Cifrado, IoT y RGPD: tres desafíos de Ciberseguridad en 2018

Javier Alonso Lecuit | Miembro Grupo de Trabajo sobre Ciberpolítica del Real Instituto Elcano

Tema

La UE ha descartado regular el uso del cifrado, afronta nuevos retos de ciberseguridad con el Internet de las cosas (IoT) y su Reglamento general para la protección de datos personales (RGPD) va a entrar en vigor.

Resumen

La Comisión acaba de pronunciarse sobre el uso de técnicas de cifrado y otros mecanismos de anonimización mediante su *Cybersecurity Act* y la propuesta de Directiva *e-evidence* para el acceso de las autoridades policiales y judiciales a pruebas electrónicas. También ha reaccionado frente al reto que supone la proliferación de dispositivos IoT y plataformas entre máquinas (M2M) junto con su progresiva integración en *cloud* públicos, recogiendo las recomendaciones de la Agencia ENISA y de la Asociación de operadores móviles GSMA. Finalmente, en mayo de 2018 entrará en vigor el Reglamento para la protección del tratamiento de datos personales (RGPD), lo que representa un salto cualitativo en las exigencias sobre la seguridad y la gestión del riesgo de la información para corporaciones, pymes y administraciones públicas en aras de la salvaguarda del derecho fundamental de la privacidad de los ciudadanos. Este análisis estudia el contenido e implicaciones de estas iniciativas para las políticas de ciberseguridad de los Estados miembros de la UE.

Análisis[1]

En diciembre de 2016, el Consejo Europeo de Ministros de Interior y Justicia solicitó a la Comisión Europea que definiera una posición sobre el uso del cifrado y otros mecanismos de anonimización en el contexto de las investigaciones policiales y judiciales contra el crimen organizado y el terrorismo. El perímetro de análisis incluía el uso de cifrado en terminales de usuario y otros dispositivos TIC, estructuras de datos, espacios de almacenamiento en servidores, *cloud*, aplicaciones de comunicaciones y redes sociales (Skype, Whatsapp, Telegram, etc), páginas *online* o redes de comunicaciones, así como otros mecanismos de anonimización en la web profunda (*darknet*).

[1] Los contenidos de este ARI fueron anticipados en los CIBER Elcano 31, 32 y 33.

(cont.)

En su Comunicación de octubre de 2017,[2] la Comisión reafirmó su firme apoyo al uso de técnicas de cifrado robustas para asegurar la economía digital, en línea con el Reglamento General para la Protección de Datos de carácter personal (art. 32) y la opinión de ENISA[3] de diciembre 2016. Básicamente, la Comisión interpreta que el uso de cifrado en Europa deriva del derecho fundamental a la privacidad de las personas físicas y jurídicas, por lo que descarta legislar o limitar la aplicación de técnicas de cifrado, excluye legalizar puertas traseras a redes, aplicaciones y dispositivos y requiere a las autoridades que las medidas para el acceso a la información cifrada sean proporcionales, no afecten de forma indiscriminada a grandes grupos de usuarios, ni debiliten o pongan en riesgo la protección de una determinada red, servicio o dispositivo.

A partir de estas premisas, la Comisión propone varias medidas técnicas y operativas para reforzar las capacidades de las autoridades nacionales a neutralizar los mecanismos de cifrado utilizados por el crimen organizado y el terrorismo en el contexto de las investigaciones policiales y judiciales. Entre ellas, el *Europol European Cybercrime Centre* (EC3) ofrecerá apoyo técnico para el descifrado o la aplicación de técnicas alternativas que faciliten la información cifrada de los sujetos investigados, sin por ello exponer al conjunto de los usuarios del servicio afectado a riesgos añadidos. Fomentará el uso compartido de un conjunto de técnicas (*toolbox*) alternativas al descifrado, utilizadas para acceder a la información cifrada en el curso de las investigaciones, y la colaboración con la industria tecnológica y proveedores de comunicaciones y proveedores de Internet, en particular aquellos que han incorporado el cifrado en sus servicios o tienen capacidad para interceptar los datos o metadatos de las comunicaciones. En el ámbito policial y judicial creará una red de expertos y programas de formación al servicio de las fuerzas de seguridad y autoridades judiciales de los Estados en colaboración con el *European Cybercrime Training and Education Group* (ECTEG) y la Academia de Policía de la UE (CEPOL). Por último, el *European Judicial Cybercrime Centre* (EJCC), en colaboración con el EC3 y Eurojust, realizará un seguimiento de mejores prácticas y monitorizará los métodos de cifrado empleados por las organizaciones criminales y terroristas.

Estas medidas tácticas se verán complementadas en 2018 con el Plan de Ciberseguridad presentado en septiembre de 2017 al Parlamento y Consejo de Europa (*The Cybersecurity Act*) con propuestas tales como el anuncio de una Directiva para el acceso de las autoridades policiales y judiciales a pruebas digitales –en particular aquellas que se encuentren cifradas– (Directiva *e-evidence)* o diversas actuaciones encaminadas a fortalecer la cooperación transfronteriza entre las autoridades nacionales mediante la creación de una plataforma de comunicación o la armonización de los mecanismos para la cooperación judicial, entre otras.

En este contexto es significativo el creciente apremio de las autoridades comunitarias y nacionales sobre los principales proveedores de aplicaciones Internet (Apple, Google,

[2] "Eleventh progress report towards an effective and genuine Security Union", 18/X/2017, pp. 8-10, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf.

[3] "ENISA's Opinion Paper on Encryption", https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption/view.

Facebook o Microsoft, etc.) y los operadores de telecomunicaciones para la interceptación y entrega en claro de datos y metadatos de las comunicaciones, tanto desde el plano de la colaboración como en cumplimiento de nuevas obligaciones legislativas que se han incorporado en las leyes de seguridad nacional, por ejemplo del Reino Unido o Francia.

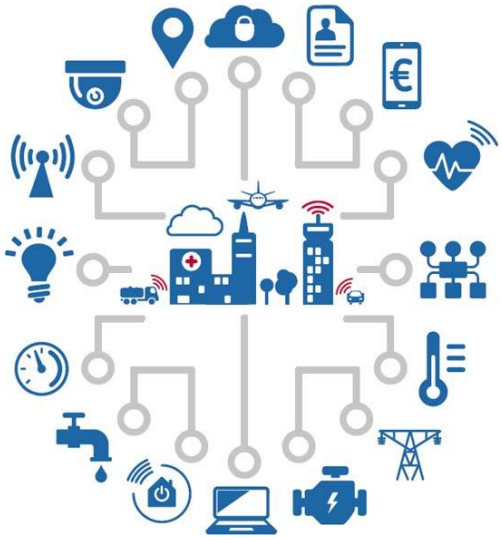
Sin embargo, las autoridades y la industria tecnológica se enfrentan a dificultades que son en ocasiones prácticamente insalvables en tiempo, forma y coste como claves sólo accesibles por el usuario final o prácticamente imposibles de descifrar aplicando los medios y plazos disponibles, así como limitaciones a la obligación de colaboración de los incriminados en aplicación del derecho de no incriminación reconocido en determinados países, entre otros.

En consecuencia, las autoridades debaten con el sector tecnológico alternativas tales como obligar a los proveedores de Internet a conocer y verificar la identidad del usuario si ofrecen aplicaciones cifradas o establecer la obligación a los usuarios y organizaciones titulares de los datos cifrados de facilitar el acceso a las autoridades. Estas alternativas desplazarían el actual foco de atención sobre el descifrado hacia nuevos ámbitos como, por ejemplo, la responsabilidad del proveedor de la aplicación de Internet en validar la identidad del usuario al tiempo de asegurar su privacidad y anonimato frente a terceros en la red. A pesar de las soluciones que se adopten, y aunque aumenten las obligaciones sobre la industria y mejoren las capacidades técnicas de interceptación de comunicaciones cifradas de uso masivo en Internet, será difícil evitar que la delincuencia organizada y las organizaciones terroristas utilicen aplicaciones de cifrado *end-to-end* específicas o mecanismos de anonimización avanzados.

El Internet de la Cosas (IoT)

El IoT es un paradigma con implicaciones técnicas, económicas y sociales en el que la adquisición de información alimenta un ciclo continuo de detección, procesado y ejecución de acciones. El IoT comprende un extenso ecosistema cibernético y físico de plataformas interconectadas donde los sensores toman, intercambian y procesan un gran volumen de datos del entorno, lo que permite una toma de decisiones autónoma adaptada dinámicamente al contexto.

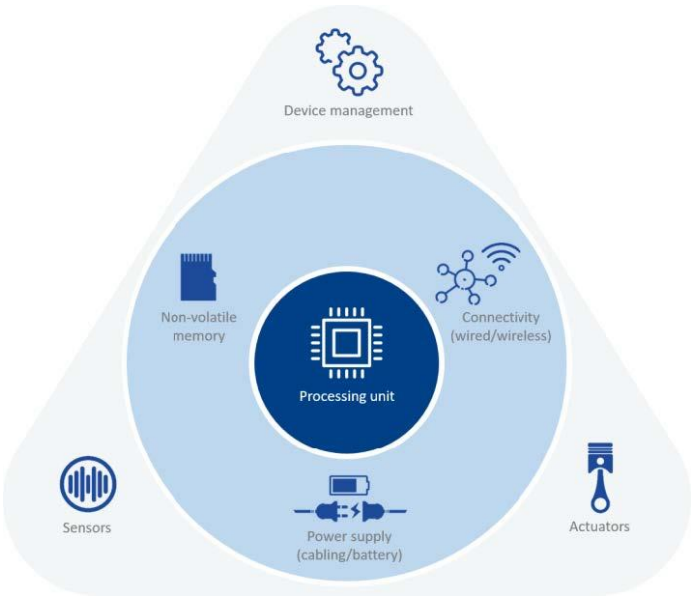
Figura 1. Ecosistema IoT



Fuente: ENISA.

En ocasiones, los términos IoT y M2M ("máquina a máquina") se han usado indistintamente. En origen, M2M hacía referencia a soluciones cerradas de uso industrial basadas en protocolos de comunicaciones entre máquinas, sensores y actuadores PLC (Programador Lógico Controlable). El IoT hacía referencia a aplicaciones abiertas del sector de consumo que utilizan sensores en dispositivos conectados por Internet (sensores para el control ambiental, elementos domóticos, cámaras de vigilancia, televisores, electrodomésticos, sistemas de videoconferencia, etc.). Actualmente, M2M menciona las aplicaciones verticales (por ejemplo, el vehículo conectado) formadas por sensores y actuadores dotados de inteligencia e interconectados mediante redes, entre ellas Internet. IoT refiere el sistema formado por la interconexión de distintas plataformas M2M de un determinado sector (industria, salud, automoción, transporte, etc.).

Figura 2. Estructura de un sistema IoT

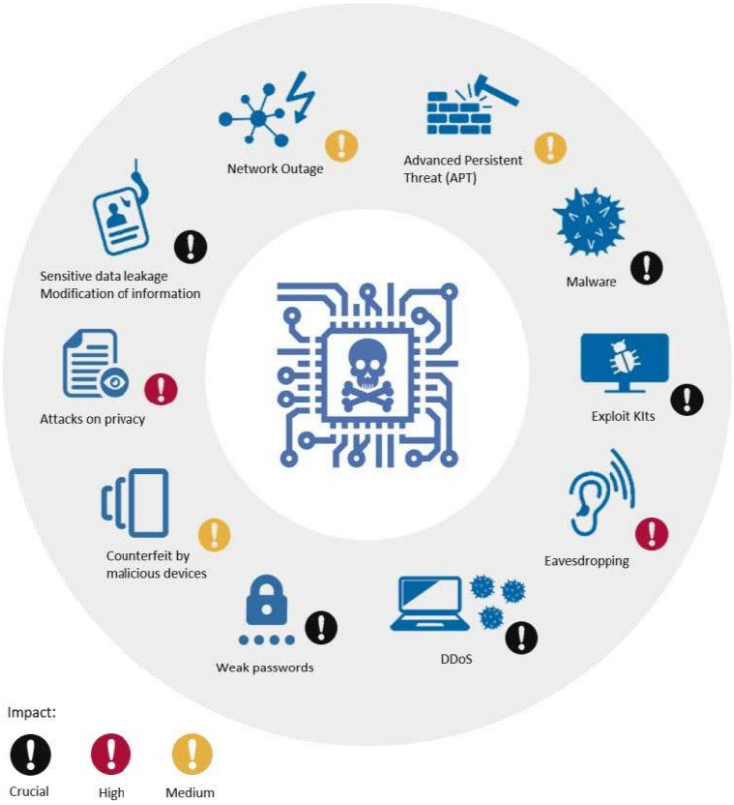


Fuente: ENISA.

El IoT experimenta un crecimiento explosivo (8.4 billones de elementos IoT conectados en 2017, 20 billones previstos en 2020) motivado por el papel que adquieren las plataformas IoT en la digitalización del sector de consumo (domótica), de los procesos de producción (Industria 4.0) e infraestructuras públicas (por ejemplo, *smartcities*). La adquisición, y análisis de grandes volúmenes de datos en tiempo real mediante algoritmos de inteligencia artificial (*Big Data)* dotan de inteligencia autónoma a los servicios y aplicaciones IoT, que son la base para la explotación comercial de los datos (*Data Economy*). Esta compleja dinámica plantea importantes retos debido a la actual fragmentación de los estándares, a la escala global de las plataformas y a la disparidad de requisitos exigidos por los distintos sectores (consumo, energía, transporte, medicina, industria, seguridad pública, entre otros).

La seguridad de las plataformas IoT frente a las ciberamenazas constituye un motivo de particular preocupación para proteger a los usuarios e infraestructuras que utilizan plataformas IoT de las ciberamenazas y evitar la ejecución de ataques hacia realizados a través de dispositivos IoT dirigidos hacia usuarios de Internet. Por otra parte, los objetivos y parámetros a considerar en la seguridad de los sistemas IoT no son conceptualmente distintos a los establecidos en otros servicios IT. Sin embargo, la escala y especificidades técnicas acrecientan considerablemente la superficie de exposición a ciberamenazas: son dispositivos a menudo de una limitada complejidad por su reducido coste y/o restringida disponibilidad de energía, con ciclos de vida muy largos, situados en emplazamientos muy dispersos y/o accesibles a terceros, y cuyo *firmware* es difícil de actualizar.

Figura 3. Amenazas de ciberseguridad de IoT



Fuente: ENISA.

Otros factores a tener en cuenta en la seguridad de IoT son los requisitos establecidos en las regulaciones sectoriales en las que cada plataforma opera, así como cuestiones legales y regulatorias vinculadas a la protección de la privacidad, los derechos de propiedad de la información, la transferencia internacional de datos o la responsabilidad y subsidiaridad legal de los agentes que intervienen en la cadena de provisión en un contexto global donde el uso masivo de datos, la inteligencia artificial o la deslocalización de las infraestructuras físicas y lógicas forman parte esencial de los servicios IoT.

Asimismo, debe tenerse en cuenta la seguridad en la conectividad IoT a través de redes de telecomunicaciones e Internet, siendo de obligada referencia en 2018 la evolución de éstas hacia la próxima generación móvil 5G, caracterizada por la integración de los servicios de telecomunicaciones móviles en plataformas de red IP virtualizadas (*Software Defined Networking-Network Functions Virtualisation*, SDN-NFV). Las redes 5G aportarán entre otras ventajas una densidad extrema de dispositivos finales interconectados junto con una gran flexibilidad en la provisión y gestión de cada tipo de servicio (ancho de banda, latencia, disponibilidad) así como una evolución del marco regulatorio. [4] Esta virtualización de las arquitecturas (*network slicing*) y de las plataformas de red mediante el uso de agrupaciones (*pools*) de servidores de propósito no específico en las redes de telecomunicaciones añaden nuevos retos de seguridad,

[4] http://berec.europa.eu/eng/document_register/subject_matter/berec/others/6088-input-paper-on-potential-regulatory-implications-of-software-defined-networking-and-network-functions-virtualisation.

de especial relevancia en aquellos ámbitos IoT que guarden una estrecha relación con la provisión de servicios esenciales e infraestructuras críticas.

Las predicciones de Forrester para 2018[5] señalan el salto de IoT a nivel comercial, caracterizado por la especialización de los dispositivos y plataformas (evolución facilitada por las economías de escala) junto a la externalización de las plataformas IoT actualmente implantadas en centros de datos privados hacia entornos de *cloud* públicos ofrecidos por grandes proveedores globales con el propósito de optimizar costes, agilizar el despliegue de servicios y ofrecer mayor escalabilidad de recursos. Forrester también señala que la necesidad de limitar la latencia en la respuesta al procesado del gran volumen de datos en tiempo real junto a la reducción de los costes de los sistemas llevará a descentralizar y dotar de inteligencia autónoma (*edge computing intelligence networks*) el procesado a los dispositivos en determinados sectores como por ejemplo la automoción. En consecuencia, subraya que los dispositivos y las plataformas IoT –en particular aquellas integradas en *cloud* público– serán el objetivo de ciberataques de alcance masivo, especialmente las aplicaciones IoT que formen parte de los servicios esenciales proporcionados por operadores de infraestructuras críticas y los ciberataques motivados por objetivos económicos.

Este complejo escenario ha disparado las alarmas de las autoridades en 2017 tal como refleja la Comisión Europea a través del *Cibersecurity Package*.[6] Por un lado, es necesario concienciar a todos los actores públicos y privados implicados, pero dado el crecimiento exponencial de las plataformas, será necesario recurrir en el futuro a sistemas de vigilancia y actuación basados en sistemas de inteligencia artificial autónomos. En respuesta, y durante 2018, la Comisión promoverá las recomendaciones de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) y de la asociación mundial de las telecomunicaciones móviles (GSMA) para mejorar la ciberseguridad de IoT en Europa.

En su informe *Baseline Security Recommendations for IoT*,[7] ENISA recomienda promover la armonización de directrices, iniciativas, estándares o regulaciones; concienciar a consumidores y empresas sobre los riesgos y medidas a adaptar, definir directrices de seguridad para el ciclo de vida de los desarrollos *software* (SSDLC) y *hardware*, acordar la soluciones interoperables válidas para la cadena de provisión del ecosistema IoT y promover incentivos administrativos y establecer responsabilidades entre los distintos agentes que intervienen en la cadena de valor de los productos y servicios IoT. Por su parte, las orientaciones de la GSMA, *GSMA IoT Security Guidelines*,[8] pretenden mejorar la seguridad y protección de la privacidad durante todo

[5] https://www.forbes.com/sites/gilpress/2017/11/09/10-predictions-for-the-internet-of-things-iot-in-2018/1/.

[6] http://www.consilium.europa.eu/en/policies/cyber-security/.

[7] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

[8] https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/.

(cont.)

el ciclo de vida de los ecosistemas IoT,[9] la explotación de dispositivos (*end points*) IoT[10] y en los servicios de telecomunicaciones móviles orientados a IoT.[11]

El Reglamento General para la Protección de Datos personales (RGPD)

El 25 de mayo de 2018 entrará en vigor del Reglamento de la UE para la protección de las personas físicas en el tratamiento de datos personales. Representa un salto cualitativo en las exigencias sobre la seguridad y la gestión del riesgo de la información para empresas y administraciones públicas en aras de la salvaguarda del derecho fundamental de la privacidad de los ciudadanos, así como en el progreso hacia un Mercado Único Digital, potenciando las oportunidades ofrecidas por la economía digital. El RGPD[12] será de aplicación a toda organización (controlador y/o procesador de datos) que ofrezca servicios a ciudadanos europeos, con independencia del emplazamiento de la empresa que realice procesado de los datos. Implicará cambios significativos en relación a la Ley orgánica para la Protección de Datos de Carácter Personal (LOPD).[13]

El RGPD se apoya en tres principios: el de responsabilidad (*accountability*), el de protección de datos por defecto y desde diseño (*privacy by design*) del producto o servicio y el de transparencia a los usuarios.[14] Establece nuevas obligaciones tales como la designación de un Delegado de Protección de Datos (DPO), la de evaluar el impacto de los riesgos, la de adoptar las medidas adecuadas para mitigarlos, la de designar un establecimiento principal a las empresas multinacionales que ofrecen sus servicios a ciudadanos europeos y la de comunicar las brechas de seguridad a las autoridades de control y, en casos graves, a los afectados, tan pronto sean conocidas, estableciéndose el plazo máximo de 72 horas.

El Reglamento no prescribe procedimientos o medios técnicos específicos para la protección de datos personales, por el contrario, establece un modelo de regulación basado en la gestión de riesgos.[15] Este enfoque supone que las compañías tendrán la flexibilidad de adoptar aquellas medidas técnicas y organizativas que consideren apropiadas para garantizar la integridad y confidencialidad de los datos de carácter personal y demostrar el cumplimiento de los principios establecidos en el Reglamento. El enfoque de riesgos habrá de evitar todo tratamiento no autorizado o ilícito de los datos de carácter personal, su pérdida, destrucción o daño accidental. Habida cuenta de la necesaria adaptación de estas medidas a lo largo del tiempo, las organizaciones tendrán que revisar la evolución tecnológica, los costes de aplicación de las medidas, la naturaleza, alcance, contexto y finalidades del tratamiento, así como la probabilidad y

[9] https://www.gsma.com/iot/iot-security-guidelines-for-iot-service-ecosystem/.

[10] https://www.gsma.com/iot/iot-security-guidelines-for-endpoint-ecosystem/.

[11] https://www.gsma.com/iot/iot-security-guidelines-for-network-operators/.

[12] https://www.boe.es/doue/2016/119/L00001-00088.pdf.

[13] https://www.boe.es/buscar/pdf/2008/BOE-A-2008-979-consolidado.pdf.

[14] ENISA ha publicado sendas guías para facilitar la implantación del principio de privacidad por diseño (https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design) a proveedores y a empresas de *Big Data* (https://www.enisa.europa.eu/publications/big-data-protection).

[15] https://www.agpd.es/blog/el-enfoque-de-riesgos-en-el-reglamento-general-de-proteccion-de-datos-ides-idPhp.php.

gravedad de los potenciales incidentes para los derechos y libertades de las personas. Las medidas de seguridad regladas en la LOPD pasaran a ser opcionales.

Para su adaptación al nuevo RGPD, las empresas tendrán que evaluar los riesgos que se derivan del tratamiento de los datos personales tales como la destrucción, pérdida o alteración accidental o ilícita de datos personales, la comunicación o el acceso no autorizados a dichos datos que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales junto a la evaluación de los riesgos tecnológicos concretos, las potenciales vulnerabilidades de los procesos y sistemas así como el impacto potencial sobre la integridad y disponibilidad de los datos.

En relación con los incidentes de seguridad –extravío, robo o acceso no autorizado a los datos de carácter personal– los controladores de los datos deberán detectar, registrar y decidir si procede comunicar el incidente a la autoridad de protección de datos, así como facilitar la información sobre el mismo ante la solicitud de la autoridad, para lo que precisan sistemas de detección, investigación, actuación y reporte internos confiables y ágiles.

Entre las medidas de seguridad aplicables se encuentran las que mejoran la privacidad (*Privacy-Enhancing Technologies*, PET)[16] como el cifrado y la (pseudo)anonimización,[17] teniendo en cuenta la difusa frontera que existe entre los datos de carácter personal anonimizados y aquellos cuya anonimización puede ser reversible (o pseudo-anonimizados) gracias a la evolución con la tecnología y la disponibilidad de información adicional. Otras medidas tienen que ver con las capacidades organizativas, tecnológicas y de inteligencia, las capacidades para restaurar la disponibilidad y acceso a datos tras un incidente o los procesos y tecnologías de monitorización para la verificación y valoración continua de la eficacia de las medidas (detectar brechas y demostrar el cumplimiento de la norma).

Las medidas de seguridad adoptadas por las organizaciones serán verificadas por la autoridad regulatoria cuando la organización notifique una brecha de seguridad o cuando esa brecha se detecte y notifique por terceros. El nuevo Reglamento aumenta notablemente la exposición de las organizaciones a elevadas sanciones y a daños reputacionales. En este sentido, la notificación de una brecha de seguridad (no siempre evitable incluso adoptando estrictas medidas de seguridad) puede exponer a la organización a sanciones en el curso de la investigación por incumplimientos o mala praxis a pesar de que no guarden relación directa con el incidente notificado. Las organizaciones tendrán que asegurarse por la vía contractual que las empresas subcontratadas cumplen el Reglamento y estar preparadas a responder ante las autoridades judiciales si se denuncia alguna brecha de seguridad ante ellas por los afectados.

[16] https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies.

[17] http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Orientaciones_y_garantias_Anonimizacion.pdf.

(cont.)

Para ayudar a su implantación, la Agencia Española de Protección de Datos ha elaborado varias guías y orientaciones dirigidas a profesionales, empresas y administraciones públicas,[18] así como una herramienta (FACILITA)[19] para las empresas y profesionales responsables o encargados de tratamientos que procesen datos personales de escaso riesgo. En el ámbito nacional, la aplicación del principio de gestión de riesgos en las administraciones públicas españolas tendrá en consideración los criterios establecidos para el tratamiento de los datos por el Esquema Nacional de Seguridad,[20] las metodologías de análisis de riesgos utilizadas por las Administraciones y las directrices establecidas por la Agencia de Protección de Datos (Orientaciones sobre el nuevo RGPD para Administraciones Públicas y para Entidades Locales).[21]

Conclusiones

El ciberespacio presenta nuevos desafíos para la ciberseguridad de la UE a medida que se generaliza el uso de la encriptación, se multiplican los dispositivos conectados o se extiende el tratamiento y almacenamiento masivo de datos de carácter personal de las personas físicas y jurídicas de la Unión. La Comisión trata de hacerles frente mediante regulaciones obligatorias y recomendaciones voluntarias que disminuyan los riesgos. Las medidas adoptadas no pueden garantizar la seguridad total pero la Comisión cumple con su objetivo de prevenir a los posibles afectados y buscar medidas que les ayuden a prevenir los riesgos. Todas esas medidas conllevan un proceso de ejecución del que se extraerán lecciones para mejorarlas, incluido el avance tecnológico que tiende a dejar obsoletas las medidas adoptadas.

En particular, la progresiva integración de los dispositivos y plataformas IoT en entornos de *cloud* públicos van a demandar la ágil respuesta de todos los actores involucrados en el desarrollo armonizado de la interoperatividad, los estándares y las certificaciones, aspectos esenciales para asegurar una evolución escalable y sostenible de IoT en el ámbito de la ciberseguridad.

Finalmente, el RGPD introduce un modelo de regulación basado en la gestión de riesgos, no en la prescripción de medidas concretas, que obliga a las empresas a demostrar su nivel de concienciación y de respuesta, evaluando el nivel de protección que prestan a sus ficheros de datos y el riesgo al que se exponen si no están a la altura de las exigencias del RGPD.

[18] http://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php.

[19] https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/herramientas_ayuda/index-ides-idphp.php.

[20] https://www.ccn-cert.cni.es/publico/ens/ens/index.html?n=6.html.

[21] http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Impacto_RGPD_en_AAPP.pdf.