Oficina de Ciencia y
Tecnología del Congreso
de los Diputados

Ciberseguridad

España en un ecosistema tecnológico y social en constante evolución

La ciberseguridad se ha convertido en una necesidad social ya que se trata de una cuestión que trasciende el ámbito tecnológico. Desde la economía o la seguridad nacional hasta la defensa de los derechos fundamentales y las libertades públicas se ponen en juego en el ciberespacio. Además de la tecnología, la ciberseguridad incluye a las personas, los procesos que las conectan y su gobernanza, así como a los datos que se generan, comparten y almacenan. España ha desarrollado importantes capacidades en ciberseguridad. No obstante, la constante evolución de la tecnología y las amenazas conducen a importantes desafíos en torno a la capacitación y colaboración en el tejido nacional, el acceso igualitario a la ciberseguridad y la gestión de la disrupción asociada a tecnologías emergentes como la inteligencia artificial o la computación cuántica.

La ciberseguridad es necesaria para garantizar el desarrollo económico y social de España y defender la libertad y los derechos fundamentales de la ciudadanía.

La ciberseguridad debe ser considerada por diseño y por defecto en los ámbitos tecnológicos, en los productos, servicios digitales y en los procesos de las empresas y la administración pública.

El marco estratégico y de gobernanza de la UE ahonda en el desarrollo de un contexto normativo y operativo que consolide la ciberseguridad dentro y fuera de nuestras fronteras.

El fortalecimiento de la ciberseguridad en España se encuentra directamente vinculado al fomento de la colaboración dentro y entre los sectores académico, público y privado, el desarrollo de mecanismos de atracción, retención y creación de talento y el incremento de la financiación.

El factor humano es esencial. La ciudadanía y el personal de pymes y grandes empresas se sitúan en el centro de la ciberseguridad por lo que la concienciación, formación y capacitación son determinantes en la construcción de una sociedad ciberresiliente.

La investigación es esencial para anticipar la constante evolución de las ciberamenzas y guiar una implantación efectiva de las tecnologías disruptivas.

Método de elaboración

Los Informes C son documentos breves sobre los temas seleccionados por la Mesa del Congreso que contextualizan y resumen la evidencia científica disponible para el tema de análisis. Además, recogen las áreas de consenso, disenso, las incógnitas y los debates en curso. El proceso de elaboración de los informes se basa en una exhaustiva revisión bibliográfica que se complementa con entrevistas a personas expertas en la materia y dos rondas de revisión posterior por su parte.

Para la elaboración de este informe la Oficina C ha referenciado 402 documentos y consultado a un total de 31 personas expertas en la materia. Se trata de un conjunto multidisciplinar del cual el 58 % pertenecen al área de ciencias físicas e ingeniería (informática, ingeniería informática, ingeniería de las telecomunicaciones, físicas y matemáticas) y el 42 % a las ciencias sociales (filosofía, economía, ciencias jurídicas y sociología). El 63 % trabaja en centros o instituciones españolas mientras que el 37 % presentan al menos una afiliación extranjera.

La Oficina C es la responsable editorial de este informe.

Personal investigador, científico y experto consultado* (por orden alfabético)

Alaiz-Moretón, Héctor[1]. Profesor Titular de la Universidad de León.

Alcaraz, Cristina[1]. Profesora Titular de la Universidad de Málaga.

Arroyo Guardeño, David[1]. Científico Titular del Instituto de Tecnologías Físicas y de la Información "Leonardo Torres Quevedo", Consejo Superior de Investigaciones Científicas.

Barrio, Félix. Director General del Instituto Nacional de Ciberseguridad (INCIBE).

Beltrán, Marta[1]. Profesora Titular de la Universidad Rey Juan Carlos.

Caballero-Gil, Pino[1]. Catedrática de la Universidad de La Laguna. Miembro del grupo de trabajo Cultura de la Ciberseguridad, Foro Nacional de Ciberseguridad.

Candau, Javier[1]. Jefe del Departamento de Ciberseguridad, Centro Criptológico Nacional (CCN).

D'Antonio, Gianluca. Presidente de la Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum). Socio del Área de Riesgos Tecnológicos, Deloitte Risk Advisory.

Degli-Esposti, Sara[1]. Investigadora Científica del Instituto de Filosofía, Consejo Superior de Investigaciones Científicas,. Investigadora Honoraria de la Universidad de Coventry. Reino Unido.

Del Real, Cristina[1]. Profesora Adjunta de la Universidad de Leiden. Países Bajos.

de Fuentes, José María[1]. Profesor Titular de la Universidad Carlos III de Madrid.

Domingo-Ferrer, Josep[1]. Catedrático de la Universidad Rovira i Virgili. Director del Centro de Investigación en Ciberseguridad de Catalunya (CYBERCAT).

Esteve-González, Patricia[1]. Investigadora Asociada de la Universidad de Oxford. Reino Unido.

Tapiador, Juan[1]. Catedrático de la Universidad Carlos III de Madrid.

Fernández, Verónica[1]. Científica Titular del Instituto de Tecnologías Físicas y de la Información "Leonardo Torres Quevedo", Consejo Superior de Investigaciones Científicas.

Gañán, Carlos H[1]. Profesor Adjunto de la Universidad Técnica de Delft. Países Bajos.

Garcia-Alfaro, Joaquín[1]. Catedrático del Télécom SudParis-Institute Polytechnique de Paris, Francia. Research Fellow de la Universidad Carleton, Canadá. Investigador Distinguido de la Universitat Politècnica de Catalunya.

Gayoso Martínez, Víctor[1]. Profesor del Centro Universitario de Tecnología y Arte Digital (U-tad).

González Fuster, Gloria[1]. Profesora de Investigación de la Universidad de Vrije-Bruselas. Bélgica.

Hernández-Ramos, Jose L[1]. Oficial para Proyectos Científicos del Centro Común de Investigación (JRC) de la Comisión Europea. Italia.

Kavanagh, Camino[1]. Investigadora en el King's College, Reino Unido. Asesora independiente en materia de ciberseguridad y TIC en la Organización de la Naciones Unidas.

Lecuit, Javier A[1]. Investigador Senior del Real Instituto Elcano. Miembro del Comité de Expertos Independientes del Foro Nacional de Ciberseguridad en el grupo de trabajo de Regulación.

Lopez, Javier[1]. Catedrático de la Universidad de Málaga. Presidente de la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC).

López, M. Mar[1]. Vicepresidenta del Capitulo Español (women4cyver Spain) de la Fundación sin ánimo de lucro women4cyber, lanzada por la Organización Europea de Ciberseguridad (ECSO). Responsable de Seguridad para Sector Público y Sanidad España, Portugal e Israel y del Advanced Technology Center Málaga en Accenture.

Massacci, Fabio. Catedrático de la Universidad de Vrije. Países Bajos. Profesor de la Universidad de Trento. Italia.

Moret Millás, Vicente[1]. Letrado de las Cortes Generales. Comisión de Defensa. Miembro del Foro Nacional de Ciberseguridad. Of Counsel en Andersen.

Pastrana, Sergio[1]. Profesor Titular de la Universidad Carlos III de Madrid.

Pérez Pajuelo, Jose Luis. Director del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC).

Rifà-Pous, Helena[1]. Profesora Titular de la Universitat Oberta de Catalunya.

Skarmeta, Antonio F[1]. Catedrático de la Universidad de Murcia.

Zurutuza, Urko[1]. Profesor Titular en la Mondragon Unibertsitatea.

** El personal experto no ha declarado tener conflicto de intereses.*
[1] Especialistas que también han participado en la revisión completa o parcial del informe.

Ciberseguridad

14 noviembre 2022

Ver el resumen gráfico del informe en nuestra página web

**esta nota no aborda el tema de la desinformación ni ahonda en algunas cuestiones como los vehículos autónomos o la lucha contra el cibercrimen.*

Introducción

El mundo digital es uno de los pilares del desarrollo económico y social[1]. Desde la industria y los servicios públicos y privados hasta las comunicaciones, todos tienen un componente digital[2]. Si bien trae consigo grandes oportunidades, abre la puerta a importantes amenazas que suponen un reto global[1,3,4]. Un uso inapropiado de la tecnología pone en juego los derechos fundamentales y las libertades públicas en el ciberespacio[5].

Vulnerabilidad: una debilidad o error en un sistema informático que puede ser aprovechada por una amenaza y, por tanto, ser explotada por un atacante. Aunque las debidas directamente a la tecnología puedan mitigarse por medio de actualizaciones, no siempre es posible corregirlas. Mientras no se subsanan, pueden ser potenciales objetivos de ciberataques.

Hoy en día, las tecnologías de la información y la comunicación (TIC) y las infraestructuras que sustentan las actividades que se desarrollan en el ciberespacio son fundamentales en la sociedad[6,7]. Al mismo tiempo, las ciberamenazas explotan **vulnerabilidades** que pueden estar vinculadas a la propia tecnología que conforma los sistemas y redes de comunicación (por diseño, despliegue, configuración, administración o uso), pero también a factores humanos como el desconocimiento o de carácter organizativo[3,8–10].

No existe una definición universalmente aceptada de ciberseguridad[11–13], un concepto que abarca a todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas[4]. Incluye, además, a la propia información y los datos. Se trata de una disciplina transversal que engloba a su vez diversas disciplinas, sectores, tecnologías y herramientas[1,11,14]. Para España, se trata de un objetivo estratégico y prioritario[6,15] y es una cuestión de Seguridad Nacional[6].

Solo en 2021, en España se han recibido y gestionado centenares de miles de ciberincidentes[10,16,17], lo que también da cuenta de la capacidad para la detección de ataques del sistema español[18]. Se calcula que en torno al 28 % de la población ha experimentado algún incidente de ciberseguridad[19]. El coste global estimado del cibercrimen (o ciberdelitos) supera el atribuido al tráfico de drogas a escala global[1], aunque dada la dificultad en su cuantificación, las cifras son aproximadas[20,21]. El Plan Nacional de Ciberseguridad (2022-2025) ha sido dotado con algo más de 1.000 millones de euros[15] y el creciente mercado de la ciberseguridad se estima que alcance los 2.000 millones en 2024 a nivel nacional[22].

Tecnología y sociedades resilientes

La tecnología y los protocolos asociados a Internet no son 100 % seguros. Se basan en una estrategia de desarrollo continuo que deja puertas abiertas a posibles ciberamenazas[23]. A ello, se suma la comercialización de la tecnología que, de forma generalizada, no ha priorizado la ciberseguridad en su desarrollo ni en su propuesta de valor[4].

Ciberresiliencia: la habilidad de prepararse, absorber, recuperarse y adaptarse a los efectos adversos de los ciberataques. Con ella se pretende la continuidad de la actividad económica y social de forma que, a pesar de un ciberataque, se mantenga el funcionamiento normal o parcial de los sistemas, servicios, industria, etc.

El resultado es que no es posible evitar todos los ataques y por ello, se impone el concepto de **ciberresiliencia**[1,23–25]. Este objetivo requiere de una aproximación transversal que refuerce las principales capas que conforman la ciberseguridad: la tecnológica, la humana y los procesos que las conectan. La sociedad digital incluye infraestructuras, servicios, industria, administraciones públicas, hogares, personas, etc. Esta complejidad hace necesario que las salvaguardas tecnológicas estén coordinadas e integradas en una capa organizativa (gobernanza)[1,26,27]. En este sentido, el bienestar social requiere de un marco estratégico, jurídico y normativo que considere los avances tecnológicos atendiendo a su evolución y transversalidad. Asimismo, ha de integrar aspectos relacionados con las personas como la formación o la ética, además de la confianza entre los diferentes actores.

El complejo y cambiante ecosistema de la ciberseguridad

La constante y rápida evolución tecnológica puede hacer que muchos mecanismos de respuesta, como los legislativos, queden obsoletos, incluso antes de su implementación[28,29]. La ciberseguridad se desarrolla en un escenario digital, el ciberespacio, en el que un gran número de tecnologías interaccionan en un complejo engranaje junto a distintos actores, cuyas acciones tienen un importante impacto en la sociedad[1].

Sociedad digital dependiente de las TIC

La dependencia general de las TIC aumentó con la crisis de la COVID-19, principalmente, debido a la generalización del teletrabajo y la fuerte digitalización experimentada por las administraciones públicas[10]. Este cambio conllevó un marcado aumento del número de ciberataques, fenómeno que ha recibido la denominación de ciberpandemia[1,10]. Por otro lado, también ha supuesto una aceleración del desarrollo digital español, algo que se puede valorar positivamente[30,31].

La sociedad avanza hacia un nivel de interconexión y globalización creciente: las fronteras geográficas se desvanecen en el ciberespacio, lo que ocasiona importantes retos jurisdiccionales[32,33]. Hoy en día, desde objetos cotidianos, como relojes o electrodomésticos, hasta servicios esenciales o infraestructuras críticas, como la red eléctrica, son susceptibles de estar conectados a internet y a otros dispositivos. Por ello, son capaces de generar y transmitir datos (datificación)[1]. Surge así el concepto de servicios inteligentes, como el del transporte, el sistema de salud o los suministros eléctricos o de agua, entre otros muchos. Estos persiguen beneficiar al conjunto de la sociedad, adaptándose a la realidad de los usuarios (datos de consumo, preferencias personalizadas, etc.) u otros parámetros de interés (eficiencia, sostenibilidad, seguridad, etc.)[34,35]. Por tanto, la ciudadanía debe estar situada en el centro de los servicios digitales y la generación y transmisión de información[1].

La digitalización afecta de forma transversal a los Estados: defensa, infraestructuras digitales, transporte, finanzas, salud, energía, administraciones públicas y un largo etcétera[11]. Son de especial relevancia las infraestructuras críticas y las cadenas de suministro, ya que ofrecen servicios esenciales para la sociedad[36–38] (**Cuadro 1**). Los ataques informáticos que sufren pueden tener graves consecuencias, por lo que se consideran un riesgo global[39]. Existe abundante evidencia sobre cómo mejorar su ciberseguridad[40–42]. Buena parte de los avances se centran en la mejora de su ciberresiliencia[1,43], entendida como la existencia de un plan de prevención, respuesta y recuperación que permita la mitigación de los ataques y la restauración completa tras ellos, en el menor tiempo posible, manteniendo la continuidad de los servicios[43].

Cuadro 1. Servicios esenciales[44]: Infraestructuras críticas (IC), industria 4.0 y cadenas de suministro

En España las IC se agrupan en torno a 12 sectores[38] (de más a menos atacados en 2021)[45]: energía, tributario y financiero, agua, transporte, TIC, químico, nuclear, espacio, alimentación, administración pública, salud e investigación.

Buena parte de las IC y la industria se basan hoy en día en sistemas ciberfísicos abiertos, interconectados y fundamentados en un modelo de producción globalizado. A los sistemas de información y redes de operaciones para la producción industrial (OT, por sus siglas en inglés) que interconectan los distintos elementos de producción en planta (sensores, controladores, reguladores, etc.) se suman los sistemas de información corporativos (IT, por sus siglas en inglés) de una industria[46]. Sobre esta arquitectura de información tradicional la industria actualmente evoluciona hacia un nuevo modelo de producción que se apoya en el uso intensivo de los nuevos habilitadores tecnológicos (como el *Big Data*, internet de las cosas y computación en la nube entre otros, ver sección "El engranaje tecnológico del ciberespacio actual") planteando nuevos retos de ciberseguridad[46]. Es la llamada industria 4.0, más vulnerable a los ciberataques[37,47–49] y los desafíos de la ciberseguridad[36,37,40,42,50,51]. De hecho, el número de ciberataques a las IC crece en España (2022)[16]. Por otro lado, las cadenas de suministro, en las que participan habitualmente distintos tipos de empresas con un nivel de ciberseguridad muy heterogéneo, conforman un canal vulnerable a los ciberataques cada vez más explotado y esencial para el normal funcionamiento no solo de las IC sino de la economía[52,53]. En ciberseguridad estas incluyen un amplio abanico de recursos (*hardware* y *software*; como chips o programas de gestión, entre otros), computación y almacenamiento externalizado (en nube) y mecanismos de distribución y gestión (aplicaciones *web*, tiendas *online*)[52]. A escala internacional, destacan ataques a IC como el de *Colonial Pipelines* en EE.UU, que afectó al abastecimiento de gasolina e incluso a su precio en ese país[54]. De igual manera, el reciente ataque a SolarWinds es buena prueba de la relevancia de la ciberseguridad en las cadenas de suministro[55].

Es necesario abordar la gestión integral de la ciberseguridad industrial desde los distintos ángulos operativos, legales e institucionales[46]. Desde la UE se plantea la necesidad de avanzar en la identificación de potenciales vulnerabilidades y la revisión de los mecanismos legales y de gobernanza, además de los tecnológicos[37]. Parte del personal señala la necesidad de recurrir a las guías técnicas, estándares y metodologías ofrecidas por los organismos de normalización y autoridades en materia de ciberseguridad industrial[46].

El engranaje tecnológico del ciberespacio actual

Las TIC actuales se basan, en gran medida, en sistemas distribuidos, compuestos por un gran número de dispositivos interconectados entre sí y a la red. Conviene recordar que el 95 % de los hogares españoles tiene acceso a Internet[56] a través de dispositivos portátiles y personales (móviles, ordenadores, tabletas, etc.). Además, cabe citar el Internet de las cosas (IoT, por sus siglas en inglés), que comprende un extenso ecosistema cibernético y físico de plataformas interconectadas (millones de dispositivos[57]) donde distintos tipos de sensores toman, intercambian y procesan un gran volumen de datos del entorno. Esto permite que los dispositivos tomen decisiones autónomas adaptadas dinámicamente al contexto[58].

El IoT conecta el mundo digital y físico, creando ecosistemas inteligentes y ofreciendo soluciones innovadoras en todos los ámbitos[59]. Se encuentran en los hogares (electrodomésticos, dispositivos inteligentes, etc.), los espacios públicos (infraestructuras inteligentes de ciudades, transportes, etc.), la industria 4.0 (**Cuadro 1**; el llamado IoT industrial) o, incluso, en el cuerpo humano (dispositivos médicos y de control de salud)[60–64]. Para poder sustentar el complejo engranaje de sistemas interconectados y gestionar el flujo de datos masivo que caracteriza el ciberespacio es necesario el despliegue de redes públicas avanzadas, como lo es la **5G**[65].

5G: hace referencia a la 5ª generación de la tecnología usada en comunicaciones móviles (evolución directa del 4G). Entre otras mejoras, permite una mayor capacidad y diferenciación en la gestión de usuarios, velocidad de transmisión y una muy baja latencia (tiempo de respuesta).

Servicio de computación en nube: servicio digital basado en un modelo de pago por uso que hace posible el acceso a un conjunto modulable y elástico de recursos de computación (entre otros, licencias de software, capacidad de procesado y memoria, almacenamiento) que se pueden compartir.

Del almacenamiento y gestión de la gran cantidad de información que se genera se encargan sistemas de computación externos, con menos constricciones de capacidad que los terminales clásicos, como los **servicios de computación en la nube**[1,34,66]. Existe una gran dependencia global respecto a la misma, lo que hace de su seguridad una cuestión crítica[67]. A pesar de que el despliegue 5G avanza con retraso respecto a las previsiones en la UE[68], en la actualidad, una parte del esfuerzo científico[69], tanto a nivel europeo[70] como nacional[71], ya mira hacia la siguiente generación de redes de comunicación 6G.

Todo lo señalado con anterioridad hace que la superficie de ataque (posibilidades y puntos de ataque) aumente constantemente y que los mecanismos clásicos basados en el control aislado de los sistemas (seguridad perimetral) sean insuficientes[1]. Además, cada día se generan grandes cantidades de datos susceptibles de ser compartidos, consumidos, vendidos y almacenados en cualquier lugar del mundo por empresas o instituciones públicas: es la llamada sociedad de los datos masivos[72,73] (*Big Data* en inglés). Supone una importante actividad económica[74] y su rápido crecimiento ha puesto de relieve que su seguridad, privacidad y control son, en muchos casos, insuficientes[75–77].

Amenazas y actores

El número, variedad, sofisticación y peligrosidad de los ataques (**Cuadro 2**) no dejan de crecer en Europa y España[10,16,78,79]. Los cibercriminales ya no necesitan conocimientos informáticos avanzados: los ataques se han industrializado y automatizado y el cibercrimen aumenta rápidamente hacia modelos de negocio como servicio bajo demanda[79,80]. Basta tener acceso a Internet para poder promover un ataque de denegación de servicio (**Cuadro 2**) por algo más de 5 euros[1]. Motivos como perder una partida en un videojuego o evitar hacer un examen pueden motivar hoy en día un ciberataque[81,82]. En España, la cibercriminalidad ha representado alrededor del 16 % del total de las actividades delictivas a escala nacional en 2020[16,45] y 2021. Resulta esencial establecer medidas legislativas que promuevan y faciliten su persecución para reforzar las garantías respecto a los derechos de la ciudadanía[6].

Cuadro 2. Algunos métodos y tipos comunes de ciberataques

Normalmente los ciberataques tratan de explotar una vulnerabilidad en un sistema, un fallo de configuración, así como la falta de precaución o una decisión errónea por parte de los usuarios o, comúnmente, una mezcla de todos ellos[83]. A pesar de su gran diversidad muchos se dan de forma combinada o son complementarios.

Ataques de denegación de servicio: Son uno de los tipos de ataques más comunes, concretamente el ataque distribuido de denegación de servicios (DDoS, por sus siglas en inglés). Se sobrecarga el tráfico de Internet (p. ej. mediante peticiones de información o *emails*) hacia un sistema, aplicación o máquina, impidiendo su normal funcionamiento[40]. Como método, pueden ser originados a través de *botnets*, una red de ordenadores o dispositivos (IoT por ejemplo) conectados a Internet (*bots*) controlados remotamente por un atacante[84]. Otros usos maliciosos comunes de las *botnets* son el envío masivo de *spam*, o el minado de criptomonedas. En España en 2021 se hicieron más de 44.000 notificaciones a ciudadanos desde el sistema Antibotnet[17].

***Ransomware* o secuestro de datos:** uno de los más preocupantes en los últimos años[10]. Es un método de ataque basado normalmente en un tipo de programa malicioso (*malware*) que bloquea el acceso al sistema o a los datos a través de su cifrado hasta que se paga un rescate, lo que se recomienda no hacer[85]. Cada vez son más sofisticados (*ransomware* controlado por personas) y es común la doble extorsión (un pago adicional para evitar publicar los datos)[10].

Ataques a sistemas de acceso remotos: método de ataque cada vez más común[10] promovido por el teletrabajo.

Phishing: ataque basado en la manipulación mediante ingeniería social (suplantación de una entidad legítima y otras) a través del correo electrónico u otros sistemas de mensajería, para robar información privada, hacer algún tipo de cargo o infectar el dispositivo. Para ello, típicamente se envían correos electrónicos (*spam*) en el que se adjuntan archivos infectados o enlaces a páginas fraudulentas[86]. Se ha sofisticado con el *phishing* corporativo (como el fraude del CEO, entre otros)[10].

Ataques *web*: método de ataque basado en la utilización malintencionada o fraudulenta de páginas *web*. Por ejemplo, la suplantación de sitios *web* o aplicaciones o modificación de los auténticos para permitir la instalación de programas maliciosos entre otros muchos[40].

Amenazas persistentes avanzadas (APT, por sus siglas en inglés): se trata de una metodología de ataque creada y definida específicamente para atacar a una empresa o gobierno concretos con un objetivo definido. Para ello, se utilizan técnicas de ciberataque e infiltración continuas, clandestinas y avanzadas para acceder a un sistema y permanecer oculto durante un notable periodo de tiempo, conocerlo en detalle, adquirir privilegios del sistema y eliminar evidencias con el fin de extraer información (ciberespionaje) o con propósitos potencialmente destructivos[87]. Puede incluir algunos de los tipos de ataques mencionados. Las APT son cada vez más comunes en España, y es el tipo de ataque más sofisticado y temido[10], especialmente en las infraestructuras críticas[41,88].

La actividad delictiva en el ciberespacio que afecta a las personas físicas y jurídicas es muy amplia e incluye delitos tradicionales, pero desarrollados a través de las TIC, así como otros nuevos dependientes de estas[89]. Entre los primeros, destaca el fraude, en aumento en el contexto europeo[90], y la distribución de contenido ilegal (pornografía infantil, etc.). En España, se estima que en torno al 70 % de los internautas ha estado expuesto a una situación de fraude en 2021[7], siendo junto con el *malware* el tipo de amenaza que más afecta a la ciudadanía y al sector privado[17].

Aunque existe una taxonomía consolidada legalmente para clasificar los tipos de ciberincidentes[91], la clasificación de los agentes que las perpetran carece de límites definidos[89]. La motivación de los actores suele usarse como criterio para su clasificación[1]. No son categorías estancas ya que las motivaciones pueden variar o entremezclarse entre grupos[92]. El grupo más común y considerado más activo es el cibercrimen[1], que persigue, esencialmente, lucro económico. Está compuesto por un amplio espectro de actores que abarca desde estructuras profesionalizadas muy bien capacitadas, similares al crimen organizado, hasta individuos aislados.

Hacking: El origen del término *hacker* no está relacionado con actividades de cibercrimen y su vinculación se debe a un uso inapropiado del término. Un *hacker* es simplemente alguien capaz de manejar con gran habilidad cualquier sistema (aparato, dispositivo - no necesariamente un ordenador), con el fin de sacarle más partido o divertirse. El término hacking desde la perspectiva del Hacktivismo puede entenderse como la actividad que involucra la manipulación de la conducta normal de un equipo y sus sistemas. Analiza la seguridad y las vulnerabilidades de los sistemas informáticos. Sus objetivos pueden ser fortalecer la seguridad o aprovechar las brechas de seguridad o vulnerabilidades de los sistemas maliciosamente.

El resto de las categorías pueden ser menos comunes, pero pueden llegar a impactar igual o de forma más severa que el cibercrimen. Los actores-Estado pueden ser agencias estatales o grupos que actúan con el apoyo o bajo el control de Estados, normalmente con una alta capacitación y recursos. Sus actuaciones están alineadas con los intereses geopolíticos, económicos y estratégicos del país "patrocinador"[1]. Parte de su actividad puede vincularse con el ciberespionaje, con carácter económico, industrial, político u otros[1,92,93,93,94], lo que constituye una seria amenaza al desarrollo económico y a la defensa nacional[95]. Otras categorías destacables son las actividades de los grupos **hacktivistas**, los actores internos o *insiders* (por suplantación o decisión propia) o el ciberterrorismo. El primero está motivado por movimientos sociales[1], aunque recientemente se ha señalado un creciente interés económico de carácter individualista y vandálico[92].

También merece atención un amplio abanico de actores oportunistas con baja preparación (llamados *script kiddies*) que desarrollan actividades ilícitas que afectan negativamente a terceros y pueden evolucionar hacia perfiles criminales[1,96]. En general, se apoyan o desarrollan en torno a foros clandestinos. Son muy comunes, acarrean un impacto negativo en la sociedad digital y tienen consecuencias económicas importantes, aunque escasamente reconocidas y definidas. Pueden estar vinculados con estafas de naturaleza económica, sexual, la utilización o venta de herramientas para ataques o de material privado de terceros sin permiso entre otros[96].

Impactos no deseados

La ciberseguridad impacta sobre la seguridad nacional, la seguridad pública y la seguridad de las personas, tanto físicas como jurídicas[97], hasta el punto de que los ciberataques pueden llegar a desestabilizar un país[4], cómo en el reciente caso de Costa Rica[98]. Generalmente el tipo de impacto más visibilizado es el coste monetario de los ciberataques. Sin embargo, el impacto económico es mucho más complejo[20,21]. Trasciende el aspecto monetario y abarca una gran cantidad de repercusiones directas y secundarias. Entre los efectos que tiene sobre empresas, instituciones o Estados[1], destacan los derivados del daño reputacional, pérdida de competitividad, cese temporal o definitivo de servicios o actividades, pérdidas indirectas y efectos colaterales a personas u otras estructuras, entre otros muchos[20,21,96]. Para hacerse una idea, el 60 % de las pymes europeas que son víctimas de ciberataques desaparecen[99]. El personal experto ha señalado la necesidad de desarrollar en más profundidad la economía de la ciberseguridad y ahondar en el estudio de los incentivos y riesgos que la caracterizan[21] y el importante debate en torno al esfuerzo inversor que desarrollan tanto el sector público como el privado[100,101]. Con ello, pueden dotarse de mayor rigor y exhaustividad las escasas cifras que existen en torno al impacto económico.

En la misma línea, los ataques informáticos también tienen el potencial de producir graves efectos sociales y sobre las personas, desde físicos a psicológicos[102–104]. También pueden dirigirse contra la integridad de las infraestructuras con los consiguientes daños para las personas[42]. La falta de ciberseguridad en la tecnología puede suponer la pérdida de confianza de la ciudadanía y, por tanto, limitar o detener el desarrollo digital[1]. Por ello, los nuevos servicios y oportunidades, además de ser innovadores, han de estar basados en sistemas seguros y resilientes.

Gobernanza: procesos para una sociedad resiliente

El marco internacional y el contexto europeo

España tiene compromisos y obligaciones internacionales, además de las derivadas de su pertenencia a la Unión Europea, en el ámbito de la ciberseguridad y el cibercrimen que han de considerarse en el marco de la gobernanza (**Cuadro 3**).

Cuadro 3. Marco internacional

Respecto al cibercrimen, el marco internacional se asienta sobre el Convenio de Budapest (firmado en 2001)[105]. Fue ratificado por España en 2010[106] y cuenta con un segundo protocolo adicional (2021) también firmado por España (2022)[107] y avalado por la UE[108]. A escala internacional, son varios los marcos que tratan de promover un uso adecuado de las TIC por parte de los Estados y así evitar que el creciente uso de operaciones cibernéticas ofensivas impacte en el mantenimiento de la paz y la seguridad internacional. De forma no exhaustiva e incluyendo aproximaciones de naturalezas distinta (recomendaciones estatales o internacionales) destacan:

- Naciones Unidas trabaja desde 1998 en el desarrollo de medidas que delimitan el marco para el comportamiento responsable de los Estados en torno al uso indebido de las TIC. El esfuerzo de los distintos grupos de trabajo (grupo de expertos gubernamentales y grupo abierto) ha dado como resultado reciente dos informes de consenso[109,110].
- Las 16 medidas propuestas por la Organización para la Seguridad y la Cooperación en Europa (OSCE) para el fomento de la confianza destinadas a reducir los riesgos de conflicto dimanantes del uso de las TIC[111]. Las medidas están diseñadas para aumentar la previsibilidad del ciberespacio y brindar instrumentos y mecanismos concretos para evitar la falta de entendimiento.
- El Manual de Tallin, sobre la aplicación de las normas existentes de derecho internacional en el nuevo marco de la Ciberguerra[112], fue desarrollado por académicos y publicado por el Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN.
- La denominada "Paris Call" es una declaración de principios y valores comunes para hacer del ciberespacio un lugar libre, seguro y abierto. Destinado a fortalecer la confianza y seguridad entre distintos actores, ha sido ratificado por todos los Estados miembros de la UE y EE.UU. entre otros[113].

El ordenamiento jurídico español y, por tanto, la gobernanza de la ciberseguridad, está vinculado a las iniciativas regulatorias (directivas y reglamentos) y políticas públicas de la UE. La soberanía tecnológica y digital europea se basa en la combinación de capacidades técnicas y seguridad jurídica para generar un entorno digital confiable[114]. La Estrategia Europea de Ciberseguridad persigue un Internet global, abierto y seguro. Para lograrlo, se centra, sobre todo, en el desarrollo de instrumentos políticos y normativos (**Cuadro 4**), así como en los mecanismos de inversión[39].

Cuadro 4. El gran paraguas normativo de la UE

La Agencia de la UE para la Ciberseguridad (ENISA, por sus siglas en inglés) es la encargada de apoyar y contribuir a la ciberseguridad de la Unión[115]. La UE también cuenta con organismos que sirven en materia de ciberseguridad a las instituciones, los cuerpos y las agencias europeas y se coordinan con los Estados miembros como es el Centro de Respuesta a Ciberincidentes de la UE (CERT-UE, por sus siglas en inglés)[116]. Además, la UE ha desarrollado un nutrido espectro de políticas y regulaciones que abordan de forma directa o transversal cuestiones de ciberseguridad[1]. Junto a la Estrategia Europea de Ciberseguridad (la actual data de 2020)[39], hay que destacar la Directiva para la Seguridad de las Redes de Información (SRI 2016; NIS, por sus siglas en inglés)[3], el Reglamento General de Protección de Datos (2016)[117], la creación de la Organización Europea para la Ciberseguridad (ECSO, 2016)[118], el Reglamento para la Ciberseguridad (2018; Cybersecurity Act en inglés)[4], la Estrategia Europea de Datos[119] y la Ley de Gobernanza de Datos (2020)[120].

En el presente, la Directiva SRI está siendo actualizada en la NIS2 (2022)[121]. Junto a ella, se desarrolla un paquete normativo complementario que incluye las propuestas del Reglamento sobre la resiliencia operativa digital del sector financiero (DORA)[122], de la Directiva relativa a la resiliencia de las entidades críticas (REC) y la del nuevo Reglamento sobre el Marco para una Identidad Digital Europea (eIDAS)[123]. Algunas normas pueden tener un efecto indirecto sobre la ciberseguridad, por ejemplo, a través de las prácticas de marcado, como la de Ley de Mercados y Servicios Digitales (2020)[124,125].

Entre otras propuestas normativas vinculadas a la ciberseguridad cabe mencionar la Ley de Inteligencia Artificial[126] o importantes paquetes en desarrollo como la Ley de Ciberresiliencia[127], que regula la seguridad de terminales (en particular IoT) y el software, o la nueva Ley de datos[128]. Recientemente, también hay que señalar la aprobación del Reglamento por el que se establece el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación (2021)[129,130]. Se encuentran en desarrollo y su objetivo es ejercer un papel proactivo en el desarrollo de una estrategia común a largo plazo en las políticas industriales e I+D+I de la Unión Europea para retener y generar capacidades tecnológicas e industriales en ciberseguridad. En España, el Consejo Nacional de Seguridad ha designado al Instituto Nacional de Ciberseguridad (INCIBE) como Centro de Coordinación Nacional del Centro Europeo de Competencia[131].

Según una parte del personal experto, existen numerosos retos en torno a la efectividad de las políticas europeas de ciberseguridad[132]. Entre los desafíos sobre la gobernanza europea[12,132–135], pueden resaltarse los derivados de la fragmentación del marco regulatorio y la implementación de la estrategia de ciberseguridad. Así mismo, destacan cuestiones concretas, como la mejora de la coordinación y estandarización, el avance en la independencia o soberanía tecnológica, el aumento de la transparencia en el desarrollo de las políticas públicas y el refuerzo de la confianza, la resiliencia y la formación de los usuarios.

Aproximación española a la ciberseguridad

Centros de Respuesta a Incidentes de Ciberseguridad: Por sus siglas en inglés se les denomina CERT o CSIRT. Aunque los acrónimos se suelen usar indistintamente existen diferencias en la terminología. Para actividades de detección y repuesta de ciberataques son también asimilables a los denominados Centros de Operaciones de Ciberseguridad (SOC, por sus siglas en inglés).

La estructura de gobernanza española se asienta en el marco del Sistema de Seguridad Nacional con las instituciones y autoridades competentes y los **Centros de Respuesta a Incidentes de Ciberseguridad** (CERT, CSIRT, SOC) por una parte, y los mecanismos de cooperación público-privada, por otra[6,101,136,137] (**Cuadro 5**). Las instituciones, además de asistir al Gobierno en materia de ciberseguridad, se encargan de tareas de coordinación, colaboración y cooperación[136]. Las autoridades competentes en materia de ciberseguridad de cada sector ejercen las funciones de promoción de las obligaciones, la vigilancia y la aplicación del régimen sancionador cuando procede. La puerta de entrada de las notificaciones de incidentes para organizar una respuesta oportuna son los CSIRT o CERT. España es el país europeo con más CERT[18].

Recientemente se ha actualizado el Esquema Nacional de Seguridad (ENS2) en relación con la ciberseguridad[149] y, en las últimas décadas, el marco normativo no ha dejado de evolucionar[166]. España cuenta con un Código de Derecho de la Ciberseguridad que recoge todas las regulaciones en la materia[167]. A pesar de ello, desde el Foro Nacional de Ciberseguridad se señala la necesidad de que las autoridades públicas y el sector privado puedan compartir la visión y anticipación estratégicas en materia normativa[168]. Son cuestiones necesarias para definir los debates y el posicionamiento en el ámbito nacional e internacional.

En cuanto a la percepción de la población, algunas estadísticas sobre confianza social en Internet o actitud ciudadana respecto a la ciberseguridad sitúan a España ligeramente por debajo de la media europea[19,169,170]. En esta línea, datos de 2021 indican que alrededor del 40 % de usuarios ven difícil acceder a información para navegar de forma segura y el 80 % considera que la administración ha de implicarse más en mejorar la seguridad[7]. A pesar de ello, el compromiso con el desarrollo digital y de la ciberseguridad nacional ha sido positivamente valorado por distintos indicadores a nivel internacional[171,172]. En concreto, se destacan como fortalezas el marco legislativo, las capacidades de desarrollo y la cooperación del sistema español[56].

Cuadro 5. Estructura organizativa de la ciberseguridad en España y actores principales

La gobernanza de la ciberseguridad en España responde a un esquema plural y algo atomizado a diferencia de otros modelos centralizados en una autoridad competente a nivel nacional[137–139]. Aunque algunos actores nacionales del sector privado han señalado su preferencia por un modelo más centralizado[140], estudios internacionales señalan ventajas e inconvenientes en ambos modelos a nivel estatal o dentro de las instituciones[135,141–143]. La reciente transposición de la Directiva NIS[91] proyecta aspectos de carácter centralizado, como la creación de una Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes ("ventanilla única").

Las actuaciones estratégicas del Estado y Fuerzas de Seguridad se enmarcan tanto en la Estrategia (2019)[6] como el Plan (2022)[15] Nacional de Ciberseguridad y el Plan estratégico contra la cibercriminalidad (2021)[144]. En el marco del Sistema Nacional de Seguridad hay que destacar el Consejo de Seguridad Nacional (CSN), el Comité de Situación (en caso de crisis), el Consejo Nacional de Ciberseguridad (CNCS) y la Comisión Permanente de Ciberseguridad[6]. Entre ellos, el CNCS es el órgano que se encarga de dar apoyo al CSN en materia de ciberseguridad. Agrupa las autoridades competentes[145], así como representantes autonómicos o del sector privado cuando es necesario[136]. La cooperación Estado-Comunidades Autónomas se desarrolla también a través de la Conferencia Sectorial para Asuntos de Seguridad Nacional[146]. Por otro lado, hay que señalar el Foro Nacional de Ciberseguridad. Destaca por ser la entidad que agrupa y cohesiona la sociedad en materia de ciberseguridad, coordinado desde el Departamento de Seguridad Nacional bajo el paraguas del CSN. Promueve la colaboración público-privada o la cultura de ciberseguridad, entre otros muchos objetivos[147].

Los principales actores que además incluyen en su organización los Centros de Respuesta a Incidentes de Ciberseguridad (CERT) de referencia estatal[136], son:

- **Centro Criptológico Nacional (CCN)[148]:** perteneciente al Centro Nacional de Inteligencia y dependiente del Ministerio de Defensa. Se encarga de la ciberseguridad en el ámbito de las administraciones públicas. Entre sus múltiples funciones lleva a cabo la coordinación nacional de la respuesta técnica ante ciberataques, y es responsable de tareas de formación y sensibilización[149] en el sector público. Actúa también como Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las TIC[149].
- **Instituto Nacional de Ciberseguridad (INCIBE)[150]:** dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, se ocupa del desarrollo de la ciberseguridad y de la confianza digital de la ciudadanía, red académica y de investigación, profesionales, empresas y sectores estratégicos. Su actividad se basa en la investigación, la prestación de servicios y la coordinación con otros agentes.
- **Mando Conjunto del Ciberespacio[151]:** subordinado al Jefe de Estado Mayor de la Defensa (Ministerio de Defensa), es el órgano de la estructura operativa responsable de la ciberseguridad y la repuesta en el ámbito militar y de defensa nacional.

A través de la Oficina de Coordinación de Ciberseguridad de la Dirección General de Coordinación y Estudios se desarrollan las funciones de coordinación operativa para el intercambio de información con la Unión Europea y los Estados miembros, de coordinación técnica entre la Secretaría de Estado y sus organismos dependientes, ejerciendo además de canal específico de comunicación entre esta Secretaría y los CERT nacionales de referencia[152]. Además, hay que señalar el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC)[38] que se ocupa de la seguridad, incluida la ciber, en el ámbito de las infraestructuras críticas y que depende del Secretario de Estado de Seguridad (Ministerio del Interior). Destacan otros actores como el Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos[153–155], y los CERT y centros autonómicos de ciberseguridad (como Andalucía, País Vasco, Comunidad Valenciana o Cataluña entre otros)[156–159] integrados en la Red Nacional de Centros de Operaciones de Ciberseguridad (RNS, Red Nacional de SOC)[160] también participada por el sector privado e impulsada por el CCN.

En cuanto a las fuerzas y cuerpos de seguridad del Estado, pertenecientes al Ministerio de Interior, pueden destacarse la Unidad de Investigación Tecnológica que actúa como Centro de Prevención y Respuesta E-Crime de la Policía Nacional (compuesta por la Brigada Central de Investigación Tecnológica y la Brigada Central de Seguridad Informática) y el Grupo de Delitos Telemáticos de la Guardia Civil[136,161] así como la existencia de diversas unidades y cuerpos autonómicos[162–164]. La Oficina de Coordinación de Ciberseguridad[165] coordina los distintos actores del Ministerio de Interior.

Redes colaborativas y coordinación

La ciberseguridad requiere de una cultura común de estrecha colaboración y confianza internacional entre los gobiernos, pero también entre sus administraciones y con el sector privado[1,6,39]. Este último sustenta buena parte de los servicios esenciales y es clave para afrontar los retos derivados de la digitalización y la implantación de nuevas tecnologías[25,101,139,139,173–175]. Este aspecto también es señalado en un estudio de carácter prospectivo en España[139]. A nivel europeo, se ha indicado que el desarrollo de servicios y productos conectados y resilientes requiere de una estrecha cooperación en relación con el mercado interno, el cumplimiento de la ley, la diplomacia y la defensa[25,39].

Un ataque puede propagarse hasta tener efectos a escala internacional, fuera del objetivo para el que se diseñó[48]. Por ejemplo, el *ransomware* NotPetya lanzado contra Ucrania en 2017 afectó a infraestructuras críticas en todo el mundo[176,177]. Por ello, la UE busca un marco común de ciberseguridad basado en la cooperación y coordinación tecnológica, normativa y de gobernanza, que asegure la coherencia y alineamiento de los Estados miembros en sus acciones y políticas de ciberseguridad[1,25]. Entre otros mecanismos de respuesta ante ataques de gran escala, en particular, aquellos promovidos por estados, la UE cuenta con un conjunto de acciones de ciberdiplomacia (*EU cyber diplomacy toolbox*) destinada a la contención de conflictos entre actores-Estados[178]. Es una cuestión especialmente crítica si se atiende al marco internacional.

El personal experto coincide en que la invasión rusa de Ucrania abarca un amplio rango de ciber-operaciones que contravienen el marco internacional[179,180]. A nivel nacional, el conflicto ha sido considerado por el gobierno como una amenaza que requiere de un refuerzo de la ciberseguridad[181]. En los últimos años, además de las capacidades

defensivas, los países, incluyendo el marco europeo[25,39], están desarrollando una ciberdefensa activa que puede habilitar capacidades ofensivas para actuar de forma disuasoria[40,182–185]. Aunque los esfuerzos internacionales se centran principalmente en evitar el uso malicioso de las TIC (**Cuadro 3**), algunos trabajos señalan la necesidad de definir límites legales en torno al denominado ciber-armamento, como existe para otro tipo de armas (destrucción masiva, etc.) fuera del ciberespacio[177]. Algún estudio reciente indica que los países (como EE. UU. o Reino Unido) no suelen responder con contundencia a los ataques protagonizados por actores-Estado[186]. El riesgo derivado de hacerlo es complejo y muy difícil de cuantificar (atribución errónea, efectos imprevistos, escalada de acciones, etc.) y se recurre a actuaciones contenidas (atribución pública, sanciones económicas y/o diplomáticas entre otras) y de carácter diplomático[178].

Para reforzar la ciberinteligencia a nivel colectivo, es necesario compartir la información sobre las amenazas en el transcurso y después de un ataque, algo que requiere de la coordinación entre los distintos actores (organismos responsables, administraciones, infraestructuras, empresas, etc.) que intervienen tanto a nivel nacional como internacional[1,39,173,187]. Además de fortalecer la transparencia, esto dificulta que las amenazas puedan migrar entre territorios (o instituciones, servicios esenciales, empresas, etc.) y permite la contención previa de las amenazas. Sin embargo, la conciencia colectiva de la UE y el tejido público y privado debe reforzarse en este sentido y conviene generar incentivos y mecanismos de confianza para ello[25,39]. Por ejemplo, en algunos ámbitos, la voluntad de colaborar puede verse mermada por el daño reputacional que pueden causar los ataques[188]. Desde la investigación, se trabaja en la mejora y potenciación de métodos para compartir la información de una forma segura, dinámica y privada[39,187,188].

Vulnerabilidad día-cero: una vulnerabilidad que acaba de ser descubierta, normalmente tras el lanzamiento de un producto, programa o sistema operativo, y que aún no tiene un parche que la solucione.

Políticas de revelación coordinada de vulnerabilidades: procesos para la detección de vulnerabilidades por parte de grupos expertos que trabajan de forma coordinada y comparten la información con los responsables, proveedores o propietarios de las TIC analizadas.

***Hacking* ético:** es *hacking* que se pone en marcha a petición de clientes que solicitan el servicio para analizar la seguridad y vulnerabilidades de sus sistemas. Se imita a un atacante, pero excluyendo el ánimo malicioso

Autonomía estratégica: El concepto abarca el propósito de la UE por asumir una mayor responsabilidad sobre su propia seguridad, la reducción de relaciones de dependencia asimétricas en sectores críticos, y el refuerzo de sus capacidades para fijar e implementar su propia agenda y prioridades. Parte de la idea de un estado actual de cierta vulnerabilidad, dependencia y gradual pérdida de poder o soberanía en ciertas áreas para lograr una mayor resiliencia, relaciones simétricas de interdependencia y mayor poder o autonomía.

Por diseño y por defecto: referido a la privacidad o la seguridad. Consiste en implementar medidas técnicas y organizativas (procesos y formación del personal) desde el comienzo y en cada paso de las operaciones de procesado de datos o en el diseño y desarrollo de tecnologías para salvaguardar la privacidad y la seguridad de los datos y las personas y hacerlo por defecto, es decir, en todos los casos. Supone un cambio desde un modelo reactivo hacia uno proactivo en el que la seguridad o la privacidad no son un añadido sino parte del propio diseño y desarrollo.

De igual manera, el personal experto ha señalado la necesidad de mejorar la gestión de las vulnerabilidades para favorecer la transparencia y la cooperación. Es especialmente relevante en las de **día-cero**, que son vendidas y compradas abiertamente en Internet[1]. El desarrollo de **políticas para la revelación coordinada de vulnerabilidades** a nivel europeo puede contribuir en esa dirección[189]. Se trata de un procedimiento común en otros países (EE. UU., Francia, o Bélgica)[189] y que en España se encuentra en desarrollo[189] bajo un marco ya establecido[190]. Además, España cuenta con algunos mecanismos para comunicar vulnerabilidades, incluyendo día-cero[191,192]. El ***hacking* ético**, desarrollado normalmente por investigadores en ciberseguridad, puede favorecer la gestión de las vulnerabilidades[193,194]. Cuenta con un tejido asociativo reconocido en España, pero no está regulado a nivel nacional[193].

España cuenta con dos plataformas independientes para la distribución de la ciberinteligencia[195–197]. Además, fomenta la cooperación y la coordinación interna e internacional[6]. Internamente, se han reforzado estos aspectos por ejemplo a través de la llamada Red Nacional de Centros de Operaciones de Ciberseguridad (SOC, por sus siglas en inglés)[160,162] o del Foro Nacional de Ciberseguridad (**Cuadro 5**). A escala internacional, se compromete con el desarrollo de un ciberespacio abierto, plural y seguro mediante la colaboración en foros, convenios, bases de datos y organismos internacionales y la cooperación bilateral[6,198–200].

Componentes de confianza: soberanía tecnológica y seguridad por diseño

Desde la comunidad científica se ha señalado la importancia del desarrollo de marcos regulatorios que consideren la seguridad y la privacidad de los productos, sistemas, etc., antes[1] y después de su comercialización[201,202]. Europa se encuentra en un escenario de las TIC dominado por terceros países en inversión y patentes[1]. Esto puede dificultar la utilización de tecnologías de confianza y con confianza[203]. Por ello, los principales actores en ciberseguridad[135] y la UE[39,76,204] consideran una cuestión central incrementar la soberanía tecnológica. En este sentido, fortalecer la capacidad e independencia tecnológica, desde un perspectiva técnica o regulatoria, puede fomentar colaboraciones más equitativas y complementarias con terceros países[76,114,204]. Las redes de comunicación como el 5G y el desarrollo de *software* son dos ejemplos de tecnología en el centro de las TIC que ilustran esta situación.

El despliegue de la tecnología 5G requiere ajustes de ciberseguridad[205,206] y una mayor armonización de los criterios seguidos por los Estados miembros para ello[68]. En línea con EE. UU., la UE ha señalado la posibilidad de limitar la participación de algunas compañías consideradas de riesgo debido a su relación con terceros países para limitar los riesgos asociados al proveedor/implementador[68,206]. Así lo ha recogido la legislación española[207]. La UE también ha identificado la necesidad de un enfoque basado en la **autonomía estratégica** en el desarrollo tecnológico, entre otros campos, que atienda a la realidad geopolítica en que vivimos[208,209].

Aunque son muchos los retos en torno a la seguridad del *software* y el *hardware*[210], existe consenso sobre la necesidad de abordarla como un elemento central desde su propia concepción y desarrollo[4]. Se trata de la llamada seguridad **por diseño y por defecto**, que ha de extrapolarse a todos los ámbitos de las TIC, ya sean dispositivos, sistemas o infraestructuras[1,211–213]. Esta debe, además, considerar el ciclo de vida completo de la tecnología, adecuándose a posibles actualizaciones, cambios de entorno o desarrollos normativos[210]. Recientemente la Unión Europea ha lanzado una iniciativa legislativa destinada a que de forma horizontal los productos con elementos digitales consideren la ciberseguridad desde su diseño[214]. El empleo preferente de *software* y *hardware* de uso libre o fuente abierta[215] y la

implementación de sistemas de certificación son otras medidas que pueden reforzar la seguridad y confianza en las TIC[1,4,216], aunque existen aún importantes disensos y retos en torno a estas cuestiones[1,28,217–219].

Certificación y cumplimiento

La certificación y la estandarización de la ciberseguridad puede considerarse la primera línea defensiva para mitigar las amenazas antes de la comercialización[1,4,220]. Son procesos que mejoran la confianza y pueden referirse a productos (IoT, *software,* etc.), servicios (como el almacenamiento y computación en la nube), procesos (aspectos administrativos y de gestión entre otros), sistemas, entidades o empresas e, incluso, conocimientos (personas)[149,221]. Algunos datos del sector privado sugieren que las empresas que carecen de certificaciones sufren un porcentaje mayor de ciberincidentes[222].

Por todo lo señalado, constituye una cuestión estratégica y de liderazgo internacional para la UE[39,114,223], también considerada un aspecto clave por el resto de actores[135]. Sin embargo, su complejidad, debida a la constante evolución tecnológica (actualizaciones, etc.) y de las propias amenazas, no permite la implantación de marcos estáticos, fijos, como en otros sectores. La UE trabaja en la creación de un marco común para la estandarización y certificación[4,127,224] que reduzca la fragmentación actual[219,225], los costes y el tiempo de certificación a las empresas de productos y servicios basados en las TIC. Esta cuestión ya se ha desarrollado tanto para los servicios en la nube[226] como el despliegue 5G[227] y seguirá avanzando hacia otros dominios. Respecto a los consumidores, los actores involucrados y el personal experto han planteado la posibilidad de implantar un sistema de etiquetado[1,217,224,228], similar al energético. El objetivo es permitir a los usuarios reconocer fácilmente el nivel de seguridad de los productos.

A pesar de todo ello, existen importantes desafíos que requieren de avances en este campo[1,135,217,219,225,229]. Destacan los asociados a la competitividad, basados en la relación coste-beneficio y tiempo del proceso de certificación o los asociados al tipo y nivel de certificación, que puede ir desde autodeclaración voluntaria a procesos de certificación obligatorios y dependientes de un agente externo. También hay que señalar aspectos vinculados a la gobernanza, es decir, quién certifica, y a la necesidad de actualizaciones durante el ciclo de vida o la certificación de componentes (cada una de las partes de los productos y sistemas) en las cadenas de suministro. La UE, a través de la Ley de Resiliencia, actualmente en desarrollo, pretende establecer unos estándares comunes de ciberseguridad en los productos de *software* y *hardware* que se comercializan, enfocándose, en particular en los dispositivos utilizados en aplicaciones críticas e IoT[127,230,231]. Actualmente, en España los organismos públicos o las empresas que dan servicios a estos y se encuentran bajo el alcance del Esquema Nacional de Seguridad, cuentan con el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC) que disponen de garantías de seguridad contrastadas[232].

Un aspecto igualmente importante para generar confianza en las TIC se refiere al cumplimiento de los criterios de seguridad[233]. Una empresa podría comprometerse a generar parches de seguridad para un dispositivo IoT durante meses, años o no hacerlo. Por tanto, puede resultar beneficioso delimitar la responsabilidad de la ciberseguridad de los actores involucrados, incluso después de la comercialización de un producto[1,12,234,235]. Para estimular estos procesos, parte de la comunidad científica señala que es necesario implementar sistemas de control e incentivos que favorezcan las buenas prácticas[1] y promuevan la ciberseguridad como una inversión y no solo como un gasto[236].

Las personas en el centro de la ciberseguridad.

Cibercultura y formación

Se estima que el 95 % de los ciberincidentes se pueden vincular a un error humano[8], bien por desconocimiento o por desinterés. De forma generalizada, se ha señalado el bajo nivel de conocimientos de las personas como un factor que debilita la ciberseguridad de los Estados[237]. La ciudadanía y la sociedad civil son corresponsables de la ciberseguridad nacional[238], por lo que la concienciación y la formación son esenciales para avanzar hacia un ecosistema más resiliente[4]. Estudios recientes han señalado cierto nivel de desconexión entre las numerosas iniciativas dirigidas a la concienciación, así como de desconocimiento por parte de la población[238]. Alrededor del 50 % de la población desconoce las principales campañas en materia de ciberseguridad y la misma proporción considera que necesitan formación en dicho ámbito[7].

Ciberhigiene: medidas rutinarias respecto al uso de las TIC para mantenernos protegidos de las amenazas y riesgos que existen en el ciberespacio.

La evidencia científica señala que las actividades y programas de concienciación no siempre son efectivas[239,240]. Así, para reforzar el nivel de **ciberhigiene** y la cultura de la ciberseguridad, conviene desarrollar programas basados en problemáticas específicas, dirigidos a audiencias concretas[241] y apoyados en evidencias científicas sobre cambio de comportamiento[240,242,243]. Igualmente, es necesario implementar métricas que evalúen la efectividad de las acciones que se desarrollan para poder avanzar[238]. Desde el Foro Nacional de Ciberseguridad se hace hincapié en la necesidad de evolucionar de la concienciación al compromiso y a promover la capacitación en ciberseguridad adecuada a la demanda del mercado[221].

En España, el CCN y el INCIBE llevan a cabo programas de concienciación y formación tanto generales como sectoriales[244–247], incluyendo sectores vulnerables como la infancia o mayores de 60 años[17,248,249]. También desarrollan o participan en programas para el fomento de la cibercultura y la captación de talento, como CyberCamp, la plataforma ATENEA o el programa Talento Hacker, entre otras[250–252]. Sin embargo, existe un déficit de profesionales cualificados en este terreno[22,253,254] que en España se ha estimado en torno a los 24.000 trabajadores en 2021[22]. Este déficit limita la productividad y es más notorio en contextos con mayor dificultad para acceder a la ciberseguridad como las pymes[99,255].

Aunque España cuenta con iniciativas orientadas a acercar la ciberseguridad a las pymes[256], el personal experto ha señalado que puede ser útil que sean las entidades u organismos cercanos al tejido de estas empresas, como pueden ser las asociaciones empresariales y sectoriales, quienes faciliten y canalicen este acceso, atendiendo a la gran diversidad del sector[221]. Además de una cuestión de seguridad, lo es de competencia. Aquellas empresas que

intervengan en la cadena de suministros de entidades críticas o en licitaciones para la prestación de servicios a las administraciones públicas se verán afectadas por regulaciones que ya están en camino[121,127], lo que puede modificar los requisitos para el desarrollo de esas actividades limitando el acceso a las mismas.

Por otro lado, los datos muestran una importante brecha de género en el sector tecnológico, concretamente, en ciberseguridad[22,257,258]. A escala nacional el 18 % de las personas que se especializan en este campo son mujeres[22] y, a nivel internacional, el 24 %[259]. Se ha señalado que, en ocasiones, la tecnología incorpora y perpetúa las desigualdades estructurales, como las de género, orientación sexual, etc. presentes en la sociedad[257,260,261]. Fomentar medidas (regulatorias, incentivos económicos, formación de talento, etc.) destinadas a reducir la brecha y aumentar la diversidad desde fases tempranas puede abordarse como una oportunidad[22] para el sector y un medio para anclar el principio de igualdad en torno a la ciberseguridad[258,260,262–264].

En lo relativo a la formación, existen recomendaciones para la inclusión de la ciberseguridad en las diferentes etapas no universitarias del sistema educativo y la formación profesional[238,253]. Esto ya ocurre en otros países de nuestro entorno[253,254,262]. Los datos indican que la proporción de ciberespecialistas aumenta y que la oferta académica universitaria[265], cada vez más armonizada a nivel europeo[266], está consolidada y bien desarrollada en España[255,267]. Sin embargo, existen dificultades para atraer y retener el talento. Por ello, los trabajos en torno a esta cuestión señalan que conviene mejorar los incentivos, especialmente, en el contexto público, incluyendo a los Cuerpos de Seguridad[268] y el sector investigador[22]. Además, conviene señalar que, a nivel internacional, el desarrollo de nuevas capacidades se está vinculando con la creación de centros y perfiles multidisciplinares que aborden de forma transversal la ciberseguridad[132,135,269–271].

Ciberderechos

El derecho a hacer un uso libre y fiable del ciberespacio, a utilizar y consumir tecnología y dispositivos con garantías de seguridad y contribuir a que así sea, es una responsabilidad compartida[6]. De hecho, parte del personal experto a nivel internacional lo vincula con los derechos fundamentales[272] y lo conectan, directa o indirectamente, con el respeto de los Derechos Humanos por parte de los Estados u otros actores[273]. Parte del personal experto ha señalado que la ciberseguridad, o algunas partes de ella, pueden considerarse como un bien público, aunque existen distintas visiones al respecto[274]. En España el Gobierno aprobó en 2021 la Carta de Derechos Digitales, un marco de referencia de naturaleza no normativa orientado a garantizar y reforzar los derechos de las personas en el mundo digital. Compila los derechos recogidos separadamente en normativas y reglamentos previos y recoge el derecho a la ciberseguridad en su sección IV[275].

La forma en que se aplica la ciberseguridad puede colisionar con valores éticos fundamentales si no es bien gestionada[276,277]: la seguridad, dirigida a la protección social y de la persona; la privacidad, asociada a la dignidad humana, el control de los datos y el secreto de las comunicaciones electrónicas; la justicia, ligada a la igualdad, la equidad y la defensa de las libertades civiles en el ciberespacio; y la rendición de cuentas. Desde la comunidad científica se ha destacado la importancia de que las cuestiones éticas planteadas se incorporen y concreten en la legislación de los entornos digitales y no se traten como cuestiones complementarias fuera del ámbito legal[278,279].

El denominado abuso o maltrato tecnológico agrupa distintas formas en las que la tecnología, como el IoT[280,281], se explota para acosar, hostigar o controlar a las personas[280,282]. En concreto, mujeres y niñas constituyen grupos vulnerables más propensos a recibir este tipo de ataques[261,264]. Incluye el ciberacoso, el ciberhostigamiento, ciberespionaje, la violación de la intimidad o la intimidación física o verbal y un largo etcétera.[261,264]. El Parlamento Europeo reconoce la ciberviolencia de género como una extensión de la violencia de género con importantes efectos negativos[261]. Aunque existen algunos estudios que profundizan en estos aspectos[257,264,280–282], destaca la falta de datos sobre esta cuestión y sobre la situación de otros grupos vulnerables[261].

Hacia un ecosistema tecnológico más seguro

Los avances en investigación pueden permitir el desarrollo de tecnologías orientadas a reforzar la ciberseguridad, ya sean nuevas herramientas, como algunas tecnologías disruptivas, o mejoras de las existentes.

Avances tecnológicos: dispositivos y sistemas más seguros

La privacidad y seguridad de los sistemas pasa por la de cada uno de sus componentes. El elemento más vulnerable o débil de un sistema determina el nivel de seguridad del sistema en su conjunto (cadena de suministro, sistemas basados en las TIC, red de comunicaciones, dispositivo, sistema operativo, etc.). Así, cualquier elemento puede constituir la vía de entrada que afecte a todo el conjunto interconectado. En cuanto a las causas que limitan la ciberseguridad, de forma generalizada, se pueden destacar la falta de incentivos económicos y competitivos para la mejora de dispositivos u otros productos y servicios (ya que, entre otros, los usuarios valoran más otras características frente a un refuerzo de seguridad), la fragmentación de los estándares de fabricación, desarrollo o implementación y el uso inapropiado de los dispositivos o sistemas, entre otras[83].

En el caso del IoT, las causas tienen que ver con su baja capacidad de computación y al ajustado margen coste-beneficio con el que se fabrican, entre otras[47,283]. También destaca la falta de una configuración segura por defecto y de mecanismos accesibles para su verificación y modificación[64,201]. El IoT se considera actualmente uno de los dominios de investigación más activos[47,61,284] (**Cuadro 6**). En relación a los dispositivos personales, como los teléfonos móviles, especialmente sensibles para la privacidad, destaca la heterogeneidad de su composición y la falta de mayores controles de seguridad y privacidad[83,285]. Ambos aspectos atañen tanto al *hardware* como al *software*, incluyendo aplicaciones preinstaladas o que instala el usuario.

Cuadro 6. Un Internet de las cosas más seguro

El Internet de las cosas se sitúa al frente de la transformación digital mundial y de los cambios económicos que conlleva[59]. La investigación, desarrollo e innovación en este campo son esenciales bajo el prisma europeo[59,63]. De hecho, el IoT es la puerta de entrada de muchos ataques[47,64,286]. Respecto a la ciberseguridad de los dispositivos IoT, buena parte de los esfuerzos se están centrando en el desarrollo de criptografía ligera compatible con sistemas con poca capacidad[287,288] y en el de procesos de certificación, evaluación y control durante todo el ciclo de vida de los dispositivos que permitan una mayor seguridad desde el propio diseño[4,217,218,289]. Además, se avanza en el desarrollo de sistemas que permitan la actualización remota del firmware y software para corregir vulnerabilidades, un sencillo manejo y conocimiento del estado de seguridad (como la seguridad por contrato)[201] y la responsabilización por parte de los fabricantes de estas cuestiones[290]. Igualmente, se trabaja en la mejora de la identificación de amenazas y vulnerabilidades mediante diversas técnicas como el *fuzzing*[291–293] y la recolección de datos (por ejemplo, usando dispositivos trampa, comúnmente llamados *honeypots* por su nombre en inglés) y el posterior desarrollo de modelos mediante técnicas de IA[286,292,294]. También se trabaja en la mejora de la interoperabilidad de la seguridad[295].

Computación en el borde: se refiere al procesamiento, análisis y almacenamiento de los datos más cerca de donde se generan para permitir análisis y respuestas más rápidos, casi en tiempo real. Incluye las técnicas conocidas como *fog* y *edge computing*.

Otro aspecto a tener en cuenta es la computación en la nube, que se apoya en la creación de nodos intermedios ubicados más cerca de los puntos donde se generan los datos, como en los rúters o las infraestructuras de comunicación. Estos se suman a los grandes sistemas centrales de procesamiento y almacenamiento y permiten que la información no tenga que viajar hasta la nube, pudiendo reducir el tiempo de respuesta o latencia[296]. Es la llamada **computación en el borde**, configurando así la conocida como computación en continuo IoT-borde-nube[297]. Aunque esta tecnología ofrece nuevas oportunidades para reforzar la privacidad y seguridad[284,298], supone también un considerable aumento de las posibilidades y puntos de ataque. La nube requiere tanto de avances técnicos en torno a la seguridad y privacidad, como de carácter social y legal. Entre estos destacan aspectos ligados a la responsabilidad compartida en el contexto cliente-servicio, la seguridad y el control sobre los datos e, incluso, responsabilidades medioambientales derivadas de la distribución de los nodos y servidores y su sostenibilidad energética (computación verde)[12,299–304].

Privacidad y seguridad de los datos

La privacidad se configura como un derecho y un valor democrático esencial[305,306]. Tanto es así que la Constitución Española señala su protección frente a las TIC[307]. Su relación principal con la ciberseguridad es a través del papel de esta para garantizar la confidencialidad, integridad y disponibilidad de los datos[1], aspectos esenciales para que pueda haber privacidad. La comunidad científica señala que no existe una dicotomía entre seguridad y privacidad[308], al contrario, la seguridad es un prerrequisito para la privacidad y viceversa. Cuando los datos se usan de forma más abierta, se recurre a técnicas como la anonimización y pseudo-anonimización o la privacidad diferencial de los datos, entre otras, que aseguren su privacidad, aunque limiten su grado de detalle[75,309,310]. Sin embargo, no hay una solución universal que permita compartir los datos con la privacidad deseada y a la vez un alto nivel de detalle para extraer de los mismos toda la información (utilidad) deseada por todos los actores potencialmente interesados[75].

El escaso control sobre los datos y su comercialización, la falta de protección o el poder derivado de su acumulación y utilización, afectan a la privacidad. Estos pueden tener severas consecuencias para la población, que van más allá de la influencia sobre las preferencias o el comportamiento individual. Por ejemplo, pueden propiciar la interferencia en procesos democráticos, poner en riesgo las oportunidades (ante un empleo, entre otros muchos casos), la dignidad o incluso la integridad y salud mental de las personas[311–313]. La relevancia de estos aspectos queda muy patente en los entornos más sensibles para la privacidad, como el sanitario[314–316].

Técnicas avanzadas para la mejora de la privacidad (PET): conjunto de tecnologías orientadas a mantener la privacidad y seguridad de los datos. Existe una gran variedad incluyendo técnicas criptográficas y de anonimización, de aprendizaje federado o pruebas de conocimiento entre otras muchas.

Criptografía: campo de estudio que se encarga del cifrado y codificación de información mediante operaciones matemáticas (algoritmos) para evitar su lectura e interpretación en caso de que esta sea interceptada.

Autenticación biométrica en continuo: se basa en la autenticación continua (en tiempo real) de la identidad de un usuario usando rasgos biométricos o de comportamiento.

Aunque existen muchas opciones para proteger la privacidad[73,305], buena parte de la investigación se centra en las **técnicas avanzadas para la mejora de la privacidad** (PET, por sus siglas en inglés)[73,317–321], en las cuales aún hay mucho margen de mejora[322]. En esta línea, se impulsa el desarrollo de la **criptografía** y de nuevos sistemas de **autenticación continua y biométricos** que, a su vez, conllevan retos específicos[28,72,323]. Otro frente de investigación lo constituye la protección personalizada de la privacidad[28,298,317,322] y el desarrollo de mecanismos para delegarla en el usuario de forma entendible[298,317], persiguiendo así que cada sistema que maneja datos personales también recoja las preferencias del sujeto que los ha generado. Asimismo, los avances en el análisis forense digital son clave para mejorar los sistemas[315].

Existe consenso en torno a la necesidad de avanzar en la identificación y recolección de solo aquellos datos que son necesarios, así como en su almacenamiento, acceso, transferencia, procesamiento y eliminación segura[34,72,73]. Además, la confidencialidad y privacidad de los datos han de conservarse en todo su ciclo de vida (desde su origen hasta su destrucción)[305]. La UE[324,325] aborda estos desafíos desde una perspectiva global, basada en la privacidad por diseño y por defecto[305], en un espacio europeo común para su gestión[326] y explotación económica[325,327]. En España se incorpora esta visión de la privacidad[328].

Identidad digital

La identidad digital es el conjunto de la información sobre una persona física o jurídica expuesta en Internet (datos, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha persona en el plano digital o ciberespacio[329]. Conviene distinguir la identidad de la reputación en línea. Esta última se refiere, sobre todo, a lo que se dice de alguien en la red, no a quién es.

Confianza cero: también denominado zero trust, por su nombre en inglés. Es un modelo de seguridad actual de las Tecnologías de la Información que descarta la idea de una red interna "confiable" y una red externa "no confiable". Asume por defecto que ningún actor es confiable, acceda desde dentro o fuera del perímetro de la red. Por ello requiere una verificación de la identidad estricta y una asignación de privilegios indispensables o mínimos y bien definidos para cada persona o dispositivo que acceda a los recursos de una red.

La identidad digital permite el reconocimiento y actuación de los individuos, las corporaciones o los poderes públicos en Internet. En el entorno corporativo, este concepto se vincula habitualmente con el control de acceso, las estrategias de concesión de privilegios, como la de **confianza cero**, a un sistema dado[329,330]. Si bien son cuestiones muy relevantes para la ciberseguridad, el concepto tiene mucho más alcance[331]. Por un lado, se compone de lo que los usuarios hacen en la red a través de, normalmente, múltiples cuentas de distintos servicios y redes sociales[28,332,333]. Por otro, también abarca la identidad legal de las personas físicas o jurídicas en el ciberespacio. Por ello, es necesario alcanzar sistemas que garanticen una identidad digital fiable y verificable, que además protejan los derechos (privacidad, seguridad, etc.) de quien los usa[322,329,334].

La UE apuesta por el desarrollo de una identidad digital interoperable entre países y sectores (poderes públicos, sanidad, banca, energía, servicios digitales, educación, etc.) mediante una cartera o *wallet* digital portable en dispositivos móviles[123,335]. Esta podrá recoger información (edad, identidad, titulaciones, salud, etc.) de la ciudadanía, residentes y negocios, para certificar su identidad, permitiendo controlar la información personal que comparten.

Internet cuántico: red futura de comunicación y computación cuánticas, en la que se intercambiará información de manera totalmente segura a través de bits cuánticos (*qubits*) entre diferentes nodos de la red, que a su vez se compondrán de procesadores o sensores cuánticos capaces de realizar mediciones o computar sin parangón clásico. Esto permitirá la resolución de problemas muchos más complejos que los actuales. Se proyecta que la red sea escalable a nivel global a través de los repetidores cuánticos, que utilizando el entrelazamiento cuántico serán capaces de mandar información sin límite en distancia. Dada la complejidad de las tecnologías que aún precisa desarrollar, constituye un objetivo a largo plazo.

El desarrollo seguro de la identidad digital puede generar beneficios para un país y facilitar, como en el caso de Estonia, el acceso a servicios públicos de salud, banca o voto electrónico[336]. Por el contrario, una mala gestión puede suponer problemas de robo de identidad y suplantación con graves consecuencias económicas y sociales. Además, no son pocos los retos tecnológicos, jurídicos, administrativos y éticos que plantea su desarrollo[329,334,337–340].

Por último, es importante destacar también la necesidad de desarrollar sistemas de identidad digital segura y confiable para los propios dispositivos IoT[341,342] ya que muchos de ellos son capaces de comunicarse de forma autónoma con otros dispositivos (comunicaciones de máquina a máquina).

Disrupción e investigación

La implantación de algunas tecnologías conlleva rediseñar los marcos regulatorios, de gobernanza, tecnológicos, comerciales o industriales[343–345]. Esta disrupción se basa en su capacidad de modificar las reglas del juego aplicadas en esos marcos. Existen diversas tecnologías, en distintos grados de desarrollo y aplicación, que por su potencial para rediseñar y ofrecer nuevos servicios, reforzar o, incluso, poner en peligro la ciberseguridad, han sido señaladas como disruptivas[1].

Tecnologías de Registro Distribuido (DLT): se trata de un sistema electrónico o base de datos gestionada por diversos participantes (por ejemplo, inclusión de información como transacciones económicas, *stocks*, etc.) de forma descentralizada (no existe una autoridad, como un banco, que ejerza de validador). El *blockchain* es el tipo de DLT más popular y que más atención acapara.

Algunas tecnologías ya presentan cierto grado de implantación, a la vez que siguen desarrollando todo su potencial, como la inteligencia artificial[346]. Otras, como la computación cuántica o el **internet cuántico**, basados en ordenadores y tecnología que opera en base a la física cuántica, se encuentran en fases incipientes[347,348]. Además, existen tecnologías desarrolladas pero cuya implementación y utilidad real aún están bajo debate, como las **tecnologías de registro distribuido** (DLT, de sus siglas en inglés) y en concreto, una de ellas, la blockchain[349–356]. Aunque esta es la que más atención acapara[357], posiblemente debido a su vinculación con las criptodivisas, existen importantes disensos en torno a ella (**Cuadro 7**).

Cuadro 7. Blockchain: disensos en torno a su potencial disruptivo.

La tecnología *blockchain* es la más conocida y con mayor potencial de las tecnologías de registro distribuido[357]. A diferencia del paradigma actual, esta tecnología permite transacciones directas de activos (dinero, criptomonedas, bonos, propiedad intelectual, información, etc.) entre partes (individuos u organizaciones) sin ningún nivel de confianza previo entre ellas. Estas quedan registradas sucesivamente como eslabones de una cadena y todos los participantes de la red guardan copias idénticas y accesibles (nodos) de la misma, lo que le confiere trazabilidad e inmutabilidad al registro[358]. Pueden llegar a ser millones de nodos distribuidos en todo el mundo a priori sin jerarquía entre ellos, de ahí que se considere un sistema descentralizado. La certificación o validación de las transacciones se lleva a cabo por parte del conjunto de nodos y no por una tercera parte que las centralice (un banco en el caso del dinero)[349,358].Su disrupción se basa en que estas propiedades le otorgan una gran potencial para implantar un nuevo marco para la gestión de la confianza y la seguridad en el manejo de datos o identidades[349,359]. Sin embargo, que conceptualmente sea segura no quiere decir que su aplicación lo sea en el mismo grado, por lo que existe un notorio nivel de disenso en torno a estas cuestiones[360].

Parte de la comunidad científica cuestiona las propiedades (inmutabilidad, descentralización, etc.) de la tecnología *blockchain*, su potencial para reforzar la confianza, sus ventajas respecto a tecnologías ya existentes y, además, aún señalan importantes retos (gobernanza, consumo energético, escalabilidad, mecanismo para evitar el fraude, etc.) en su implementación[349–356,360]. Se han propuesto aplicaciones de la *blockchain* en la mayor parte de las TIC (de la nube al IoT)[361,362] y sectores (agrícola, construcción, logística, finanzas, etc.)[359,359,363,364]. También destaca el gran potencial de los contratos inteligentes[365–367] asociados a esta tecnología. Sin embargo, no existe actualmente consenso en torno a su aplicación a escala general o en ámbitos públicos. La Infraestructura Europea de servicios basados en *Blockchain* (EBSI, por sus siglas en inglés) trata de avanzar en este aspecto en el ámbito público[368]. España participa con tres nodos. Uno de ellos persigue la aplicación de la blockchain en las universidades españolas para la verificación de credenciales académicas[369,370].

Inteligencia Artificial (IA)

La IA y otras técnicas estadísticas para el análisis de datos incorporan a la ciberseguridad nuevos métodos avanzados para la detección y predicción de amenazas y la mejora de la resiliencia[292,371–374]. Mediante el análisis del flujo de datos de un sistema, la IA puede detectar patrones anómalos o asociados a algún tipo de ataque, e incluso, proponer mecanismos optimizados de repuesta. Existe consenso en torno a la necesidad de mejorar estas aplicaciones para alcanzar todo el potencial de esta tecnología que puede marcar la evolución de la ciberseguridad[374–376]. A la vez, también es necesario mitigar los riesgos asociados a la IA que pueden hacer más inseguro el ciberespacio[377]. Esta plantea retos tecnológicos, éticos y regulatorios que hay que abordar para una implantación segura. La UE los afronta a través de su propia estrategia y el desarrollo legislativo[126,316,378].

Aprendizaje federado: es una técnica de inteligencia artificial que favorece la privacidad y seguridad de los datos al trabajar simultáneamente con varios dispositivos (las técnicas clásicas son centralizadas) los cuales contienen sus propios datos locales y privados.

La IA abre la puerta a nuevos tipos de ataques[374,376,379]. Por un lado, los datos y los mecanismos en base a los que actúa pueden ser modificados malintencionadamente para una toma de decisión equivocada. Por otro, existen retos inherentes a la propia tecnología[375,376,380–383]. Entre ellos, destaca el desarrollo y uso de sistemas que cumplan con mejores criterios de seguridad, confianza, privacidad y explicabilidad. También hace falta reforzar la integridad y privacidad de los datos y las cuestiones éticas que implica su utilización.

Inteligencia de enjambre: es una rama de la Inteligencia artificial que se basa en el comportamiento colectivo de sistemas descentralizados y autoorganizados naturales (como un enjambre de abejas) o artificiales (un conjunto de dispositivos).

Nuevas líneas de trabajo como el **aprendizaje federado** o la **inteligencia de enjambre** pueden mejorar la privacidad de los datos que se usan y comparten en la IA[384,385]. Además, la combinación de esta tecnología con otras como la computación cuántica (aprendizaje cuántico) abren el futuro a nuevas formas de ciberseguridad y de manejo de la información[386].

Tecnologías cuánticas

La computación cuántica abre la puerta a avances significativos en multitud de campos[66,348]. Aunque algunas previsiones establecen un margen de 10 años para su implantación[387], no todo el mundo comparte el optimismo acerca de esta tecnología y se apunta la necesidad de más evidencias sobre su potencial y desarrollo[388]. Aún existen importantes retos, como la escalabilidad o la reducción del índice de errores entre otros[348,389].

Según la evidencia científica, su potencial disruptivo en ciberseguridad se basa en que los ordenadores cuánticos serán capaces de romper buena parte de los sistemas de cifrado (criptografía) que protegen las comunicaciones y datos en la actualidad[347,387]. Así, los esfuerzos para gestionar la disrupción que supone se centran en el desarrollo de la **criptografía postcuántica y cuántica**[72,347,390–393]. La primera consiste en el desarrollo de algoritmos para cifrar la información que puedan resistir ataques tanto de ordenadores convencionales como cuánticos y que se puedan integrar directamente en las redes de comunicación convencionales[72,347,390]. No obstante, nadie puede asegurar que, en el futuro, no se descubra alguna vulnerabilidad en los algoritmos o se invente algún método de ataque novedoso que les pueda afectar. El Instituto Nacional de Estándares y Tecnología de EE. UU. (NIS, por sus siglas en inglés) ha llevado a cabo un proceso a nivel mundial para el desarrollo y selección de estos algoritmos que ha culminado recientemente, de forma que existen varias opciones en caso de que alguno falle.

Por su parte, la criptografía cuántica se basa en el uso de la mecánica cuántica para transmitir de forma confidencial la información y requiere de un importante desarrollo y despliegue de tecnología previa (canales cuánticos basados en infraestructura satelital y terrestre por fibra óptica)[72,393,394]. A través de la distribución cuántica de clave (QKD, de sus siglas en inglés) es posible intercambiar claves de cifrado con seguridad incondicional, es decir, no condicionada a la capacidad computacional de un adversario[72]. Por tanto, resistiría cualquier tipo de ataque de un ordenador cuántico (conocidos o no). Se trata de una garantía importante para información sensible que debe ser garantizada a largo plazo, como aquella relativa a seguridad nacional, comunicaciones gubernamentales, secretos industriales o información médica o personal de la ciudadanía.

La comunicación cuántica es una tecnología crítica a nivel global con importantes implicaciones estratégicas de futuro[388]. Su desarrollo práctico e implantación son más cercanos que los de la computación cuántica y por ello, la Infraestructura de Comunicación Cuántica (EuroQCI) de la UE pretende desplegar su propia red de comunicaciones cuántica en los próximos 10 años. De acuerdo con el principio de soberanía tecnológica, esta debe basarse en tecnología desarrollada por cada Estado miembro[395]. España anunció recientemente la inversión de 54 millones de euros en el Plan Complementario de Comunicaciones Cuánticas[396], pero existen notables diferencias respecto a las estrategias y estimación de inversión de algunos países de nuestro entorno[388,397].

Disrupción segura

Junto con un adecuado marco regulatorio y de gobernanza, la investigación en ciberseguridad es clave para alcanzar cierto nivel de autonomía sobre las tecnologías, que permita minimizar los posibles impactos negativos de su desarrollo e implantación[344,345]. Además, conviene recordar que los propios centros de investigación y universidades son objetivo de los distintos actores que protagonizan las ciberamenazas[398,399]. El desarrollo de la ciberseguridad requiere de disciplinas tecnológicas y sociales. Además, se ha identificado la necesidad de reducir la fragmentación del ecosistema de I+D+I que existe en la actualidad tanto a escala europea[25,400] como nacional[221], y generar incentivos para retener el talento[22,401] y favorecer su distribución entre el sector público y privado[382].

Por todo ello, es conveniente mejorar la coordinación y cooperación de los esfuerzos en investigación pública, así como

el nivel de conexión y transferencia entre los sectores académico, empresarial e industrial y los Cuerpos y Fuerzas de Seguridad del Estado[221]. Asimismo, el desarrollo científico de la ciberseguridad debe incluir una perspectiva ética, como ocurre en otras ramas científicas[402]. En España, la información disponible señala que hay que reforzar el nivel de financiación y los incentivos para la inversión en el desarrollo tecnológico[221]. Además, es previsible que una sociedad bien formada y conocedora de sus derechos demande servicios y tecnologías seguras. Esta concienciación puede actuar como incentivo en la industria para reforzar la seguridad de los servicios o productos[236].

En definitiva, la ciberseguridad constituye una herramienta esencial para garantizar el bienestar y progreso de la sociedad.

Cómo citar este informe:

Oficina de Ciencia y Tecnología del Congreso de los Diputados (Oficina C). Informe C: Ciberseguridad. 2022. doi: 10.57952/c8hy-6c31

Equipo Oficina C (por orden alfabético)

Ana Elorza*. Coordinadora de la Oficina C en la Fundación Española para la Ciencia y la Tecnología.
Izaskun Lacunza. Coordinadora de la Oficina C en la Fundación Española para la Ciencia y la Tecnología.
Maite Iriondo de Hond. Técnica de evidencia científica y tecnológica.
Rüdiger Ortiz-Álvarez. Técnico de evidencia científica y tecnológica.
Sofía Otero. Técnica de evidencia científica y tecnológica.
Jose L. Roscales*. Técnico de evidencia científica y tecnológica.
Cristina Fernández-García. Técnica de conexión con la comunidad científica y la sociedad.

*Personas de contacto para este informe.

Bibliografía

1. Nai Fovino I, Barry G, Chaudron S, et al. Cybersecurity, our digital anchor. EUR 30276 EN, Publications Office of the European Union. Luxemburgo. 2020; https://doi.org/10.2760/352218.

2. Gobierno de España. España Digital 2025. 2020.

3. Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. 2016.

4. Reglamento (UE) 2019/881 del Parlamento Europeo y de la Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n. o 526/2013 («Reglamento sobre la Ciberseguridad»). 2019.

5. Cortes Generales. Aprobación por La Comisión Mixta de Seguridad Nacional del informe de La Ponencia para el estudio de diversas cuestiones relativas a la ciberseguridad en España, creada en el seno de la Comisión Mixta de Seguridad Nacional. Ponencia de estudio. 2019.

6. Departamento de Seguridad Nacional. Gobierno de España. Estrategia Nacional de Ciberseguridad 2019. 2019.

7. Observaciber. Cómo se protege a la ciudadanía ante los ciberriesgos. Estudio sobre percepción y nivel de confianza en España. 2022.

8. World Economic Forum. Global risks report 2022. 17th Edition. 2022.

9. Leukfeldt R, Holt TJ. The Human factor of cybercrime. Routledge; 2019.

10. CCN-CERT. Centro Criptológico Nacional. Ministerio de Defensa. Gobierno de España. Ciberamenazas y tendencias. Edición 2021. 2021.

11. Nai Fovino I, Neisse R, Hernández Ramos JL, et al. A Proposal for a European cybersecurity taxonomy. EUR 29868, Publications Office of the European Union, Luxembourg. 2019; https://doi.org/10.2760/106002.

12. González Fuster G, Jasmontaite L. Cybersecurity regulation in the European Union: the digital, the critical and fundamental rights. En: The ethics of cybersecurity. (Christen M, Gordijn B, Loi M. eds). The International Library of Ethics, Law, and Technology Springer International Publishing: Cham; 2020; pp. 97–115; https://doi.org/10.1007/978-3-030-29053-5_5.

13. European Union Agency for Network and Information Security (ENISA). Definition of cybersecurity. Gaps and overlaps in standardisation. 2015; https://doi.org/10.2824/4069.

14. Arroyo Guardeño D, Gayoso Martínez V, Hernández Encinas L. Ciberseguridad. CSIC; 2019.

15. Departamento de Seguridad Nacional. Plan Nacional de Ciberseguridad. 2022.

16. Departamento de Seguridad Nacional. Informe Anual de Seguridad Nacional 2021. 2022.

17. Instituto Nacional de Ciberseguridad (INCIBE). Balance de ciberseguridad 2021. 2021.

18. Observaciber. Ciberseguridad en Cifras. 2022. Disponible en: https://observaciber.es/#encifras [Último acceso: 18/04/2022].

19. Observaciber. Indicadores sobre confianza digital y ciberseguridad en España y la Unión Europea. 2021.

20. GañánCH, CiereM, vanEetenM. BeyondthePrettyPenny: The economic impact of cybercrime. En: Proceedings of the 2017 new security paradigms workshop. NSPW 2017 Association for computing machinery: New York, NY, USA; 2017; pp. 35–45; https://doi.org/10.1145/3171533.3171535.

21. Anderson R, Barton C, Bohme R, et al. Measuring the Changing Cost of Cybercrime. The 2019 workshop on the economics of information security, Boston, US. 2019.

22. Observaciber. Análisis y diagnóstico del talento de ciberseguridad en España. 2022.

23. Kott A, Linkov I. Cyber Resilience of systems and networks. Risk, Systems and Decisions (RSD). Springer; 2019.

24. van der Kleij R, Leukfeldt R. Cyber Resilient behavior: integrating human behavioral models and resilience engineering capabilities into cyber security. En: Advances in human factors in cybersecurity. (Ahram T, Karwowski W. eds). Advances in Intelligent Systems and Computing Springer International Publishing: Cham; 2020; pp. 16–27; https://doi.org/10.1007/978-3-030-20488-4_2.

25. Comisión Europea. Comunicación conjunta al Parlamento Europeo y al Consejo. Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE. JOIN(2017) 450 final. 2017.

26. Centro Criptológico Nacional. Ministerio de Defensa. Gobierno de España. Aproximación al marco de gobernanza de la ciberseguridad. 2022.

27. Anderson R, Baqer K. Reconciling Multiple Objectives – Politics or markets? En: Security protocols XXV. (Stajano F, Anderson J, Christianson B, et al. eds). Lecture Notes in Computer Science Springer International Publishing: Cham; 2017; pp. 144–156; https://doi.org/10.1007/978-3-319-71075-4_17.

28. Scientific Advice Mechanism (SAM), European Commission, Directorate-General for Research and Innovation. Cybersecurity in the European digital single market. 2017; https://doi.org/10.2777/466885

29. Dodge C, Burruss G. Policing Cybercrime: responding to the growing problem and considering future solutions. En: The human factor of cybercrime. Routledge; 2019.

30. López Peláez A, Erro-Garcés A, Pinilla García FJ, et al. Working in the 21st Century. The coronavirus crisis: a driver of digitalisation, teleworking, and innovation, with unintended social consequences. Information 2021;12(9):377; https://doi.org/10.3390/info12090377.

31. Gavrila Gavrila S, de Lucas Ancillo A. COVID-19 as an entrepreneurship, innovation, digitization and digitalization accelerator: Spanish Internet domains registration analysis. Br Food J 2021;123(10):3358–3390; https://doi.org/10.1108/BFJ-11-2020-1037.

32. Écija Á. El ciberespacio, un mundo sin ley. Wolters Kluwer. 2017.

33. Barrio Andrés M. Derecho Público e Internet: la actividad administrativa de regulación de la red. Instituto Nacional de Administración Pública; 2017.

34. Hernández-Ramos JL, Geneiatakis D, Kounelis I, et al. Toward a data-driven society: a technological perspective on the development of cybersecurity and data-protection policies. IEEE Secur Priv 2020;18(1):28–38; https://doi.org/10.1109/MSEC.2019.2939728.

35.Sánchez-CorcueraR,Núñez-MarcosA,Sesma-Solance J, et al. Smart cities survey: technologies, application domains and challenges for the cities of the future. Int J Distrib Sens Netw 2019;15(6):1550147719853984; https://doi.org/10.1177/1550147719853984.

36. Dawson M, Bacius R, Gouveia LB, et al. Understanding the challenge of cybersecurity in critical infrastructure sectors. Land Forces Acad Rev 2021;26(1):69–75; https://doi.org/10.2478/raft-2021-0011.

37. Tessari P, Muti K. Strategic or critical infrastructures, a way to interfere in Europe: state of play and recommendations. Policy Department. 2021.

38. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. 2011.

39. . Comunicación Conjunta al Parlamento Europeo y al Consejo. La Estrategia de Ciberseguridad de La UE para la década digital. JOIN/2020/18 Final. 2020.

40. Beeson H. Cyber security of UK infrastructure. POST Office. UK Parliament. 2017.

41. Rubio JE, Alcaraz C, Roman R, et al. Current cyber-defense trends in industrial control systems. Comput Secur 2019;87:101561; https://doi.org/10.1016/j.cose.2019.06.015

42. Alcaraz C, Zeadally S. Critical infrastructure protection: requirements and challenges for the 21st century. Int J Crit Infrastruct Prot 2015;8:53–66; https://doi.org/10.1016/j.ijcip.2014.12.002.

43. Roshanaei M. Resilience at the core: critical infrastructure protection challenges, priorities and cybersecurity assessment strategies. J Comput Commun 2021;9(8):80–102; https://doi.org/10.4236/jcc.2021.98006.

44. Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. 2018.

45. Dirección General de Coordinación y Estudios. Secretaría de Estado de Seguridad. Informe sobre la cibercriminalidad en España. 2021.

46. Lecuit JA. Hacia la fusión entre la ciberseguridad industrial y los sistemas de información corporativos. Real Instituto Elcano. 2019.

47. Stellios I, Kotzanikolaou P, Psarakis M, et al. A Survey of IoT-enabled cyberattacks: assessing attack paths to critical infrastructures and services. IEEE Commun Surv Tutor 2018;20(4):3453–3495; https://doi.org/10.1109/COMST.2018.2855563.

48. Makrakis GM, Kolias C, Kampourakis G, et al. Industrial and critical infrastructure security: technical analysis of real-life security incidents. 2022.; https://doi.org/10.1109/ACCESS.2021.3133348 .

49. Instituto Nacional de Ciberseguridad (INCIBE), Ministerio de Economía y Empresas. Gobierno de España. Estudio de tendencias en ciberseguridad. Ciberseguridad en sistemas de control industrial IC/SCADA.

50. Fischer-Hübner S, Alcaraz C, Ferreira A, et al. Stakeholder perspectives and requirements on cybersecurity in Europe. J Inf Secur Appl 2021;61:102916; https://doi.org/10.1016/j.jisa.2021.102916.

51. Bécue A, Praça I, Gama J. Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities. Artif Intell Rev 2021;54(5):3849–3886; https://doi.org/10.1007/s10462-020-09942-2.

52. European Union Agency for Network and Information Security (ENISA). Threat landscape for supply chain attacks. ENISA 2021; https://doi.org/10.2824/168593.

53. Ghadge A, Weiß M, Caldwell ND, et al. Managing cyber risk in supply chains: a review and research agenda. Supply Chain Manag Int J 2019;25(2):223240; https://doi.org/10.1108/SCM-10-2018-0357.

54. Tsvetanov T, Slaria S. The effect of the Colonial Pipeline shutdown on gasoline prices. Econ Lett 2021;209:110122; https://doi.org/10.1016/j.econlet.2021.110122.

55. Willett M. Lessons of the SolarWinds Hack. Survival 2021;63(2):7–26; https://doi.org/10.1080/00396338.2021.1906001.

56. Gutiérrez JL, Jiménez FS, Sánchez DH, et al. Estudio sobre la cibercriminalidad en España. Ministerio del Interior. Gobierno de España. 2020;62.

57. Ferraris D, Fernandez-Gago C, Lopez J. A model-driven approach to ensure trust in the IoT. Hum-Centric Comput Inf Sci 2020;10(1):50; https://doi.org/10.1186/s13673-020-00257-3.

58. Lecuit JA. Cifrado, IoT y RGPD: tres desafíos de Ciberseguridad en 2018. Real Instituto Elcano. 2018.

59. Europe's Internet of Things Policy. Shaping Europe's Digital Future. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy [Último acceso: 12/06/2022].

60. Khanna A, Kaur S. Internet of Things (IoT), Applications and challenges: a comprehensive review. Wirel Pers Commun 2020;114(2):1687–1762; https://doi.org/10.1007/s11277-020-07446-4 .

61. Tawalbeh L, Muheidat F, Tawalbeh M, et al. IoT privacy and security: challenges and solutions. Appl Sci 2020;10(12):4102; https://doi.org/10.3390/app10124102.

62. de Fuentes JM, Gonzalez-Manzano L, Lopez J, et al. Editorial: Security and privacy in internet of things. Mob Netw Appl 2019;24(3):878–880; https://doi.org/10.1007/s11036-018-1150-8.

63. Molina Castro F, Facca FM, Heijnen A, et al. A roadmap for the next-generation IoT in Europe. Shaping Europe's Digital Future.

64. Scarfò A. Chapter 3 - The cyber security challenges in the IoT era. En: Security and resilience in intelligent data-centric systems and communication networks. (Ficco M, Palmieri F. eds). Intelligent Data-Centric Systems Academic Press; 2018; pp. 53–76; https://doi.org/10.1016/B978-0-12-811373-8.00003-3.

65. Dangi R, Lalwani P, Choudhary G, et al. Study and investigation on 5G technology: a systematic review. Sensors 2022;22(1):26; https://doi.org/10.3390/s22010026.

66. Zambrini R, Rius G, Bausells J, et al. White paper on digital and complex information. Libro blanco Consejo Superior de Investigaciones Científicas (CSIC) 10. Consejo Superior de Investigaciones Científicas (España); 2020.

67. Sunyaev A. Cloud computing. En: Internet computing: principles of distributed systems and emerging Internet-based technologies. (Sunyaev A. ed) Springer International Publishing: Cham; 2020; pp. 195–236; https://doi.org/10.1007/978-3-030-34957-8_7.

68. European Court of Auditors. Special report 03/22: 5G roll-out in the EU. 2022.

69. Jiang W, Han B, Habibi MA, et al. The road towards 6G: a comprehensive survey. IEEE Open J Commun Soc 2021;2:334–366; https://doi.org/10.1109/OJCOMS.2021.3057679.

70. European Commission. Europe launches first large-scale 6G research and innovation programme. Shaping Europe's Digital Future. 2021. Disponible en: https://digital-strategy.ec.europa.eu/en/news/europe-launches-first-large-scale-6g-research-and-innovation-programme [Último acceso: 7/9/2022].

71. La Moncloa. El Gobierno lanza una nueva convocatoria de ayudas para impulsar la investigación y el desarrollo de la tecnología 6G. 2022. Disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/asuntos-economicos/Paginas/2022/180822_ayudas-unico-6g.aspx [Último acceso: 7/9/2022].

72. Hernández Encinas L, Martínez Martínez R, Baturone I, et al. Trust and security in the digital information. En: White paper on digital and complex information. CSIC Scientific Challenges: Towards 2030 CSIC España; 2020.

73. European Union Agency for Network and Information Security (ENISA). Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics. ENISA 2015; https://doi.org/10.2824/641480.

74. Wiener M, Saunders C, Marabelli M. Big-data business models: A critical literature review and multiperspective research framework. J Inf Technol 2020;35(1):66–91; https://doi.org/10.1177/0268396219896811.

75. Stadler T, Troncoso C. Why the search for a privacy-preserving data sharing mechanism is failing. Nat Comput Sci 2022;2(4):208–210; https://doi.org/10.1038/s43588-022-00236-x.

76. Madiega T. Think Tank, European Parliament. Digital sovereignty for Europe. 2020.

77. Hummel P, Braun M, Tretter M, et al. Data sovereignty: a review. Big Data Soc 2021;8(1):2053951720982012; https://doi.org/10.1177/2053951720982012.

78. European Union Agency for Network and Information Security (ENISA). ENISA Threat Landscape 2021. 2021; https://doi.org/10.2824/324797.

79. European Union Agency for Law Enforcement Cooperation. IOCTA 2021: Internet organised crime threat assessment 2021. Publications Office: LU; 2021.

80. Akyazi U. Measuring cybercrime as a service (CaaS) offerings in a cybercrime forum. 2021;14.

81. Moneva A, Leukfeldt ER, Klijnsoon W. Alerting consciences to reduce cybercrime: a quasi-experimental design using warning banners. J Exp Criminol 2022; https://doi.org/10.1007/s11292-022-09504-2.

82. Noroozian A, Korczyński M, Gañan CH, et al. Who gets the boot? Analyzing victimization by DDoS-as-a-Service. En: Research in attacks, intrusions, and defenses. (Monrose F, Dacier M, Blanc G, et al. eds). Lecture Notes in Computer Science Springer International Publishing: Cham; 2016; pp. 368–389; https://doi.org/10.1007/978-3-319-45719-2_17.

83. West C, Harriss L. Cyber security of consumer devices. POST Office. UK Parliament; 2019.

84. Instituto Nacional de Ciberseguridad (INCIBE). Botnet. Fichas técnicas. 2020. Disponible en: https://www.incibe.es/aprendeciberseguridad/botnet [Último acceso: 13/06/2022].

85. Instituto Nacional de Ciberseguridad (INCIBE). Enfrentándonosalransomware.2015. Disponibleen: https://www.incibe-cert.es/blog/enfrentandonosransomware [Último acceso: 13/06/2022].

86. Instituto Nacional de Ciberseguridad (INCIBE). Phishing. 2020. Disponible en: https://www.incibe.es/aprendeciberseguridad/phishing [Último acceso: 13/06/2022].

87. Kaspersky. ¿Qué es una amenaza avanzada persistente (APT)? 2022. Disponible en: https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats [Último acceso: 13/06/2022].

88. Cazorla L, Alcaraz C, Lopez J. Cyber stealth attacks in critical information infrastructures. IEEE Syst J 2018;12(2):1778–1792; https://doi.org/10.1109/JSYST.2015.2487684.

89. European Commission. Cybercrime. 2022. Disponible en: https://ec.europa.eu/home-affairs/cybercrime_en [Último acceso: 10/05/2022].

90. Kemp S, Miró-Llinares F, Moneva A. The dark figure and the cyber fraud rise in Europe: evidence from Spain. Eur J Crim Policy Res 2020;26(3):293–312; https://doi.org/10.1007/s10610-020-09439-2.

91. Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el real decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. 2021.

92. Centro Criptológico Nacional. Ministerio de Defensa. Gobierno de España. Hacktivismo y ciberyihadismo. Informe Anual 2021. CCN-CERT IA-0322 2021;42.

93. Buchan R, Navarrete I. Cyber espionage and international law. Res Handb Int Law Cyberspace 2021.

94. Cornish P. The Oxford Handbook of cyber security. Oxford University Press; 2021.

95. Candau J. Ciberespionaje, una amenaza al desarrollo económico y la defensa. Seguritecnia 2019.

96. Pastrana S, Hutchings A, Caines A, et al. Characterizing Eve: Analysing cybercrime actors in a large underground forum. En: Research in attacks, intrusions, and defenses. (Bailey M, Holz T, Stamatogiannakis M, et al. eds) Springer International Publishing: Cham; 2018; pp. 207–227; https://doi.org/10.1007/978-3-030-00470-5_10.

97. Lecuit JA. Ciberseguridad: marco jurídico y operativo. Real Inst Elcano ARI 512017 2017.

98. Murray C, Srivastava M. How Conti ransomware group crippled Costa Rica — Then fell apart. Financ Times 2022.

99. Google. La ciberseguridad en España: una perspectiva desde las pymes, sociedad civil y administración pública. 2019.

100. LecuitJA.Ciberseguridad,privacidadeinterceptación legal en las redes 5G: una realidad poliédrica. 2020.

101. Arteaga F. Ciberseguridad: la consolidación de la cooperación público-privada. Real Inst Elcano 2022.

102. Agrafiotis I, Nurse JRC, Goldsmith M, et al. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. J Cybersecurity 2018;4(1); https://doi.org/10.1093/cybsec/tyy006.

103. Bada M, Nurse JRC. Chapter 4 - The social and psychological impact of cyberattacks. En: Emerging cyber threats and cognitive vulnerabilities. (Benson V, Mcalaney J. eds) Academic Press; 2020; pp. 73–92; https://doi.org/10.1016/B978-0-12-816203-3.00004-6.

104. Modic D, Anderson R. It's all over but the crying: the emotional and financial impact of internet fraud. IEEE Secur Priv 2015;13(5):99–103; https://doi.org/10.1109/MSP.2015.107.

105. Budapest Convention. Disponible en: https://www.coe.int/en/web/cybercrime/the-budapest-convention [Último acceso: 14/06/2022].

106. Jefatura del Estado. Instrumento de ratificación del Convenio sobre la ciberdelincuencia, hecho En Budapest El 23 de noviembre de 2001. 2010.

107. Ministerio de Asuntos Exteriores, Unión Europea y Cooperación. España firma segundo protocolo adicional al Convenio de Budapest. 2022. Disponible en: https://www.exteriores.gob.es/RepresentacionesPermanentes/ConsejodeEuropa/es/Comunicacion/Noticias/Paginas/Articulos/Espa%C3%B1a-firma-el-Segundo-Protocolo-Adicional-al-Convenio-de-Budapest.aspx [Último acceso: 20/09/2022].

108. Proposal for a Council Decision authorising member states to ratify, in the interest of the European Union, the second additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. 2021.

109. Asamblea General de las Naciones Unidas. Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. 2021.

110. Asamblea General de las Naciones Unidas. Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. 2021.

111. Organización para la Seguridad y la Cooperación en Europa 10 March 2016, Consejo Permanente. Decisión No 1202. Medidas de la OSCE para el fomento de la confianza destinadas a reducir los riesgos de conflicto dimanantes del uso de la tecnología de información y de la comunicación. 2016.

112. Schmitt MN. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd ed. Cambridge University Press: Cambridge; 2017.; https://doi.org/10.1017/9781316822524.

113. Paris Call for Trust and Security in Cyberspace — Paris Call. Disponible en: https://pariscall.international/en/ [Último acceso: 06/09/2022].

114. Grupo de Reflexión AMETIC. Soberanía tecnológica y soberanía digital. Ametic Voz Ind Digit 2022.

115. Agencia de la Unión Europea para la Ciberseguridad (ENISA). Acerca de ENISA. About ENISA. 2022. Disponible en: https://www.enisa.europa.eu/about-enisa/about/es [Último acceso: 26/09/2022].

116. CERT-EU - About Us. Disponible en: https://cert.europa.eu/about-us [Último acceso: 06/10/2022].

117. 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). 2016.

118. European Cyber Security Organisation (ECSO). About ECSO. 2022. Disponible en: http://www.ecs-org.eu [Último acceso: 01/03/2022].

119. 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. 2020.

120. Propuesta de reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos (Ley de gobernanza de datos). 2020.

121. European Commission. Commission welcomes agreement on new rules on cybersecurity. Press Release. 2022. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985 [Último acceso: 15/06/2022].

122. Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.o 1060/2009, (UE) n.o 648/2012, (UE) n.o 600/2014 y (UE) n.o 909/2014. 2020.

123. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.o 910/2014 en lo que respecta al establecimiento de un Marco para una identidad digital europea. 2021.

124. Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales). 2020.

125. Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se modifica la Directiva 2000/31/CE. 2020.

126. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. 2021.

127. Comisión Europea. Cyber resilience act, shaping Europe's digital future. Regulación. 2022. Disponible en: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act [Último acceso: 22/09/2022].

128. Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre normas armonizadas para un acceso justo a los datos y su utilización (Ley de Datos). 2022.

129. European Cybersecurity Competence Centre and Network. Disponible en: https://cybersecurity-centre.europa.eu/index_en [Último acceso: 26/05/2022].

130. Reglamento (UE) 2021/ del Parlamento Europeo y del Consejo, de 20 de mayo de 2021, por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación. 2021.

131. PAe - El CNS designa a INCIBE como Centro de Coordinación Nacional del Centro Europeo de Competencia en Ciberseguridad. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2022/Septiembre/Noticia-2022-09-30-CSN-designa-INCIBE-Centro-Coordinacion-Europeo-Ciberseguridad.html [Último acceso: 10/6/2022].

132. European Court of Auditors. Challenges to effective EU cybersecurity policy. Brief Pap 2019;74.

133. Dutton WH, Creese S, Esteve-González P, et al. Next steps for the EU: building on the Paris call and EU cybersecurity strategy. Available at SSRN 4052728. 2022.

134. Creese S, Dutton WH, Esteve-González P, et al. The Solution is in the details: Building cybersecurity capacity in Europe. Available at SSRN 4178109. 2022.

135. Sterlini P, Massacci F, Kadenko N, et al. Governance challenges for European cybersecurity policies: stakeholder views. IEEE Secur Priv 2020;18(1):46–54; https://doi.org/10.1109/MSEC.2019.2945309.

136. CCN-CERT. Centro Criptológico Nacional. Ministerio de Defensa. Gobierno de España. Aproximación española a la ciberseguridad. 2019.

137. Del-Real C, Díaz-Fernández AM. Understanding the plural landscape of cybersecurity governance in Spain: a matter of capital exchange. Int Cybersecurity Law Rev; Aceptado.

138. Estado de Israel. Prime Minister's Office. National Cyber Directorate. Israel national cyber security strategy in brief. 2017.

139. Del-Real C. La gobernanza de la ciberseguridad en España: un estudio empírico de los actores, redes de colaboración y prospectiva desde las teorías de la seguridad plural. http://purl.org/dc/dcmitype/Text. Universidad de Cádiz; 2021.

140. LecuitJA.LarevisióndelaEstrategiadeCiberseguridad Nacional: una visión desde el sector privado. Real Inst Elcano 2019.

141. Cavan S. Cybersecurity: Changing the Model. 2019. Disponible en: https://www.atlanticcouncil.org/in-depth-research-reports/report/cybersecurity-changing-the-model/ [Último acceso: 27/07/2022].

142. Blomquist DM. Comparing centralized and decentralized cybersecurity in state and local government. M.S. Faculty of Utica College. Ann Arbor, United States; 2020.

143. Liu C-W, Huang P, Lucas HC. Centralized IT decision making and cybersecurity breaches: evidence from U.S. higher education institutions. J Manag Inf Syst 2020;37(3):758–787; https://doi.org/10.1080/07421222.2020.1790190.

144. La Moncloa. 09/03/2021. Interior aprueba un plan stratégicopararefor zarlaluchacontralacibercriminalidad [Prensa/Actualidad/Interior]. Disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Paginas/2021/090321-cibercriminalidad.aspx [Último acceso: 05/10/2022].

145. MinisteriodelaPresidenciayparalasAdministraciones Territoriales. Orden PRA/33/2018, de 22 de enero, por la que se publica el acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad. 2018.

146. Conferencia sectorial para asuntos de la Seguridad Nacional. Departamento de Seguridad Nacional. Disponible en: https://www.dsn.gob.es/es/actualidad/sala-prensa/conferencia-sectorial-para-asuntos-seguridad-nacional [Último acceso: 06/10/2022].

147. Foro Nacional de Ciberseguridad - Funciones. Disponible en: https://foronacionalciberseguridad.es/index.php/sobre-el-foro/funciones [Último acceso: 02/09/2022].

148. Centro Criptológico Nacional (CCN). Disponible en: https://www.ccn-cert.cni.es/sobre-nosotros/centro-criptologico-nacional.html [Último acceso: 15/06/2022].

149. Boletín Oficial Del Estado. Real Decreto 311/2022, de 3 de Mayo, por el que se regula el esquema nacional de seguridad.

150. Instituto Nacional de Ciberseguridad (INCIBE). Qué es INCIBE. 2016. Disponible en: https://www.incibe.es/que-es-incibe [Último acceso: 15/06/2022].

151. Mando Conjunto Del Ciberespacio (MCCE) - EMAD. Disponible en: https://emad.defensa.gob.es/unidades/mcce/ [Último acceso: 03/03/2022].

152. Directiva 2013/40/UE Del Parlamento Europeo y Del Consejo, de 12 de Agosto de 2013, Relativa a los ataques contra los sistemas de información y por la que se sustituye la decisión marco 2005/222/JAI Del Consejo. 2013.

153. SOC-AGE - Esquema Nacional de Seguridad. Disponible en: https://ens.ccn.cni.es/es/allcategories-es-es/12-categoria-es-es/101-soc-age [Último acceso: 07/09/2022].

154. PAe - CTT - General - Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos. Disponible en: https://administracionelectronica.gob.es/ctt/verPestanaGeneral.htm?idIniciativa=ciberseguridad&idioma=es#.Y0QEYnZBw2y [Último acceso: 10/10/2022].

155. Centro de Operaciones de Seguridad de La AGE, Servicios Horizontales de Ciberseguridad. Disponible en: https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/5686-centro-de-operaciones-de-seguridad-de-la-age-servicios-horizontales-de-ciberseguridad.html [Último acceso: 07/10/2022].

156. Andalucía-CERT. Disponible en: https://csirt.es/index.php/es/miembros/andaluciacert [Último acceso: 07/10/2022].

157. CATALONIA-CERT. Disponible en: https://csirt.es/index.php/es/miembros/cataloniacert [Último acceso: 07/10/2022].

158. CSIRT-CV. Disponible en: https://csirt.es/index.php/es/miembros/csirt-cv [Último acceso: 07/10/2022].

159. Centro Vasco de Ciberseguridad. Disponible en: https://csirt.es/index.php/es/miembros/bcsc [Último acceso: 07/10/2022].

160. Red Nacional de SOC. Disponible en: https://rns.ccn-cert.cni.es/es/ [Último acceso: 21/04/2022].

161. Comisaría General de Policía Judicial; Policía Nacional; Conócenos. Disponible en: https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial.php [Último acceso: 10/10/2022].

162. CCN-CERT. Centro Criptológico Nacional. Ministerio de Defensa. Gobierno de España. Aproximación del CCN-CERT: desarrollando la Red Nacional de SOC. 2021.

163. UCIBER - Mossos d'Esquadra. Disponible en: https://www.csirt.es/index.php/es/miembros/uciber-mossos-d-esquadra [Último acceso: 07/10/2022].

164. Ertzaintza SCDTI. Disponible en: https://csirt.es/index.php/es/miembros/ertzaintza-scdti [Último acceso: 07/10/2022].

165. Ministerio Del Interior. Dirección General de Coordinación y Estudios. Disponible en: https://www.interior.gob.es/opencms/es/el-ministerio/funciones-y-estructura/secretaria-de-estado-de-seguridad/direccion-general-de-coordinacion-y-estudios/ [Último acceso: 22/09/2022].

166. Esquema Nacional de Seguridad (ENS) 2022. Evolución del panorama de la ciberseguridad. 2022.

167. Boletín Oficial Del Estado. Código de Derecho de La Ciberseguridad. Disponible en: https://www.boe.es/biblioteca_juridica/codigos/codigo.php?modo=2&id=173_Codigo_de_Derecho_de_la_Ciberseguridad [Último acceso: 07/06/2022].

168. Foro Nacional de Ciberseguridad - Regulación. GT 5 Regulación. Disponible en: https://foronacionalciberseguridad.es/index.php/grupos-de-trabajo/regulacion [Último acceso: 20/09/2022].

169. Europeans' attitudes towards cyber security (Cybercrime) - Enero 2020 - - Eurobarometer Survey. Disponible en: https://europa.eu/eurobarometer/surveys/detail/2249 [Último acceso: 18/05/2022].

170. European citizens' knowledge and attitudes towards science and technology. Special Eurobarometer. European Comission; 2021.

171. International Communication Union. Global Cybersecurity Index 2020. 2020.

172. European Commission. The Digital Economy and Society Index (DESI). Shaping Europe's Digital Future. 2021. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/desi [Último acceso: 26/05/2022].

173. European Union Agency for Network and Information Security (ENISA). Public Private Partnerships (PPPs). Disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps [Último acceso: 13/06/2022].

174. Christensen KK, Petersen KL. Public–private partnerships on cyber security: a practice of loyalty. Int Aff 2017;93(6):1435–1452; https://doi.org/10.1093/ia/iix189.

175. Calcara A, Marchetti R. State-industry relations and cybersecurity governance in Europe. Rev Int Polit Econ 2021;0(0):1–26; https://doi.org/10.1080/09692290.2021.1913438.

176. Fayi SYA. What Petya/NotPetya ransomware is and what its remidiations are. En: Information Technology - New Generations. (Latifi S. ed). Advances in Intelligent Systems and Computing Springer International Publishing: Cham; 2018; pp. 93–100; https://doi.org/10.1007/978-3-319-77028-4_15.

177. Massacci F, Vidor S. Building principles for lawful cyber lethal autonomous weapons. IEEE Secur Priv 2022;20(2):101–106; https://doi.org/10.1109/MSEC.2022.3143269.

178. The EU Cyber Diplomacy Toolbox. Disponible en: https://www.cyber-diplomacy-toolbox.com/ [Último acceso: 23/09/2022].

179. Kavanagh C. Ukraine: Cyber operations and digital technologies. 2022. Disponible en: https://directionsblog.eu/ukraine-cyber-operations-and-digital-technologies/ [Último acceso: 20/04/2022].

180. Salt A, Sobchuk M. Russian cyber-operations in Ukraine and the Implications for NATO. 2021.

181. La Moncloa. 29/03/2022. El Gobierno aprueba el Plan Nacional de respuesta a las consecuencias de la guerra en Ucrania [Consejo de Ministros/Resúmenes]. Disponible en: https://www.lamoncloa.gob.es/consejodeministros/resumenes/Paginas/2022/290322-rp-cministros.aspx [Último acceso: 08/06/2022].

182. Derian-Toth G, Walsh R, Sergueeva A, et al. Opportunities for public and private attribution of cyber operations. Tallin Pap 2021.

183. Arteaga F. Capacidades ofensivas, disuasión y ciberdefensa. Real Instituto Elcano 2019.

184. Davis JK. Developing applicable standards of proof for peacetime cyber attribution. Tallinn Paper. The NATO Cooperative Cyber Defence Centre of Excellence. 2022.

185. Arteaga F. Ciberseguridad: llegan las acciones ofensivas. Real Inst Elcano 2018.

186. Kaminska MK. Restraint under conditions of uncertainty: why the United States tolerates cyberattacks. J Cybersecurity 2021;7(1); https://doi.org/10.1093/cybsec/tyab008.

187. Wagner TD, Mahbub K, Palomar E, et al. Cyber threat intelligence sharing: Survey and research directions. Comput Secur 2019;87:101589; https://doi.org/10.1016/j.cose.2019.101589.

188. Preuveneers D, Joosen W, Bernal Bernabe J, et al. Distributed security framework for reliable threat intelligence Sharing. Secur Commun Netw 2020;2020:1–15; https://doi.org/10.1155/2020/8833765.

189. European Union Agency for Network and Information Security (ENISA). Coordinated vulnerability disclosure policies in the EU. News Item. Disponible en: https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu [Último acceso: 03/06/2022].

190. Instituto Nacional de Ciberseguridad (INCIBE). Política de reporte de vulnerabilidades. 2017. Disponible en: https://www.incibe-cert.es/sobre-incibe-cert/politica-reporte-vulnerabilidades [Último acceso: 03/06/2022].

191. Instituto Nacional de Ciberseguridad (INCIBE). Asignación y publicación de CVE. 2022. Disponible en: https://www.incibe-cert.es/asignacion-publicacion-cve [Último acceso: 06/10/2022].

192. Instituto Nacional de Ciberseguridad (INCIBE). Vulnerabilidades. Disponible en: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades [Último acceso: 06/10/2022].

193. Instituto Nacional de Ciberseguridad (INCIBE). Estudio de tendencias en ciberseguridad. Hacking ético. 2016.

194. Del-RealC, Rodríquez-MesaMJ. Fromblacktowhite:the regulation of ethical hacking in Spain. Inf Commun Technol Law ;Aceptado; https://doi.org/10.1080/13600834.2022.2132595.

195. Instituto Nacional de Ciberseguridad (INCIBE). Estudio de tendencias en ciberseguridad. Distribución de ciberinteligencia. 2016.

196. CCN-CERT. Centro Criptológico Nacional. Ministerio de Defensa. Reyes. Defensa frente a las amenazas. Disponible en: https://www.ccn-cert.cni.es/herramientas-ciberseguridad-2/reyes.html [Último acceso: 28/06/2022].

197. Instituto Nacional de Ciberseguridad (INCIBE). ICARO. 2016. Disponible en: https://www.incibe-cert.es/servicios-operadores/icaro [Último acceso: 23/09/2022].

198. Departamento de Seguridad Nacional (DSN). Líneas de acción de carácter internacional desarrolladas en el ámbito de la ciberseguridad. 2016. Disponible en: https://www.dsn.gob.es/es/actualidad/sala-prensa/l%C3%ADneas-acci%C3%B3n-car%C3%A1cter-internacional-desarrolladas-%C3%A1mbito-ciberseguridad [Último acceso: 03/06/2022].

199. Instituto Nacional de Ciberseguridad (INCIBE). Membresías. 2016. Disponible en: https://www.incibe.es/que-es-incibe/con-quien-trabajamos/membresias [Último acceso: 06/10/2022].

200. National Institute of Standards and Technology.

U.S. Department of Commerce. NVD - Data Feeds. 2022. Disponible en: https://nvd.nist.gov/vuln/data-feeds [Último acceso: 06/10/2022].

201. Giaretta A, Dragoni N, Massacci F. IoT security configurability with security-by-contract. Sensors 2019;19(19):4121; https://doi.org/10.3390/s19194121.

202. Bouwmeester B, Rodríguez E, Gañán C, et al. ``The thing doesn't have a name'': learning from emergent real-world interventions in smart home security. USENIX. 2021.

203. European Commission. Study on the need of cybersecurity requirements for ICT products. No. 2020-0715. 2021.

204. Edler J, Blind K, Frietsch R, et al. Technology sovereignty. From demand to concept. Fraunhofer Inst Syst Innov Res ISI 2020.

205. European Commission. NIS Cooperation Group. Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures. Shaping Europe's Digital Future. 2020. Disponible en: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures [Último acceso: 01/06/2022].

206. Recomendación (UE) 2019/534 de la Comisión, de 26 de marzo de 2019, Ciberseguridad de las redes 5G. 2019.

207. Boletín Oficial del Estado. Real Decreto-Ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones Electrónicas de Quinta Generación. 2022.

208. Arteaga F. La UE: a la búsqueda de la soberanía digital. Real Inst Elcano 2020.

209. Cagnin C, Muench S, Scapolo F, et al. Shaping and securing the EU's open strategic autonomy by 2040 and beyond. 2021.; https://doi.org/10.2760/414963.

210. CyberSec4Europe. Research Challenges and Requirements for Secure Software Development. D 3.9. 2019.

211. Siddhanti P, Asprion P, Schneider B. Cybersecurity by design for smart home environments: En: Proceedings of the21stInternationalConferenceonEnterpriseInformation Systems SCITEPRESS - Science and Technology Publications: Heraklion, Crete, Greece; 2019; pp. 587–595; https://doi.org/10.5220/0007709205870595.

212. Unal DB, Brunt R. Cybersecurity by design in civil nuclear power plants. Policy Commons 2019.

213. Strategic programs for advanced research and technology in Europe (SPARTA). Security-by-design framework for the intelligent infrastructure. D6.1. 2020.

214. Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending regulation (EU) 2019/1020. 2022. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52022PC0454 [Último acceso: 10/10/2022].

215. Directorate-General for Communications Networks C and T (European C, Blind K, Pätsch S, et al. Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, Blind, K., Pätsch, S., Muto, S., et al., The impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy : Final Study Report, Publications Office, 2021, Https://Data.Europa.Eu/Doi/10.2759/430161. Publications Office of the European Union: LU; 2021.

216. Strategic programs for advanced research and technology in Europe (SPARTA). International and national cybersecurity certification initiatives. D11.1. 2020.

217. Matheu SN, Hernández-Ramos JL, Skarmeta AF, et al. A Survey of cybersecurity certification for the Internet of Things. ACM Comput Surv 2021;53(6):1–36; https://doi.org/10.1145/3410160.

218. Matheu SN, Hernández-Ramos JL, Skarmeta AF. Toward a cybersecurity certification framework for the Internet of Things. IEEE Secur Priv 2019;17(3):66–76; https://doi.org/10.1109/MSEC.2019.2904475.

219. Hernández-Ramos JL, Matheu SN, Skarmeta A. The challenges of software cybersecurity certification [Building Security In]. IEEE Secur Priv 2021;19(1):99–102; https://doi.org/10.1109/MSEC.2020.3037845.

220. European Commission. Cybersecurity Certification Framework. Shaping Europe's Digital Future. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework [Último acceso: 11/03/2022].

221. Foro Nacional de Ciberseguridad. Informe Global de Trabajos Realizados. 2022.

222. Deloitte. El estado de la ciberseguridad en España. Post pandemia: un camino inexplorado. 2022.

223. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de Las Regiones. Estrategia de La UE en materia de normalización para establecer normas mundiales para apoyar un mercado único de La Unión resiliente, ecológico y digital. COM(2022) 31 Final. 2022.

224. European Union Agency for Network and Information Security (ENISA). Cybersecurity certification: candidate EUCC scheme. 2020. Disponible en: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme [Último acceso: 08/04/2022].

225. European Parliament. Directorate General for Parliamentary Research Services. Achieving a sovereign and trustworthy ICT industry in the EU. Publications Office: LU; 2017.

226. European Union Agency for Network and Information Security (ENISA). Cloud certification scheme: building trusted cloud services across Europe. Disponible en: https://www.enisa.europa.eu/news/enisa-news/cloud-certification-scheme [Último acceso: 12/06/2022].

227. European Union Agency for Network and Information Security(ENISA).SecuringEU's Visionon5G:Cybersecurity Certification. Disponible en: https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification [Último acceso: 6/12/2022].

228. European Cyber Security Organisation (ECSO) EW. European cyber security certification: a meta-scheme approach v1.0. 2017.

229. European Cyber Security Organisation (ECSO). European cyber security certification assessment options WG1. Standardisation, certification, labelling and supply chain management. 2019.

230. European Commission. Cyber Resilience Act – New cybersecurity rules for digital products and ancillary services. 2022. Disponible en: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en [Último acceso: 04/10/2022].

231. European Commission. Cyber Resilience Act

- Factsheet. Shaping Europe's Digital Future. 2022. Disponible en: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet [Último acceso: 05/10/2022].

232. OC-CCN. Organismo de Certificación - Centro Criptológico Nacional. Organismo de Certificación

- Catálogo productos STIC. Disponible en: https://oc.ccn.cni.es/catalogo-productos-stic [Último acceso: 17/10/2022].

233. Fernández BC. Cybercompliance: A legal but also ethical concept that allows to reduce the current high risks of corporations. En: Security and Defence: Ethical and legal challenges in the face of current conflicts. (Cayón Peña J. ed). Advanced Sciences and Technologies for Security Applications Springer International Publishing: Cham; 2022; pp. 73□80; https://doi.org/10.1007/978-3-030-95939-5_5.

234. Singh J, Millard C, Reed C, et al. Accountability in the IoT: systems, law, and ways forward. Computer 2018;51(7):54–65; https://doi.org/10.1109/MC.2018.3011052.

235. Al Alsadi AA, Sameshima K, Bleier J, et al. No spring chicken: quantifying the lifespan of exploits in IoT malware using static and dynamic analysis. En: Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security ACM: Nagasaki Japan; 2022;

pp. 309–321; https://doi.org/10.1145/3488932.3517408.

236. Garg V. Covenants without the sword: market incentives for cybersecurity investment. SSRN Scholarly Paper. Social Science Research Network: Rochester, NY; 2021.; https://doi.org/10.2139/ssrn.3896578.

237. Creese S, Dutton WH, Esteve-González P, et al. Cybersecurity capacity-building: cross-national benefits and international divides. J Cyber Policy 2021;6(2):214–235; https://doi.org/10.1080/23738871.2021.1979617.

238. Foro Nacional de Ciberseguridad. Informe sobre la cultura de la ciberseguridad en España. 2021.

239. Bada M, Sasse AM, Nurse JRC. Cyber Security awareness campaigns: why do they fail to change behaviour? arXiv; 2019.; https://doi.org/10.48550/arXiv.1901.02672.

240. van Steen T, Norris E, Atha K, et al. What (if any) behaviour change techniques do government-led cybersecurityawarenesscampaignsuse?JCybersecurity 2020;6(1):tyaa019; https://doi.org/10.1093/cybsec/tyaa019.

241. Corallo A, Lazoi M, Lezzi M, et al. Cybersecurity awareness in the context of the Industrial Internet of Things: a systematic literature review. Comput Ind 2022;137:103614; https://doi.org/10.1016/j.compind.2022.103614.

242. Rhee H-S, Kim C, Ryu YU. Self-efficacy in information security: Its influence on end users' information security practice behavior. Comput Secur 2009;28(8):816–826; https://doi.org/10.1016/j.cose.2009.05.008.

243. van Bavel R, Rodríguez-Priego N, Vila J, et al. Using protection motivation theory in the design of nudges to improve online security behavior. Int J Hum-Comput Stud 2019;123:29–39; https://doi.org/10.1016/j.ijhcs.2018.11.003.

244. Centro Criptológico Nacional. Ministerio de Defensa. Gobierno de España. ÁNGELES - Inicio. Disponible en: https://angeles.ccn-cert.cni.es/index.php/es/ [Último acceso: 26/05/2022].

245. Instituto Nacional de Ciberseguridad (INCIBE). Formación. 2016. Disponible en: https://www.incibe.es/protege-tu-empresa/formacion [Último acceso: 26/05/2022].

246. Instituto Nacional de Ciberseguridad (INCIBE). Políticas de seguridad para la PYME. 2017. Disponible en: https://www.incibe.es/protege-tu-empresa/herramientas/politicas [Último acceso: 26/05/2022].

247. Centro Criptológico Nacional. Ministerio de Defensa. Gobierno de España. El portal de formación, capacitación y talento del CCN, ÁNGELES, supera los 10.000 usuarios registrados. Disponible en: https://www.ccn.cni.es/index.php/es/actualidad-ccn/891-el-portal-de-formacion-capacitacion-y-talento-del-ccn-angeles-supera-los-10-000-usuarios-registrados [Último acceso: 26/05/2022].

248. Instituto Nacional de Ciberseguridad (INCIBE). Oficina de Seguridad del Internauta (OSI). Guía de ciberseguridad - La ciberseguridad al alcance de todos. 2022.

249. Instituto Nacional de Ciberseguridad (INCIBE). Experiencia senior, el nuevo programa de concienciación de INCIBE destinado a usuarios de más de 60 años. 2021. Disponible en: https://www.incibe.es/sala-prensa/notas-prensa/experiencia-senior-el-nuevo-programa-concienciacion-incibe-destinado [Último acceso: 13/07/2022].

250. Instituto Nacional de Ciberseguridad (INCIBE). Invitación pública para la colaboración en la promoción de la cultura de la ciberseguridad mediante la organización de eventos CyberCamp en España. 2021;22.

251. CCN-CERT. Centro Criptológico Nacional. ATENEA. Disponible en: https://www.ccn-cert.cni.es/soluciones-seguridad/atenea.html [Último acceso: 23/09/2022].

252. Programa Talento Hacker. España Digital 2026. Disponible en: https://espanadigital.gob.es/ca/linies-dactuacio/programa-talento-hacker [Último acceso: 06/10/2022].

253. De Zan T. Mind the gap: the cyber security skills shortage and public policy interventions. 2019.

254. European Union Agency for Network and Information Security (ENISA). Addressing skills shortage and gap through higher education. 2021; https://doi.org/10.2824/033355.

255. Comisión Europea. Índice de la economía y la sociedad digitales (DESI) 2021. España.

256. Instituto Nacional de Ciberseguridad (INCIBE). Protege tu empresa. 2016. Disponible en: https://www.incibe.es/protege-tu-empresa [Último acceso: 06/10/2022].

257. Sharl L, Goussac N, Currey E, et al. System update: towards a women, peace and cybersecurity agenda. United Nations Institute for Disarmament and Research UNDIR 2021.

258. Poster WR. Cybersecurity needs women. Nature 2018;555(7698):577–580; https://doi.org/10.1038/d41586-018-03327-w.

259. (ISC)2 Cybersecurity Workforce. Women in cybersecurity. 2019.

260. García-Holgado A, Gonzalez-González CS, Peixoto A, et al. Bridging the diversity gap: actions and experiences fostering diversity in STEM. En: Eighth International Conference on Technological Ecosystems for Enhancing Multiculturality. TEEM'20 Association for Computing Machinery: New York, NY, USA; 2020; pp. 126–129; https://doi.org/10.1145/3434780.3436714.

261. Parlamento Europeo. Textos aprobados - Lucha contra la violencia de género: la ciberviolencia - martes 14 de diciembre de 2021. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0489_ES.html [Último acceso: 07/07/2022].

262. González-González CS, Caballero-Gil P, García-Holgado A, et al. COEDU-IN Project: an inclusive co-educational project for teaching computational thinking and digital skills at early ages. En: 2021 International Symposium on Computers in Education (SIIE) 2021; pp. 1–4; https://doi.org/10.1109/SIIE53363.2021.9583648.

263. European Commission. Directorate General for Employment, Social Affairs and Inclusion., Organisation for Economic Co-operation and Development. Policy Brief on Women's Entrepreneurship. Publications Office: LU; 2016.

264. Millar K, Shires J, Tropina T. Gender Approaches to Cybersecurity: Design, defence and response. The United Nations Institute for Disarmament Research UNDIR; 2021.; https://doi.org/10.37559/GEN/21/01.

265. Instituto Nacional de Ciberseguridad (INCIBE). Formación reglada en ciberseguridad en España. Másteres, Especializaciones, Grados y Especializaciones en Formación Profesional. 2021.

266. Strategic Programs for Advanced Research and Technology in Europe SPARTA. Cybersecurity skills framework. D9.1. 2020.

267. Dragoni N, Lafuente AL, Massacci F, et al. Are we preparing students to build security in? A survey of European cybersecurity in higher education programs. IEEE Secur Priv 2021;19(01):81–88; https://doi.org/10.1109/MSEC.2020.3037446.

268. Consejo General del Poder Judicial (España), Cooperación Española. Curso la ciberdelicuencia. Tratamiento preventivo, procesal y sustantivo desde una perspectiva internacional. 2021.

269. University of Oxford. Global Cyber Security Capacity Centre. Disponible en: https://www.oxfordmartin.ox.ac.uk/cyber-security/ [Último acceso: 26/05/2022].

270. University of Leiden. Institute of Security and Global Affairs. Disponible en: https://www.universiteitleiden.nl/en/governance-and-global-affairs/institute-of-security-and-global-affairs [Último acceso: 26/05/2022].

271. Department of Computer Science and Technology: Cambridge Cybercrime Centre. Disponible en: https://www.cambridgecybercrime.uk/ [Último acceso: 06/09/2022].

272. Cavelty MD, Kavanagh C. Cybersecurity and human rights. Chapter 5: Cybersecurity and human rights. Research Handbooks in Human Rights series. 2019; Chapter 5: Cybersecurity and human rights.

273. Kavanagh C. The United Nations, Cyberspace and International Peace and Security. Responding to Complexity in the 21st Century. 2017.

274. Taddeo M. Is Cybersecurity a public good? Minds mach 2019;29(3):349–354; https://doi.org/10.1007/s11023-019-09507-5.

275. Gobierno de España. Carta de Derechos Digitales. 2021.

276. Christen M, Gordijn B, Loi M, (eds). The ethics of cybersecurity. Springer Nature; 2020.; https://doi.org/10.1007/978-3-030-29053-5.

277. Domingo-Ferrer J, Blanco-Justicia A. Ethical value-centric cybersecurity: a methodology based on a value graph. Sci Eng Ethics 2020;26(3):1267–1285; https://doi.org/10.1007/s11948-019-00138-8.

278. Floridi L. Soft ethics, the governance of the digital and the General Data Protection Regulation. Philos Trans R Soc Math Phys Eng Sci 2018;376(2133):20180081; https://doi.org/10.1098/rsta.2018.0081.

279. González Fuster G, Gutwirth S. Ethics, Law and privacy: disentangling law from ethics in privacy discourse. En: 2014 IEEE International Symposium on Ethics in Science, Technology and Engineering 2014; pp. 1–6; https://doi.org/10.1109/ETHICS.2014.6893376.

280. Tanczer L, Neira IL, Parkin S, et al. Gender and IoT research report. Lond Glob Univ 2018.

281. Lopez-Neira I, Patel T, Parkin S, et al. 'Internet of Things': How abuse is getting smarter. Domest Abuse Q 2019; 63:22–26.

282. Tanczer LM, López-Neira I, Parkin S. 'I feel like we're really behind the game': perspectives of the United Kingdom's intimate partner violence support sector on the rise of technology-facilitated abuse. J Gend-Based Violence 2021;5(3):431–450; https://doi.org/10.1332/239868021X16290304343529.

283. Meng W, Lopez J, Xu S, et al. IEEE Access Special Section Editorial: Internet-of-Things attacks and defenses: recent advances and challenges. IEEE Access 2021; 9:108846–108850; https://doi.org/10.1109/ACCESS.2021.3101889.

284. Grande E, Beltrán M. Edge-centric delegation of authorization for constrained devices in the Internet of Things. Comput Commun 2020; 160:464–474; https://doi.org/10.1016/j.comcom.2020.06.029.

285. Gamba J, Rashed M, Razaghpanah A, et al. An analysis of pre-installed android software. En: 2020 IEEE Symposium on Security and Privacy (SP) IEEE: San Francisco, CA, USA; 2020; pp. 1039–1055; https://doi.org/10.1109/SP40000.2020.00013.

286. Vidal-González S, García-Rodríguez I, Aláiz-Moretón H, et al. Analyzing IoT-based botnet malware activity with distributed low interaction honeypots. En: Trends and innovations in information systems and technologies. (Rocha Á, Adeli H, Reis LP, et al. eds). Advances in Intelligent Systems and Computing Springer International Publishing: Cham; 2020; pp. 329□338; https://doi.org/10.1007/978-3-030-45691-7_30.

287. Thakor VA, Razzaque MA, Khandaker MR. Lightweight cryptography algorithms for eesource-constrained IoT devices: A Review, Comparison and Research Opportunities. IEEE Access 2021;9; https://doi.org/10.1109/ACCESS.2021.3052867.

288. Orúe AB, Hernández Encinas L, Fernández V, et al. A review of cryptographically secure PRNGs in constrained devices for the IoT. En: International Joint Conference SOCO□17-CISIS□17-ICEUTE□17 León, Spain, September 6□8, 2017, Proceeding. (Pérez García H, Alfonso-Cendón J, Sánchez González L, et al. eds). Advances in Intelligent Systems and Computing Springer International Publishing: Cham; 2018; pp. 672–682; https://doi.org/10.1007/978-3-319-67180-2_65.

289. Matheu SN, Hernández-Ramos JL, Skarmeta A, et al. A Survey of cybersecurity certification for the Internet of Things. ACM Comput Surv CSUR 2020;53(6).

290. Rodríguez E, Verstegen S, Noroozian A, et al. User compliance and remediation success after IoT malware notifications. J Cybersecurity 2021;7(1):tyab015; https://doi.org/10.1093/cybsec/tyab015.

291. Eceiza M, Flores JL, Iturbe M. Fuzzing the Internet of Things: a review on the techniques and challenges for efficient vulnerability discovery in embedded systems. IEEE Internet Things J 2021;8(13):10390–10411; https://doi.org/10.1109/JIOT.2021.3056179.

292. Jove E, Aveleira-Mata J, Alaiz-Moretón H, et al. Intelligent one-class classifiers for the development of an intrusion detection system: the MQTT case study. Electronics 2022;11(3):422; https://doi.org/10.3390/electronics11030422.

293. Aguayo-Canela FJ, Alaiz-Moretón H, García-Ordás MT, et al. Middleware-based multi-agent development environment for building and testing distributed intelligent systems. Clust Comput 2021;24(3):2313–2325; https://doi.org/10.1007/s10586-021-03270-y.

294. Franco J, Aris A, Canberk B, et al. A survey of honeypots and honeynets for Internet of Things, Industrial Internet of Things, and cyber-physical systems. IEEE Commun Surv Tutor 2021;23(4):2351–2383; https://doi.org/10.1109/COMST.2021.3106669.

295. Lee E, Seo YD, Oh SR, et al. A Survey on standards for interoperability and security in the Internet of Things. IEEE Commun Surv Tutor 2021;23(2).

296. Ali B, Gregory MA, Li S. Multi-access edge computing architecture, data security and privacy: a review. IEEE Access 2021; 9:18706–18721; https://doi.org/10.1109/ACCESS.2021.3053233.

297. Moustafa N. A systemic IoT–Fog–Cloud architecture for Big-Data analytics and cyber security systems: a review of fog computing. En: Secure Edge Computing CRC Press; 2021.

298. Rios R, Onieva JA, Roman R, et al. Personal IoT privacy control at the Edge. IEEE Secur Priv 2022;20(1):23–32; https://doi.org/10.1109/MSEC.2021.3101865.

299. Ahvar E, Ahvar S, Mann ZA, et al. DECA: A Dynamic energy cost and Carbon emission-efficient application placement method for Edge clouds. IEEE Access 2021; 9:70192–70213; https://doi.org/10.1109/ACCESS.2021.3075973.

300. Ghaffari F, Gharaee H, Arabsorkhi A. Cloud security Issues based on people, process and technology model: a survey. En: 2019 5th International Conference on Web Research (ICWR) 2019; pp. 196–202; https://doi.org/10.1109/ICWR.2019.8765295.

301. Ahmad W, Rasool A, Javed AR, et al. Cyber security in IoT-based Cloud computing: a comprehensive survey. Electronics 2022;11(1):16; https://doi.org/10.3390/electronics11010016.

302. European Commission. Rolling Plan for ICT Standardisation. Cloud and Edge computing - Joinup. 2021. Disponible en: https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/cloud-and-edge-computing [Último acceso: 08/06/2022].

303. European Union Agency for Network and Information Security (ENISA). Cloud security. Disponible en: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security [Último acceso: 28/05/2022].

304. Grande E, Beltrán M. Securing device-to-cloud interactions in the Internet of Things relying on Edge devices. 2022; pp. 559–564.

305. European Union Agency for Network and Information Security (ENISA). Privacy and data protection by design. From policy to engineering. 2014; https://doi.org/10.2824/38623.

306. Diario Oficial de la Unión Europea. Carta de los Derechos Fundamentales de la Unión Europea. 2016.

307. Boletín Oficial del Estado. Constitución Española. Texto Consolidado. Última modificación: 27 de septiembre de 2011. 1978.

308. Degli Esposti S, Ball K, Dibb S. What's in It for us? Benevolence, national security, and digital surveillance. Public Adm Rev 2021;81(5):862–873; https://doi.org/10.1111/puar.13362.

309. Agencia Española de Protección de Datos. Anonimización y seudonimización. 2021. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/blog/anonimizacion-y-seudonimizacion [Último acceso: 05/10/2022].

310. Pawar A, Ahirrao S, Churi PP. Anonymization techniques for protecting privacy: a survey. En: 2018 IEEE Punecon 2018; pp. 1–6; https://doi.org/10.1109/PUNECON.2018.8745425.

311. Véliz C. Privacidad es poder: datos, vigilancia y libertad en la era digital. Penguin Random House Grupo Editorial España; 2021.

312. Esposti SD. When big data meets dataveillance: the hidden side of analytics. Surveill Soc 2014;12(2):209–225; https://doi.org/10.24908/ss.v12i2.5113.

313. Acquisti A, Brandimarte L, Loewenstein G. Secrets and likes: the drive for privacy and the difficulty of achieving it in the digital age. J Consum Psychol 2020;30(4):736–758; https://doi.org/10.1002/jcpy.1191.

314. Chernyshev M, Zeadally S, Baig Z. Healthcare data breaches: implications for digital forensic readiness. J Med Syst 2018;43(1):7; https://doi.org/10.1007/s10916-018-1123-2.

315. Dutta N, Jadav N, Tanwar S, et al. Introduction to digital forensics. En: Cyber security: issues and current trends. (Dutta N, Jadav N, Tanwar S, et al. eds). Studies in Computational Intelligence Springer: Singapore; 2022; pp. 71–100; https://doi.org/10.1007/978-981-16-6597-4_5.

316. Oficina de Ciencia y Tecnología del Congreso de los Diputados (Oficina C). Informe C: Inteligencia artificial y salud. 2022; https://doi.org/10.57952/tcsx-b678.

317. Galván E, Garcia-Alfaro J, Navarro-Arribas G, et al. Agents in a privacy-preserving world. Trans Data Priv 2021;14(1):53–63.

318. Kaaniche N, Laurent M, Belguith S. Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. J Netw Comput Appl 2020; 171:102807; https://doi.org/10.1016/j.jnca.2020.102807.

319. Adams C. Introduction to Privacy Enhancing Technologies: a classification-based approach to understanding PETs. Springer Nature; 2021.

320. European Union Agency for Network and Information Security (ENISA). Privacy Enhancing Technologies: evolution and state of the art. ENISA 2016.

321. Domingo-Ferrer J, Blanco-Justicia A. Privacy-preserving technologies. En: The ethics of cybersecurity. (Christen M, Gordijn B, Loi M. eds). The International Library of Ethics, Law and Technology Springer International Publishing: Cham; 2020; pp. 279–297; https://doi.org/10.1007/978-3-030-29053-5_14.

322. CyberSec4Europe. Cyber Security for Europe. D3.11. Definition of privacy by design and privacy preserving enablers. 2020.

323. Hernández-Álvarez L, de Fuentes JM, González-Manzano L, et al. Privacy-preserving sensor-based continuous authentication and user profiling: A Review. Sensors 2021;21(1):92; https://doi.org/10.3390/s21010092.

324. 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) (Texto pertinente a efectos del EEE). 2016.

325. European Commission. Data Act: Measures for a Fair and innovative data economy. Text. 2022. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113 [Último acceso: 06/06/2022].

326. Commission Staff Working Document. Guidance on sharing private sector data in the European data economy accompanying the Document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Towards a common European data space." 2018.

327. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions "Building a European Data Economy" COM/2017/09 Final, May 22, 2019. 2017.

328. Agencia Española de Protección de Datos. A Guide to Privacy by Design. 2019;54.

329. Lecuit JA. Identidad digital y seguridad online. Real Instituto Elcano 2020.

330. Arroyo D, Diaz J, Gayoso V. On the difficult tradeoff between security and privacy: challenges for the management of digital identities. En: International Joint Conference. (Herrero Á, Baruque B, Sedano J, et al. eds). Advances in Intelligent Systems and Computing Springer International Publishing: Cham; 2015; pp. 455–462; https://doi.org/10.1007/978-3-319-19713-5_39.

331. Instituto Nacional de Ciberseguridad (INCIBE). Ciberseguridad en la identidad digital y la reputación online. Una Guía de Aproximación Para El Empresario. 2016.

332. Gálik S. On Human Identity in Cyberspace of Digital Media. Eur J Tranformation Stud 2019;7(2):33□44.

333. González-Larrea B, Hernández-Serrano MJ. Digital identity built through social networks: new trends in a hyperconnected world. En: Eighth International Conference on Technological Ecosystems for Enhancing Multiculturality. TEEM'20 Association for Computing Machinery: New York, NY, USA; 2020; pp. 940–944; https://doi.org/10.1145/3434780.3436629.

334. Sule M-J, Zennaro M, Thomas G. Cybersecurity through the lens of digital identity and data protection: issues and trends. Technol Soc 2021;67:101734; https://doi.org/10.1016/j.techsoc.2021.101734.

335. European Commission. European digital identity. Text. 2020. Disponible en: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en [Último acceso: 21/09/2022].

336. World Economic Forum. Strategic intelligence. Disponible en: https://intelligence.weforum.org [Último acceso: 14/06/2022].

337. European Commission. A trusted and secure European E-ID - Regulation. Shaping Europe's Digital Future. 2021. Disponible en: https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation [Último acceso: 20/9/2022].

338. European Union Agency for Network and Information Security (ENISA). Digital identity: leveraging the SSI concept to build trust. 2022; https://doi.org/10.2824/8646.

339. European Union Agency for Network and Information Security (ENISA). Remote identity proofing - attacks & countermeasures. 2022; https://doi.org/10.2824/183066.

340. Beduschi, A. Digital Identity: Contemporary challenges for data protection, privacy and non-discrimination rights. 2019. Disponible en: https://journals.sagepub.com/doi/full/10.1177/2053951719855091 [Último acceso: 22/09/2022].

341. Bernal Bernabe J, Hernández-Ramos JL, Skarmeta Gómez AF. Holistic privacy-preserving identity management system for the Internet of things. Mob Inf Syst 2017;2017:1–20; https://doi.org/10.1155/2017/6384186.

342. Ning H, Zhen Z, Shi F, et al. A survey of identity modeling and identity addressing in Internet of Things. IEEE Internet Things J 2020;7(6):4697–4710; https://doi.org/10.1109/JIOT.2020.2971773.

343. Lewallen J. Emerging technologies and problem definition uncertainty: the case of cybersecurity. Regul Gov 2021;15(4):1035–1052; https://doi.org/10.1111/rego.12341.

344. Llewellyn Evans G. Disruptive Technology and the board: the tip of the iceberg. Econ Bus Rev 2017;3(17)(1); https://doi.org/10.18559/ebr.2017.1.11.

345. Taeihagh A, Ramesh M, Howlett M. Assessing the regulatory challenges of emerging disruptive technologies. Regul Gov 2021;15(4):1009–1019; https://doi.org/10.1111/rego.12392.

346. Pupillo L, Fantin S, Ferreira A, et al. Artificial Intelligence and cybersecurity technology, governance and policy challenges: Final Report of a CEPS Task Force. 2021.

347. Wallden P, Kashefi E. Cybersecurity in the quantum era. Commun ACM 2019;62(4):120–120; https://doi.org/10.1145/3241037.

348. Cirac JI. Quantum computing and simulation: Where we stand and what awaits us. Nanophotonics 2021;10(1):453–456; https://doi.org/10.1515/nanoph-2020-0351.

349. Arroyo Guardeño DA, Hernández Encinas L, Díaz Vico J. Blockchain. CSIC; 2019.

350. Khan D, Jung LT, Hashmani MA. Systematic literature review of challenges in blockchain scalability. Appl Sci 2021;11(20):9372; https://doi.org/10.3390/app11209372.

351. Jairam S, Gordijn J, Da Silva Torres I, et al. A decentralized fair governance model for permissionless blockchain systems: 15th International Workshop on Value Modelling and Business Ontologies, VMBO 2021. Guizzardi G, Sales TP, Griffo C, et al. eds. VMBO 2021 Value Model 2021;2835:23–31.

352. Arroyo Guardeño D. Blockchain y democracia digital:

¿descentralización o acto de fe? 2019. Disponible en: http://theconversation.com/blockchain-y-democracia-digital-descentralizacion-o-acto-de-fe-118282 [Último acceso: 25/04/2022].

353. Shin D, Bianco WT. In blockchain we trust: does blockchain itself generate trust? Soc Sci Q 2020;101(7):2522–2538; https://doi.org/10.1111/ssqu.12917.

354. Schneier B. There's No good reason to trust blockchain technology. Wired. 2019.

355. Ziolkowski R, Miscione G, Schwabe G. Decision problems in blockchain governance: old wine in new bottles or walking in someone else's shoes? JManag Inf Syst 2020;37(2):316–348; https://doi.org/10.1080/07421222.2020.1759974.

356. Letter in Support of Responsible Fintech Policy. 2022. Disponible en: https://concerned.tech [Último acceso: 07/07/2022].

357. El Ioini N, Pahl C. A Review of distributed ledger technologies. En: On the move to meaningful internet systems. OTM 2018 Conferences. (Panetto H, Debruyne C, Proper HA, et al. eds). Lecture Notes in Computer Science Springer International Publishing: Cham; 2018; pp. 277–288; https://doi.org/10.1007/978-3-030-02671-4_16.

358. Pérez-Medina D. Blockchain, criptomonedas y los fenómenos delictivos: entre el crimen y el desarrollo. Bol Criminológico 2020;27; https://doi.org/10.24310/Boletin-criminologico.2020.v27i.11283.

359. Ali Syed T, Alzahrani A, Jan S, et al. A Comparative analysis of blockchain architecture and its applications: problems and recommendations. IEEE Access 2019; 7:176838–176869; https://doi.org/10.1109/ACCESS.2019.2957660.

360. Lecuit JA. La seguridad y privacidad del blockchain, más allá de la tecnología y las criptomonedas. Real Inst Elcano 2019.

361. Kumar R, Sharma R. Leveraging blockchain for ensuring trust in IoT: a survey. J King Saud Univ - Comput Inf Sci 2021; https://doi.org/10.1016/j.jksuci.2021.09.004.

362. Li W, Wu J, Cao J, et al. Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. J Cloud Comput 2021;10(1):35; https://doi.org/10.1186/s13677-021-00247-5.

363. Antonucci F, Figorilli S, Costa C, et al. A review on blockchain applications in the agri-food sector. J Sci Food Agric 2019;99(14):6129–6138; https://doi.org/10.1002/jsfa.9912.

364. Kiu MS, Chia FC, Wong PF. Exploring the potentials of blockchain application in construction industry: a systematic review. Int J Constr Manag 2020;0(0):1–10; https://doi.org/10.1080/15623599.2020.1833436.

365. Álvarez-Díaz N, Herrera-Joancomartí J, Caballero-Gil P. Smart contracts based on blockchain for logistics management. En: Proceedings of the 1st International Conference on Internet of Things and Machine Learning. IML '17 Association for Computing Machinery: New York, NY, USA; 2017; pp. 1–8; https://doi.org/10.1145/3109761.3158384.

366. Ante L. Smart contracts on the blockchain – A bibliometric analysis and review. Telemat Inform 2021;57:101519; https://doi.org/10.1016/j.tele.2020.101519.

367. Cong LW, He Z. Blockchain Disruption and smart contracts. Rev Financ Stud 2019;32(5):1754–1797; https://doi.org/10.1093/rfs/hhz007.

368. European Blockchain Services Infrastructure (EBSI). Home - EBSI -. Disponible en: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home [Último acceso: 08/04/2022].

369. European Commission. Setting up of EBSI compliant nodes and case use in Spain. 2020-ES-IA-0013. Text. 2021. Disponible en: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2020-es-ia-0013 [Último acceso: 31/05/2022].

370. Conferencia de Rectores de Universidades Españolas CRUE. Blue: Blockchain Universidades Españolas Crue-TIC. 2017. Disponible en: https://tic.crue.org/blue/ [Último acceso: 31/05/2022].

371. Garcia-Font V, Garrigues C, Rifà-Pous H. Difficulties and challenges of anomaly detection in smart cities: a laboratory analysis. Sensors 2018;18(10):3198; https://doi.org/10.3390/s18103198.

372. Sarker IH, Kayes ASM, Badsha S, et al. Cybersecurity data science: an overview from machine learning perspective. J Big Data 2020;7(1):41; https://doi.org/10.1186/s40537-020-00318-5.

373. Naik B, Mehta A, Yagnik H, et al. The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review. Complex Intell Syst 2021; https://doi.org/10.1007/s40747-021-00494-8.

374. CEPS Task Force Report. Artificial Intelligence and cybersecurity. Technology, governance, and policy challenges. 2021.

375. Degli Esposti S, Sierra C, Manyà F, et al. White Paper on Artificial Intelligence, Robotics and Data Science. 2020; https://doi.org/10.20350/digitalCSIC/12658.

376. Taddeo M, McCutcheon T, Floridi L. Trusting artificial intelligence in cybersecurity is a double-edged sword. Nat Mach Intell 2019;1(12):557–560; https://doi.org/10.1038/s42256-019-0109-1.

377. Lecuit JA. Implicaciones sobre el uso de la inteligencia artificial en el campo de la ciberseguridad. Real Inst Elcano 2019.

378. Comisión Europea. Comunicación de La Comisión al Parlamento Europeo, al Consejo Europeo, al Comité Económico y Social Europeo y al Comité de Las Regiones. Inteligencia Artificial para Europa. COM(2018) 237 Final. 2018.

379. Comiter M. Attacking Artificial Intelligence. Belfer Cent Sci Int Aff 2019.

380. European Union Agency for Network and Information Security (ENISA). Securing Machine Learning Algorithms. ENISA 2021; https://doi.org/10.2824/874249.

381. Garitano I, Iturbe M, Ezpeleta E, et al. Who's there? Evaluating data source integrity and veracity in IIoT using multivariate statistical process control. En: Security and privacy trends in the Industrial Internet of Things. (Alcaraz C. ed). Advanced Sciences and Technologies for Security Applications Springer International Publishing: Cham; 2019; pp. 181–198; https://doi.org/10.1007/978-3-030-12330-7_9.

382. Degli Esposti S, Mocholí Ferrándiz E. After the GDPR: Cybersecurity is the elephant in the artificial intelligence room. Eur Bus Law Rev 2021;32(1); https://doi.org/10.54648/eulr2021001.

383. Blanco-Justicia A, Domingo-Ferrer J, Martínez S, et al. Machine learning explainability via microaggregation and shallowdecisiontrees. Knowl-Based Syst 2020;194:105532; https://doi.org/10.1016/j.knosys.2020.105532.

384. Blanco-Justicia A, Domingo-Ferrer J, Martínez S, et al. Achieving security and privacy in federated learning systems: survey, research challenges and future directions. Eng Appl Artif Intell 2021; 106:104468; https://doi.org/10.1016/j.engappai.2021.104468.

385. Warnat-Herresthal S, Schultze H, Shastry KL, et al. Swarm learning for decentralized and confidential clinical machine learning. Nature 2021;594(7862):265–270; https://doi.org/10.1038/s41586-021-03583-3.

386. Schuld M, Petruccione F. Supervised learning with quantum computers. Quantum science and technology. Springer International Publishing: Cham; 2018.; https://doi.org/10.1007/978-3-319-96424-9.

387. Easttom W. Quantum computing and cryptography. En: Modern cryptography: applied mathematics for encryption and information security. (Easttom W. ed) Springer International Publishing: Cham; 2021; pp. 385–390; https://doi.org/10.1007/978-3-030-63115-4_19.

388. Barbeau M, Beurier E, Garcia-Alfaro J, et al. The quantum what? Advantage, utopia or threat? Digit Welt ;4:5.

389. Cirac JI. The long journey from prototype to the ideal quantum computer. Digit Welt 2021;5(2):62–64; https://doi.org/10.1007/s42354-021-0339-3.

390. Moody D, Alagic G, Apon DC, et al. Status Report on the second round of the NIST post-quantum cryptography standardization process. National Institute of Standards and Technology: Gaithersburg, MD; 2020.; https://doi.org/10.6028/NIST.IR.8309.

391. Ahn J, Kwon H-Y, Ahn B, et al. Toward quantum secured distributed energy resources: adoption of post-quantum cryptography (PQC) and quantum key distribution (QKD). Energies 2022;15(3):714; https://doi.org/10.3390/en15030714.

392. Fernández Mármol V, Orúe AB, Arroyo Guardeño D. Securing blockchain with quantum safe cryptography: when and how? 2020; https://doi.org/10.1007/978-3-030-57805-3_35.

393. Carrasco-Casado A, Fernández V, Denisenko N. Free- space quantum key distribution. En: Uysal, M., Capsoni, C., Ghassemlooy, Z., Boucouvalas, A., Udvary, E. (eds) Optical Wireless Communications. Signals and Communication Technology. Springer, Cham. 2016; https://doi.org/10.1007/978-3-319-30201-0_27.

394. García-Martínez MJ, Denisenko N, Soto D, et al. High-speed free-space quantum key distribution system for urban daylight applications. Appl Opt 2013;52(14):3311–3317; https://doi.org/10.1364/AO.52.003311.

395. European Commission. The European Quantum Communication Infrastructure (EuroQCI) initiative. Shaping Europe's Digital Future. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci [Último acceso: 17/05/2022].

396. La Moncloa. 18/03/2022. Ciencia e Innovación destina 54 millones de euros al Plan Complementario de Comunicación Cuántica para reforzar la ciberseguridad a través de la I+D+I [Prensa/Actualidad/Ciencia e Innovación]. Disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/ciencia-e-innovacion/Paginas/2022/180322-comunicacion-cuantica.aspx [Último acceso: 17/05/2022].

397. Overview on Quantum Initiatives Worldwide - Update 2022. 2022. Disponible en: https://qureca.com/overview-on-quantum-initiatives-worldwide-update-2022/ [Último acceso: 17/05/2022].

398. Consejo Superior de Investigaciones Científicas. El CSIC recupera la normalidad tras recibir un ciberataque. 2022. Disponible en: https://www.csic.es/ [Último acceso: 12/09/2022].

399. JASON Defense Advisory Panel: reports on defense science and technology. Disponible en: https://irp.fas. org/agency/dod/jason/ [Último acceso: 07/10/2022].

400. CyberSec4Europe. Cyber security for Europe. D2.3. Governance structure v2.0. 2021.

401. Spidalieri F. Meeting the growing demand for cybersecurityskillsandtalentin Europe. Eur Cybersecurity Context Policy-Oriented Comp Anal 2022.

402. Kenneally E, Dittrich D. The Menlo Report: Ethical principles guiding information and communication technology research. SSRN Electron J 2012; https://doi.org/10.2139/ssrn.2445102.