría alta.

El análisis de riesgos realizado en el ámbito del ENS deberá incluir también todos los requerimientos establecidos para el análisis de riesgos en el ámbito de la protección de datos, dado que, aunque el Anexo IV afirma que deberá considerarse el impacto en la organización, la medida mp.info 1.1, protección de los datos personales (apartado 5.7.1. del Anexo II), establece que se tendrán que implementar los requisitos necesarios conforme, entre otros criterios, a «l*os riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD*».

[41] Previsto en el artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, desarrollado por el Real Decreto 3/2010, de 8 de enero y derogado por el nuevo Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

Además, cabe destacar que el ENS, en su Anexo II, apartado 6, establece que, para valorar la implantación de las medidas de seguridad, incluyendo los análisis de riesgos, se estimará su nivel de madurez conforme a la siguiente escala:

- L0 - Inexistente: la medida no está implantada.
- L1 - Inicial. Ad hoc: se realiza algún tipo de actividad de análisis de riesgos, pero limitada y no sistemática.
- L2 - Reproducible, pero intuitivo: las actividades son comunes a nivel corporativo porque existen procedimientos, pero estos no están documentados o la documentación es incompleta.
- L3 - Proceso definido: existen para toda la organización procedimientos y normativa detallada y documentada.
- L4 - Gestionado y medible: además de procedimientos documentados, también se dispone de métricas que se usan sistemáticamente para analizar la efectividad y eficiencia de la gestión del riesgo.
- L5 - Optimizado: el riesgo no solo está gestionado, con procedimientos y métricas definidas, sino que se busca a la mejora continua

III.4. Inteligencia Artificial como herramienta para la gestión del riesgo

La inteligencia artificial y el *machine learning* (aprendizaje automático) suelen ser vistos desde el punto de vista de la protección de datos como posibles amenazas o tratamientos objeto de regulación. Sin embargo, podrían ser tecnologías muy útiles como herramientas para la gestión de riesgos. Su uso se encuentra bastante desarrollado en ámbitos como la gestión de riesgos financieros, en el que es habitual el uso de algoritmos de clasificación o *clustering* para elaborar modelos de *rating* de clientes y la calificación de riesgos de crédito[42], así como para la gestión de riesgos de mercado, operacionales, de aseguramiento, mediante la detección y prevención de eventos de riesgo y datos anómalos (ej. quiebras o detección de fraude)[43].

[42] FRITZ-MORGENTHAL, S., HEIN, B., & PAPENBROCK, J., «Financial Risk Management and Explainable, Trustworthy, Responsible AI». *Frontiers in Arificial Intelligence*, n. 5, 2022, págs. 9 a 13

[43] MASHRUR, A., LUO, W., NAYYAR A., Z., & ROBLES-KELLY, A., «Machine Learning for Financial Risk Management: A Survey». *IEEE Access,* n. *8*, 2020, págs.

Otro campo donde su uso está más desarrollado es el de la seguridad de la información, sobre todo para modelos de detección y filtrado de spam mediante el reconocimiento de patrones; la detección de trafico de red malicioso y url´s maliciosas mediante el análisis de comportamientos anómalos; o más novedosamente, el control de accesos, que tradicionalmente se realiza mediante rígidas políticas de acceso pero que podría realizarse incorporando combinaciones con técnicas de aprendizaje no supervisado (*clustering*) y reconocimiento de comportamientos anómalos[44].

El grado de desarrollo de estas técnicas en el campo de la protección de datos es menor, siendo la aplicación más habitual la localización de datos personales y su etiquetado automático, mediante técnicas de identificación de patrones y clasificación[45].

Sin embargo, estas aplicaciones son más medidas preventivas de tratamiento del riesgo que de análisis de riesgos. Aun así, se están realizando desarrollos en herramientas comerciales combinando inteligencia artificial generativa con técnicas de clasificación o *clustering*, de tal forma que el motor de IA, dadas las características de una organización, sugiera un listado de posibles amenazas que el usuario puede seleccionar. Estos asistentes de IA, actualmente, no ofrecen muchas ventajas frente a los clásicos catálogos de amenazas[46].

Posiblemente, la principal causa por la que no se están adoptando más rápidamente estas nuevas tecnologías al campo que nos ocupa es la falta de disponibilidad de datos para el desarrollo de modelos de IA, por lo que su solución pasaría por la puesta en común de dichos datos, tanto en el ámbito de la iniciativa privada como pública, lo que permitiría poner a disposición de los desarrolladores suficiente información como para entrenar nuevos modelos. Para ello se cuenta con el marco establecido por la Directiva Europea de datos abiertos y reutilización de la información del sector público y del Reglamento sobre Gobernanza Europea del Dato.

203203-203223 y MARTIN, L., SUNEEL, S., & MADDULETY, K., «Machine Learning in Banking Risk Management: A Literature Review». *Risks,* n. 7, 2019, págs. 1-29

[44] CHIO, C., Y FREEMAN, D., *Machine learning and security: Protecting systems with data and algorithms,* , O'Reilly Media Inc, Sebastopol CA 2018, págs. 1, 13 y 14

[45] https://www.onetrust.com/es/products/data-discovery/

[46] https://www.youtube.com/watch?v=CoKuWOON62U

IV. LAS ORGANIZACIONES FRENTE A LA GESTIÓN DEL RIESGO EN PROTECCIÓN DE DATOS

Tras el análisis del contexto jurídico y de las diferentes propuestas metodologías disponibles, se han realizado distintas entrevistas en profundidad con delegados de protección de datos (DPD) y otros profesionales responsables de protección de datos, lo que ha permitido alcanzar diversas conclusiones, no solo sobre sus criterios y opiniones, sino también sobre las organizaciones donde prestan sus servicios (empresas públicas y privadas, del sector de la construcción, emergencias, consultoría, transporte de viajeros, mensajería, organizaciones sindicales y sanidad). Igualmente, se ha estudiado en detalle un caso de implantación real de un sistema de gestión del riesgo para los derechos y libertades en una organización de gran tamaño, así como su normativa interna.

IV.1. La experiencia de los expertos

Todas estas organizaciones realizan una gestión del riesgo sobre protección de datos personales que generalmente abarca todas las actividades de tratamiento de datos, siendo la situación más común, en cuanto a la madurez del sistema, el nivel L3, con procedimientos definidos y documentados para toda la organización, siendo habitual el apoyo de consultoras externas en momentos iniciales de su implantación.

Además, casi todas siguen el esquema de las antiguas guías de la AEPD, es decir, realizan un análisis básico de todos los tratamientos y una evaluación de impacto más detallada en los casos más críticos. Menos habitualmente siguen el nuevo criterio de la AEPD, esto es, un único proceso de gestión de riesgos indiferenciado para todos los tratamientos, al que se añade el análisis de necesidad, idoneidad y proporcionalidad en los tratamientos de alto riesgo.

Por otro lado, la mitad de las organizaciones incluyen como riesgos los posibles incumplimientos de la normativa de protección de datos, en tanto que la otra mitad no lo hace, ciñéndose al criterio de la última guía de la AEPD.

En cuanto a la integración de los riesgos de seguridad de la información y de protección de datos, el abanico es muy amplio, pero la situación más habitual es la de un contacto estrecho y colaboración entre ambas áreas, pero sin una integración formal. La organización con mayor grado de madurez importa los riesgos y controles de los

riesgos en seguridad dentro del sistema de riesgos de protección de datos.

Respecto a los aspectos más puramente metodológicos, la mayoría de las organizaciones entrevistadas utilizaba la última metodología AEPD, basada en escenarios, con métodos semicuantitativos y utilizando sus catálogos de amenazas y controles, si bien adaptados a cada organización. Los profesionales con perfil no jurídico sino técnico, sin embargo, tienden a adaptar metodologías COSO, MAGERIT o ISO 27005, es decir, no específicas para la protección de datos y basadas en activos.

De las técnicas y métodos utilizados, dos son prácticamente unánimes: los listados de verificación sobre amenazas o controles, y las entrevistas con los propietarios o responsables de los riesgos (métodos sencillos, pero sujetos a una mayor subjetividad). También se ha identificado, aunque esporádicamente, el uso del método Delphi para la valoración de los riesgos o herramientas de *pen-testing,* y árboles de fallos para la identificación de amenazas.

Por último, casi todos los entrevistados indican que el factor más importante para el buen funcionamiento del sistema es lograr la implicación e impulso de la dirección de la organización.

IV.2. Estudio de un caso de implantación

La organización analizada comenzó la implantación de un sistema de gestión de la protección de datos con la entrada en vigor del RGPD y con el nombramiento de una Delegada de Protección de Datos. Durante año y medio se abordó la elaboración del registro de actividades de tratamiento y otras medidas de responsabilidad activa.

Al mismo tiempo, a iniciativa de la DPD, con ayuda de consultoras externas y sin participación de otras unidades, se realizan las primeras aproximaciones puntuales a la gestión del riesgo en protección de datos; dos análisis de riesgos consecutivos pero independientes centrados sobre todo en riesgos de cumplimiento del RGPD. El primer análisis supuso pasar de un nivel de madurez L0-Inexistente, a uno L1-Inicial, en tanto que el segundo, dado que se realizó en base a la metodología MAGERIT, usando la herramienta PILAR[47], y por tanto

[47] Conjunto de herramientas desarrolladas por el CCN (Centro Criptológico Nacional), para el análisis y gestión de riesgos en sistemas de información siguiendo esta metodología

de forma más sistemática, podría considerarse el salto hasta un nivel L2-Reproducible, aunque intuitivo.

Durante el segundo y tercer año se elabora la normativa interna, que incluye una norma específica sobre gestión del riesgo. Además, durante este periodo se realizan las primeras evaluaciones de impacto, realizadas conforme a la metodología incluida en la normativa interna, basada en la de la AEPD. Aun así, no se alcanza el nivel L3, dado que, a pesar de la existencia de los procedimientos, la gestión del riesgo sigue sin ser un proceso continuo, planificado y común para toda la organización, sino que sigue dependiendo de las iniciativas puntuales de la DPD.

A finales del tercer año comienza la implantación de una herramienta informática específica para la gestión del riesgo; y con ayuda de esta, la participación de todas las unidades organizativas y el asesoramiento de la DPD, durante el cuarto y quinto año se elaboran los análisis básicos de riesgos de todos los tratamientos de la organización. Tras esta acción se logra alcanzar el nivel L3-Proceso definido.

Respecto a la normativa interna, que según lo previsto en el artículo 24 del RGPD puede considerarse una medida organizativa de cara a cumplir con el principio de responsabilidad activa, establece roles como el de unidad propietaria del tratamiento y responsable de seguridad del tratamiento, lo que permite asignar a unidades y personas concretas las funciones sobre responsabilidades que el RGPG y la Ley 3/2018 atribuyen al responsable de tratamiento.

En este sentido, el CEPD, en su Directriz 07/2020 aclara, que «*aunque un departamento o unidad de una organización ostente la responsabilidad operativa de asegurar la conformidad de determinada actividad de tratamiento, ello no significa que dicho departamento o unidad (en lugar de la organización en su conjunto) devenga responsable del tratamiento*»[48]. Sin embargo, en una organización de gran tamaño, si no se definen las funciones a un nivel organizativo inferior, sería imposible la gestión de la protección de datos con criterios de eficacia y seguridad y, de hecho, esta definición de roles y responsables dentro de una organización se contempla como medida organizativa en la Guía de Gestión de Riesgos de la AEPD[49]. De igual forma también

[48] EUROPEAN DATA PROTECTION BOARD, *Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD*, 2021, págs. 11 y 12

[49] AEPD, *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*, 2021, págs. 106 y 107, en https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

en la guía de Privacidad desde el diseño de la AEPD se afirma que «*es preciso definir un marco de privacidad y una estructura de gobernanza que incluya […] los roles y responsabilidades que velen por su cumplimiento*»[50].

Concretamente, se asigna la responsabilidad de efectuar los análisis de riesgos a las distintas unidades organizativas propietarias de los tratamientos, debiendo ser impulsados por el responsable de seguridad designado y garantizando el asesoramiento de el/la DPD en tiempo oportuno, para evitar que su participación no sea en fases tan tardías del tratamiento que sea imposible aplicar el principio de la privacidad desde el diseño.

En cuanto a otros aspectos, como análisis de ciclo de vida, catálogos de amenazas, criterios para evaluar impacto, probabilidad y nivel de riesgo, etc.… la norma adapta la metodología más actualizada de la AEPD.

V. CONCLUSIONES Y BUENAS PRÁCTICAS

A la hora de implantar un sistema de gestión de riesgos en protección de los datos, las organizaciones se encuentran ante la decisión de escoger entre metodologías complejas y basadas en activos o metodologías basadas en escenarios, más sencillas, pero menos rigurosas y objetivas. Frente a esta disyuntiva suelen tomar la segunda opción, sacrificando objetividad frente a una menor necesidad de recursos. Esta implantación suele ser resultado de un proceso de aprendizaje que deviene generalmente en una propuesta metodológica adaptada a la organización, a su actividad, nivel de conocimiento del personal, experiencia y recursos disponibles. Pero, dado que ese contexto organizativo evoluciona, de igual forma debería hacerlo el sistema de gestión del riesgo.

De esta forma, es recomendable que su implantación sea progresiva. Es preferible tener a tiempo un análisis de riesgos imperfecto y que no entre en detalles (*quick and dirty*), pero suficiente para abordar los puntos más urgentes, que embarcarse en un sistema que, desde el primer momento, contemple todos los tratamientos de datos, todos los activos con sus interrelaciones y que intente estimar probabilidades e impactos con métodos cuantitativos, sin tener personal adecuado, experiencia, tiempo y recursos para ello. Una vez atajados los puntos más urgentes, entrará en juego la mejora continua, aumen-

[50] AEPD, *Guía de Privacidad desde el Diseño,* 2019, pág. 22, en https://www.aepd.es/guias/guia-privacidad-desde-diseno.pdf

tando sucesivamente la eficiencia y exactitud del sistema. Para esta evolución podría adoptarse un modelo de madurez como el explicado en apartados anteriores.

En cuanto a los procedimientos y normativas internas, es deseable que estas no se limiten a repetir lo ya establecido en la legislación, guías o directrices, sino que se adapten al contexto de cada organización y que no especifiquen sólo qué debe hacerse, sino cómo y quién, es decir, que definan claramente roles, funciones y responsabilidades.

Respecto de los indicadores, cuya inclusión puede no ser una necesidad apremiante en las primeras fases de implantación del sistema, deben permitir medir la eficiencia del sistema, lo que implica evaluar su capacidad de predecir y minimizar riesgos. El registro de brechas de privacidad sería una buena fuente de información a partir del cual se pueden obtener fácilmente indicadores útiles.

En fases de madurez avanzada podría plantearse, siempre que se cuente con los recursos suficientes, pasar gradualmente de un sistema basado en escenarios a uno basado en activos o integrar la gestión de riesgos de seguridad de la información con la de protección de datos, evitando así duplicar esfuerzos y recursos.

En cuanto a la integración de los incumplimientos normativos en protección de datos como riesgos, algo que contemplaban las primeras guías de la AEPD pero sigue siendo habitual, solo podría asumirse siempre y cuando estos riesgos se consideren inaceptables, sea cual sea su probabilidad. Esto tendría la ventaja de documentar, dentro del sistema de gestión de riesgos, los controles implantados para evitar los incumplimientos.

Respecto a las técnicas concretas utilizadas, las entrevistas pueden ser adecuadas siempre que los sujetos entrevistados tengan los conocimientos suficientes, o al menos sean asesorados por personas que sí cuentan con esos conocimientos. El uso de catálogos y listados, aunque facilitan la identificación a sus usuarios pueden dar lugar, por simple agotamiento, a decisiones poco meditadas. Además, su uso implica encorsetar y perder flexibilidad en el análisis de unos eventos que son complejos, inciertos, dinámicos y volubles, lo que puede llevar a reducir la capacidad para descubrir, entender y hacer frente a nuevos riesgos[51]; por ello se aconseja simplificarlos y dotarlos de mayor flexibilidad.

[51] OLSEN, O., «Dilemmas of standardization in risk governance» en Olsen, O., Juhl, K., Lindøe, P. y Engen, O., *Standardization and Risk Governance. A Multi-Disciplinary Approach*, Taylor & Francis Group, Abingdon 2019, págs. 275-280, esp. págs. 278 y 279

Es habitual mencionar la regla de Pareto según la cual, gestionando el 20% de los riesgos más importantes podría controlarse el 80% del riesgo total, de esta forma resulta razonable incorporar la escalabilidad del análisis para que, en función de la gravedad del riesgo, éste sea más o menos profundo, realizando un mayor esfuerzo en ese 20% de riesgos más graves.

Por otro lado, todo el sistema de gestión de riesgos para la protección de datos tiene como finalidad última cumplir y demostrar el cumplimiento de la *diligencia debida*. Por esa razón sería deseable que fuera verificado por cuenta de un tercero. Es decir, debería someterse periódicamente a auditorías de terceros que evaluasen si el sistema se ajusta a unas garantías mínimas.

En definitiva, la implantación de un sistema de gestión de riesgos sobre los derechos y libertades de las personas físicas es una tarea compleja y por tanto sujeta a muchas dificultades. Una de ellas puede ser la falta de conocimientos multidisciplinares de las personas implicadas, tanto para comprender el contexto y flujos de datos, como para identificar el riesgo, analizarlo, entender las tecnologías implicadas, etc... Para suplir estas carencias es fundamental la colaboración de las diferentes áreas implicadas; propietarias del riesgo, de protección de datos y de seguridad de la información, de forma que el conocimiento de unas complemente el de otras.

Sin embargo, la más crítica de las dificultades puede ser la falta de apoyo desde la dirección de la organización, que a su vez puede tener como consecuencia la falta de implicación del resto de la organización y la falta de recursos, no solo en términos económicos, sino humanos, sin los cuales la eficiencia del sistema se vería gravemente comprometida[52].

VI. BIBLIOGRAFÍA

CHIO, C., Y FREEMAN, D., *Machine learning and security: Protecting systems with data and algorithms,* , O'Reilly Media Inc, Sebastopol CA 2018.

COTINO HUESO, L., y OTROS, «Encuesta sobre la protección de datos personales», *Teoría y realidad constitucional*, n. 46, 2020, p*ágs*. 15-118.

[52] Este artículo es un extracto de una obra más extensa que podrá consultarse en breve en TESEO

ESTEPA MONTERO, M., «El principio de responsabilidad proactiva o rendición de cuentas como informador del régimen jurídico de la protección de datos de las personas físicas», *Anuario jurídico y económico escurialense*, n. 55, 2022, págs. 67-90.

FRITZ-MORGENTHAL, S., HEIN, B., & PAPENBROCK, J., «Financial Risk Management and Explainable, Trustworthy, Responsible AI». *Frontiers in Arificial Intelligence*, n. 5, 2022, págs. 9 a 13.

GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales: en la Era del Big Data y de la computación ubicua*, Edit. Dykinson , Madrid 2016.

MADRID CONESA, F., *Derecho a la intimidad, informática y estado de derecho*, Universidad de Valencia, Valencia 1984.

MARTINEZ DE PISÓN, J., «Vida privada sin intimidad. Una aproximación a los efectos de las intromisiones tecnológicas en el ámbito íntimo», *Derechos y Libertades*, n. 37, 2017, págs. 51-84.

MASHRUR, A., LUO, W., NAYYAR A., Z., & ROBLES-KELLY, A., «Machine Learning for Financial Risk Management: A Survey», *IEEE Access,* n. *8*, 2020, págs. 203203-203223.

MARTIN, L., SUNEEL, S., & MADDULETY, K., «Machine Learning in Banking Risk Management: A Literature Review», *Risks,* n. 7, 2019, págs. 1-29.

OLSEN, O., «Dilemmas of standardization in risk governance» en Olsen, O., Juhl, K., Lindøe, P. y Engen, O., *Standardization and Risk Governance. A Multi-Disciplinary Approach*, Taylor & Francis Group, Abingdon 2019, págs. 275-280.

ONTIVEROS E., LÓPEZ SABATER, V., *Economía de los Datos. Riqueza 4.0,* Fundación Telefónica y Editorial Ariel, Madrid 2017.

PEREZ LUÑO, A., «La protección de la Intimidad frente a la Informática en la Constitución Española de 1978», *Revista de Estudios Políticos*, n. 9, 1979, pags. 59-72.

PEREZ LUÑO, A., «La tutela de la libertad informática en la sociedad Globalizada», *Isegoría : revista de filosofía moral y política*, n, 2000, 2020, págs. 59-68.

RALLO LOMBARTE, A., «Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma», *Revista de Derecho Político,* n.85, 2012, págs.13-56.

RALLO LOMBARTE, A., «Una nueva generación de derechos digitales», *Revista de Estudios Políticos,* n. 187, 2020, págs. 101-135.

REBOLLO DELGADO, L., *Vida privada y protección de datos en la Unión Europea,* , Dykinson, Madrid 2008.

REBOLLO DELGADO, L., y SERRANO PÉREZ, M., *Manual de protección de datos*, Dykinson: Universidad Nacional de Educación a Distancia, Madrid 2019.

REBOLLO DELGADO, L., *Inteligencia artificial y derechos fundamentales*, Dykinson, Madrid 2023.

ZACHARIS, A. y OTROS, *Compendium of risk management frameworks with potential interoperability,* Europena Union Agency for cybersecurity (ENISA), Athens 2022.

Resoluciones AEPD y Jurisprudencia

AEPD, Expediente N.º: PS/00059/2022. Procedimiento sancionador, 2022.

AEPD, *Expediente N.º: PS/00078/2024. Procedimiento sancionador*, 2024.

AEPD, *Expe*diente N.º: PS/00677/2022. *Procedimiento Sancionador, 2023.*

STC 14/2003, de 28 de enero. (Tribunal Constitucional, 2003).

STC 17/2013, de 31 de enero. (Tribunal Constitucional, 2013).

STC 254/1993, de 20 de julio. (Tribunal Constitucional, 1993).

STC 290/2000, de 20 de noviembre . (Tribunal Constitucional, 2000).

STC 292/2000, de 30 de noviembre. (Tribunal Constitucional, 2000).

STC 39/2016, de 3 de marzo. (Tribunal Constitucional, 2016).

STC 58/2018, de 4 de junio. (Tribunal Constitucional, 2018).

STC 94/1998, de 4 de mayo. (Tribunal Constitucional, 1998).

STJUE C-340/21, de 14 de diciembre EU:C:2023:986 (Tribunal Superior de Justicia de la UE, 2023).

STS 188/2022, de 15 de febrero. (Tribunal Supremo, sala de lo Contencioso, 2022).

Legislación

Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019 relativa a los datos abiertos y la reutilización de la información del sector público.

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

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 respeta al tratamiento de datos personales y a la libre circulación de estos datos.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos.

Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales).

Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales).

Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos).

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.o 300/2008, (UE) n.o 167/2013, (UE) n.o

168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).

Guías e informes

AEPD, *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*, 2021, en https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

AEPD, *Guía de Privacidad desde el Diseño, 2019,* en https://www.aepd.es/guias/guia-privacidad-desde-diseno.pdf

AEPD, *Guía Practica de Análisis de Riesgos en los Tratamientos de Datos Personales Sujetos al RGPD, 2018* en https://www.aec.es/wp-media/uploads/DPD-00117.AEPD-D-GUI-005-guia-analisis-de-riesgos-rgpd.pdf

AEPD, *Guía Practica para las Evaluaciones de Impacto en la Protección de los Datos Sujetas al RGPD*, 2018,ven https://www.aec.es/wp-media/uploads/DPD-00116.AEPD-D-GUI-004-guia-evaluaciones-de-impacto-rgpd.pdf

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 3/2010 on the principle of accountability (WP173)*, 2010.

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (UNE). COMITE TÉCNICO CTN 307 GESTIÓN DE RIESGOS, *UNE-EN ISO/IEC 27701. Técnicas de seguridad. Extensión de las Normas ISO/IEC 27001 e ISO/IEC 27002 para la gestión de privacidad de la información. Requisitos y directrices. (ISO/IEC 27701:2019)*, AENOR, Madrid 2021.

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (UNE). COMITE TÉCNICO CTN 307 GESTIÓN DE RIESGOS, *UNE-ISO 31000 Gestión del riesgo — Directrices*, AENOR, Madrid 2018.

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (UNE). COMITÉ TÉCNICO CTN-UNE 320 CIBERSEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES, *UNE-ISO/IEC 27001 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos*, AENOR, Madrid, 2023.

APDCAT, *Evaluación de impacto relativa a la protección de datos,* 2022, en https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Guia-EIPD.pdf

COMISIÓN EUROPEA, *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una estrategia europea de datos,* Bruselas 2020.

CNIL, *Privacy Impact Assessment (PIA). Application to IoT devices*, 2018, en https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-en.pdf

CNIL, *Privacy Impact Assessment (PIA). Knowledge bases*, 2018, en https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

CNIL, *Privacy Impact Assessment (PIA). Methodology*, 2018, en https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

CNIL, *Privacy Impact Assessment (PIA). Templates*, 2018, en https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA, *MAGERIT– versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método*, M. de Hacienda y Adm. Públicas, Madrid 2012.

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA, *MAGERIT– versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos*, M. de Hacienda y Adm. Públicas, Madrid 2012.

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA, *MAGERIT– versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnica*, M. de Hacienda y Adm. Públicas, Madrid 2012.

EUROPEAN DATA PROTECTION BOARD, *Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD*, 2021.

GRUPO «PROTECCIÓN DE DATOS» DEL ARTÍCULO 29, *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679 (WP 248 rev.01),* 2017.

GRUPO ESPECÍFICO DE CARÁCTER TEMPORAL AEN/GET13 GESTIÓN DE RIESGOS, *UNE-EN 31010. Gestión del Riesgo. Técnicas de Apreciación del Riesgo*, AENOR, Madrid, 2011.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). TECHNICAL COMMITTEE ISO/IEC JTC 1 «INFORMATION TECHNOLOGY, *UNE-EN ISO/IEC 29134:2020. Tecnología de la información. Técnicas de seguridad. Directrices para la evaluación del impacto de la privacidad (ISO/IEC 29134:2017) (Ratificada por la Asociación Española de Normalización en mayo de 2020)*, AENOR, Madrid 2020.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). TECHNICAL COMMITTEE ISO/IEC JTC 1 «INFORMATION TECHNOLOGY», SUBCOMMITTEE SC 27, INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION, *ISO/IEC 27005. Information, security, cybersecurity and privacy protection - Guidance on managing information security risks*, ISO/IEC, Vernier, 2022.