INTRODUCCIÓN

En pocos años, la ciberseguridad ha pasado de ser un término desconocido para gran parte de la población a aparecer con creciente frecuencia en los medios de comunicación, tanto por la prevalencia y gravedad de los ciberataques que sufren nuestros sistemas y redes de ordenadores como por su alcance, que abarca desde organismos públicos y empresas a individuos.

Así, incidentes impensables hasta hace poco, como el cierre de grandes empresas por estos ataques (caso del infausto *WannaCry* del pasado año), la revelación de datos personales de 30 millones de personas de todos los países (caso de una empresa de citas en línea) o el robo de millones de credenciales de usuarios de varias de las mayores redes sociales se han convertido en noticias cotidianas y no han pasado, no han podido pasar, desapercibidas por la sociedad. Ello por no citar los ataques a infraestructuras críticas, que están haciendo crecer la preocupación por posibles disrupciones en la prestación de servicios esenciales críticos para la sociedad, como es el caso de la caída de las redes de transporte de energía eléctrica en un país europeo en diciembre de hace tres años.

Por ello, según señala el *Global Risks Report* 2018 del *World Economics Forum* de Davos, los riesgos asociados a la ciberseguridad ocupan la tercera posición en la clasificación de riesgos globales según su probabilidad de ocurrencia y la sexta atendiendo a su impacto. Por lo que respecta a la clasificación de los riesgos más preocupantes para los negocios, los ciberataques ocupan la octava posición, detrás del desempleo, crisis fiscales, energéticas, de instituciones financieras, etc.

No obstante, debemos ser muy cuidadosos de no exagerar estas amenazas y sus consiguientes riesgos, pues ello no podría sino lastrar el desarrollo y expansión de las tecnologías de la información y comunicaciones, que son el soporte de esta revolución de la información que estamos viviendo y están propiciando, por su profundidad y rápida expansión, un insólito avance de nuestras sociedades, que están alcanzando cotas de bienestar y desarrollo humano insólitas en la historia.

En su lugar, lo único procedente es acentuar los esfuerzos en concienciar y formar, sin alarmar, a la población e implementar en nuestros recursos informáticos y de telecomunicaciones las numerosas medidas de seguridad existentes, que abarcan desde las de naturaleza técnica a las de gestión, pasando por las físicas. Y, así mismo, instar a nuestros legisladores para que sigan aprobando medidas de carácter legal pertinentes para dificultar los ciberataques y obligar a los organismos públicos y a los sectores económicos más expuestos (los suministradores de servicios esenciales definidos en la Ley de protección de infraestructuras críticas) a adoptar todos los controles adecuados al estado de la tecnología para contrarrestar estos ciberriesgos.

Este monográfico de **Economía Industrial**, coordinado por el profesor **Arturo Ribagorda Garnacho** de la Universidad Carlos III de Madrid, pretende ilustrar a lo largo de 12 artículos enmarcados en cuatro bloques, la situación actual y las perspectivas futuras de la ciberseguridad, desde el punto de vista del sector empresarial y público, así como exponer los desarrollos legales recientes en la materia, todo ello precedido de una introducción al mercado y la situación laboral en nuestro país y una visión académica del tema.

El primer bloque comprende dos artículos que pretenden dar una visión global de la ciberseguridad desde distintos puntos de vista. En el primero de ellos, **Arturo Ribagorda Garnacho** tras definir con precisión el término ciberseguridad y repasar someramente el mercado laboral, presenta una visión académica de las causas de la inseguridad de las tecnologías de la información y las comunicaciones y sus vulnerabilidades, de las principales amenazas y riesgos para concluir exponiendo los diversos controles de seguridad: técnicos, físicos, de gestión y legales, enfatizando la importancia creciente de estos dos últimos. En el segundo de los artículos, **Luis Fernández Delgado** marca el contexto internacional de la ciberseguridad, para centrarse seguidamente en el mercado español, cuantificando sus cifras de negocio e ilustrando su pujanza con casos de éxito (empresas nacionales que se han abierto un hueco en el mercado internacional), para tratar finalmente el mercado español oferente y el papel del sector público en todo ello.

En el segundo bloque, cuatro autores tratan el tema desde una visión puramente empresarial. De este modo, **Ana I. Ayerbe Fernández-Cuesta** se detiene en el estudio de la Industria 4.0, repasando la evolución histórica de los sistemas de control industrial y resaltando que es a partir de la conectividad de los sistemas de control industrial a través de TCP/IP y su integración con las TI corporativos (es decir, del paso de protocolos de propietario a protocolos abiertos, y de equipos de propósito específico a generales), cuando se empiezan a producir los primeros ciberataques, muchos de ellos diseñados expresamente con este fin, para concluir exponiendo las vulnerabilidades más comunes a estos sistemas de control, los tipos de ataques, los impactos que producen y la necesidad de considerar la seguridad como un proceso y sus paradigmas de seguridad. A su vez, **Juan González Martínez**, muestra el valor de la innovación para enfrentarse a unos atacantes que están demostrando ser enormemente innovadores en sus tácticas y herramientas de ataque. Para ello, se apoya en las iniciativas europeas (programa marco Horizonte 2020 y *ECSO*, *European Cibersecurity Organization*) y nacionales (línea 6 de la Estrategia de ciberseguridad nacional, Plan de confianza en el ámbito digital), repasando seguidamente los problemas que tratan de resolver las líneas que concentran la I+D+i en ciberseguridad: anonimización de datos personales; biometría; criptografía postcuántica y homeomórfica; etc. Seguidamente, **Tomás Castro Alonso**, se centra en los *Digital Innovation Hub* (agrupaciones de empresas, asociaciones, centros de I+D+i, universidades y entidades públicas o privadas interesadas en la promoción del sector de las Tecnologías Avanzadas o emergentes, especialmente a la Ciberseguridad), como dinamizadores de la transformación digital de las empresas y su mano de obra, actuando como una "ventanilla única" para dar solución a los problemas del sector en el ámbito de la Ciberseguridad: la dificultad para captar y retener talento especializado en las empresas, el fomento de la I+D+i industrial, el trabajo en codesarrollo, la formación especializada o la tutela de emprendedores. Para concluir, **Roberto Baratta Martínez**, trata de la función de gobierno de la ciberseguridad, exponiendo las expectativas de esta función y como las organizaciones pueden y deben contemplarla y afrontarla en sus procesos internos, y especialmente como tenerla en cuenta en las decisiones corporativas donde la diligencia debida, la responsabilidad social y penal, la regulación y la operación y actividad financiera deben reflejarla. Para ello, expone cómo cada organización tendrá que desarrollar una estructura, una organización y unos medios específicos, a partir de los cuales la ciberseguridad pueda operar y cumplir sus misiones, tras lo cual establecer métricas de evaluación del desempeño e igualmente del riesgo y estimar la aportación de valor esperable de la ciberseguridad.

Un campo de tanta importancia como la ciberseguridad, debe estar soportado por políticas públicas que la impulsen, impongan normas y controles de obligado cumplimiento y supervisen su aplicación, así como por sistemas propios de gobierno, a todo lo cual se dedica el tercer bloque del monográfico de políticas públicas y gobernaza de la ciberseguridad. En este, **Alberto Hernández Moreno** a partir de la Estrategia de Ciberseguridad Nacional, pone el foco en el INCIBE (Centro de excelencia digital del Gobierno de España) para explicar sus objetivos, líneas y ámbitos de actuación y sus capacidades de prevención, concienciación, detección y respuesta frente a los ciberataques dirigidos a ciudadanos y empresas (que constituyen legalmente su ámbito de actuación), así como sus acciones para fortalecer, dinamizar e internacionalizar la industria nacional de ciberseguridad, dado que la ciberseguridad no sólo supone un reto a la seguridad nacional sino también una oportunidad para el desarrollo la economía española. Tras ello, **Fernando J. Sánchez Gómez**, examina los objetivos y funciones del Centro de Protección de las Infraestructuras Críticas y Ciberseguridad, órgano del Ministerio del Interior responsable de la protección de las citadas infraestructuras desde una doble perspectiva, la más tradicional, orientada a la protección de dichas infraestructuras y los servicios esenciales, que tiene un carácter integral y por tanto engloba tanto la seguridad física como la ciberseguridad entre sus objetivos. Y la segunda, más reciente, dedicada a la coordinación de los cometidos de ciberseguridad encomendados al Ministerio del Interior. Para estudiar esto último, se detiene en la Oficina de Coordinación Cibernética cuya misión es asegurar la coordinación técnica entre el Ministerio del Interior y sus organismos dependientes (por ejemplo, Guardia Civil y Policía Nacional) y el CERT de Seguridad e Industria y la cooperación con el sector privado de los operadores críticos. Por su parte, **Miguel Ángel Amutio Gómez** analiza con detenimiento el Esquema Nacional de Seguridad (ENS) de aplicación a todo el Sector Público y también de interés para las empresas proveedoras de servicios y soluciones tecnológicas a dicho sector, pues les es exigible el cumplimiento del ENS para demostrar la correspondiente conformidad. Se exponen el contexto, objetivos y condiciones establecidas en el Esquema y su impacto en las empresas proveedoras de servicios y soluciones al Sector Público, así como los seis principios básicos que orientan las decisiones en materia de seguridad y los 15 requisitos mínimos que permiten una protección adecuada de la información manejada y de los servicios prestados, sin olvidar el mecanismo de categorización que prevé la adopción de medidas de seguridad proporcionadas a la naturaleza de la información y los servicios a proteger, categorizando para ello los sistemas en Básicos; Medios y Altos. Por último, **Miguel García-Menéndez** reflexiona sobre la "fragilidad digital" que comporta el nuevo escenario digital, concluyendo en la necesidad de adoptar políticas públicas de ciberseguridad, materializadas frecuentemente en las denominadas "estrategias nacionales de ciberseguridad". El análisis comparado de las estrategias de 15 países analizados, refleja la doble vertiente de la regulación (estrategias nacionales de ciberseguridad) y la autorregulación (códigos de gobierno corporativo). En el primer caso, se atiende

especialmente a la presencia o ausencia en dichas estrategias de Normativas de protección de infraestructuras críticas y de Ciberseguridad industrial y, en el segundo, el "marco de cumplimento" o "marco de conformidad" del código de gobierno corporativo.

El último de los bloques del monográfico está consagrado a los aspectos legales y regulatorios, donde **Antonio Troncoso Reigada** estudia el Reglamento General de Protección de Datos (RGPD) y el proyecto (en el momento de redacción del artículo) de Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales, destacando el cambio de paradigma del principio de seguridad de los tratamientos de datos personales, que en nuestro ordenamiento jurídico se vinculaba al cumplimiento de unas concretas medidas de seguridad aprobadas en una norma administrativa (Reglamento de desarrollo de la LOPD), para pasar a ser el principio de responsabilidad proactiva el que guíe las actuaciones para proteger los datos personales. Igualmente analiza los dos ámbitos de la seguridad que contempla la RGPD: como principio del tratamiento y como obligación del responsable y del encargado. Respecto de esto último se detiene en las obligaciones del responsable respecto del principio de seguridad: la "Seguridad el tratamiento"; la "Notificación de una violación de la seguridad de los datos personales a la autoridad de control" y la "Comunicación de una violación de la seguridad de los datos personales al interesado". En este mismo bloque, **Francisco Lázaro Anguís** aborda el complejo reto que comporta para las empresas y organismos públicos compaginar eficaz y eficientemente las obligaciones impuestas por la ya abundante legislación acerca de la ciberseguridad. Con este fin, estas entidades deben armonizar en su estrategia y por tanto en su Política, esas obligaciones: los análisis de riesgo, las auditorías, los roles de responsabilidad, la gestión de incidentes de seguridad y la notificación de incidentes graves a las diferentes autoridades de control, entre otras cuestiones. Si bien no todas las empresas deben cumplir toda la legislación al respecto, el autor se centra en un caso concreto: una empresa que deba cumplir con el RGPD, el ENS, la Ley de Protección de infraestructuras críticas (PIC) y Real Decreto-ley de seguridad de las redes y sistemas de información (que traspone la Directiva NIS).