*Fernando Ballestero**

CÓMO MEJORAR LA CIBERSEGURIDAD EN ESPAÑA
Pasos ante una gran oportunidad

Mejorar la ciberseguridad debe hoy ser una prioridad. En las empresas e instituciones ello se consigue fundamentalmente incorporando soluciones técnicas y procedimientos de gestión, pero a nivel colectivo, como país, es necesario un papel activo de la Administración en un esfuerzo colectivo basado en la colaboración público-privada. En este contexto hay una gran oportunidad de mejorar la ciberseguridad en España con la iniciativa Next Generation y el Plan de Recuperación, Transformación y Resiliencia. Que se consiga dependerá de que el marco institucional sea adecuado y de que se trabaje conjuntamente con eficiencia en una serie de acciones.

Palabras clave: ciberriesgos, mejorar ciberseguridad, colaboración público-privada, oportunidad de mejora, ecosistema de ciberseguridad, reto de ciberseguridad.
Clasificación JEL: A19, D81, H41, L86, M14, O30.

1. Introducción. Amenazas y riesgos en el momento actual

Un año más, el *Informe de Riesgos Globales 2022* elaborado por el Foro Económico de Davos incluye las ciberamenazas como uno de los riegos más importantes, en términos de probabilidad e impacto, a los que se enfrentan hoy nuestras sociedades, detrás, por supuesto, de los riesgos medioambientales y de la pérdida de biodiversidad (World Economic Forum, 2022b).

Es más, la realidad de los hechos ha puesto de manifiesto que en estos dos años que llevamos de pandemia los incidentes de ciberseguridad han ido creciendo de modo intenso, provocando fuertes impactos en la actividad de muchas empresas e instituciones. La generalización del teletrabajo, de las compras y operaciones *online* y del uso del correo y mensajería electrónica, en muchos casos sin adoptar las mínimas precauciones de seguridad, ha provocado un aumento de los riesgos y los incidentes.

Un repaso a los datos publicados es elocuente. INCIBE (Instituto Nacional de Ciberseguridad) gestionó en 2021 a través de su centro de respuesta más de 109.216 incidentes, de los que 90.168 afectaron a ciudadanos y empresas, y 18.287 a la red académica y de investigación española (RedIRIS). Hay que mencionar que se notificaron 44.777 casos ▷

* Doctor en Economía, Técnico Comercial y Economista del Estado, Presidente del Consejo Asesor de CyberMadrid, exmiembro del Consejo de la OCDE.

Versión de junio de 2022.
https://doi.org/10.32796/bice.2022.3148.7457

de ciudadanos con sus ordenadores infectados por redes zombi o *botnets* controlados a distancia, aunque sin duda debe de haber muchos más de los cuales sus usuarios no son conscientes. Según la consultora Deloitte, la media de incidentes entre 2020 y 2021 ha aumentado considerablemente, con un 26 % más de ciberincidentes. Según su encuesta, el 69 % de las empresas afirma que ha sufrido entre uno y dos ciberincidentes de gravedad durante este último año. A esto habría que sumar los 69.202 incidentes en el sector público gestionado por el Centro Criptológico Nacional Computer Emergency Response Team (CCN-CERT), y los 619 en las redes y sistemas del Ministerio de Defensa gestionados por el Mando Conjunto del Ciberespacio (ESPDEF-CERT) (Deloitte, 2022; Departamento de Seguridad Nacional, 2021; Instituto Nacional de Ciberseguridad, 2021). Aunque la suma total puede recoger algunos datos repetidos, puede que, a su vez, no estén incluidas incidencias no reportadas por otros centros privados.

En cualquier caso, es claro que estamos ante cifras muy elevadas. Mejorar la ciberseguridad es sin duda un gran reto. Ahora bien, ¿cómo hacerlo?

A nivel individual, esto es, para una empresa, una institución o un ciudadano, la respuesta es muy sencilla: incorporar soluciones tecnológicas adecuadas y eficaces, reforzar la formación y la capacitación e incorporar estos riesgos en la gestión. Pero a nivel colectivo, como país, la solución no es tan simple, aparte de que exige dedicar muchos recursos. Han de ser las Administraciones públicas y el propio sector empresarial los que impulsen, trabajando juntos, ese esfuerzo colectivo.

Pero en medio de este panorama hay dos hechos que aportan un elemento de optimismo y esperanza: en primer lugar, que la conciencia sobre el problema que supone la ciberseguridad está aumentando, aunque en nuestro país todavía sea baja; y, en segundo lugar, la decisión de haber incluido a la ciberseguridad dentro de los objetivos del plan de ayudas para la recuperación económica tras la pandemia, que debe optimizar la utilización de los fondos Next Generation.

Estamos, por tanto, ante una oportunidad real que las empresas y las Administraciones públicas deben aprovechar. Y deben hacerlo conjuntamente, colaborando, ya que los intereses son comunes: hacer frente a una forma sofisticada de delincuencia y posicionar a España como un país líder en soluciones de ciberseguridad.

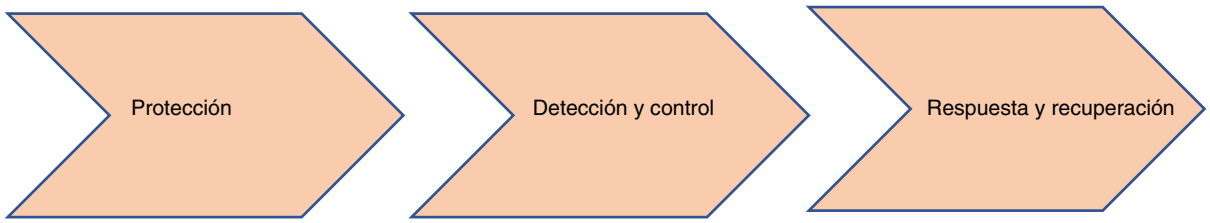
Que se consiga o no dependerá de tres factores: que el marco legal e institucional creado sea el adecuado; que la implementación práctica del Plan de Recuperación, Transformación y Resiliencia sea eficaz y se ajuste a las necesidades y prioridades reales; y, por último, que haya un seguimiento de monitorización y evaluación de los pasos que se van dando en estos próximos años para poder corregir los fallos y las decisiones ineficaces. Hagamos un repaso de estos tres condicionantes.

2. Cómo mejorar la ciberseguridad

Ante todo, es fundamental tener claro cómo puede mejorarse la ciberseguridad. En una empresa o en una institución la mejora de la ciberseguridad implica reforzar los tres ámbitos o fases del ciclo de todo ataque o incidencia, que se sintetizan en la Figura 1.

Así, para hacer frente a la fase de protección (Ballestero, 2020), hay que actuar instalando o estableciendo: ▷

FIGURA 1
CICLO OPERATIVO DE LA CIBERSEGURIDAD



Fuente: Elaboración propia a partir del esquema muy utilizado en el sector.

- Aplicaciones y procedimientos *anti-malware*.
- Sistemas y procedimientos antifraude.
- Procedimientos para evitar fugas de información.
- Protección de las comunicaciones.
- Seguridad en dispositivos.

Para hacer frente a la fase de detección y control, hay que implementar y llevar a cabo:

- Controles de trazabilidad.
- Auditorías técnicas.
- Soluciones de certificación.
- Programas de *compliance* o cumplimiento legal.

Por último, frente a la fase de recuperación, es importante:

- Conocer y evaluar los impactos reales.
- Tener un plan de contingencia, que incluya un plan de continuidad en la actividad.

Pero para poder llevar a cabo estas acciones de manera eficiente se requiere que la empresa o institución disponga en su equipo de una o varias personas (dependiendo del tamaño) con un cierto grado de formación y capacitación en la materia, o al menos con un mínimo conocimiento y criterio para poder subcontratar los servicios externos de una empresa especializada.

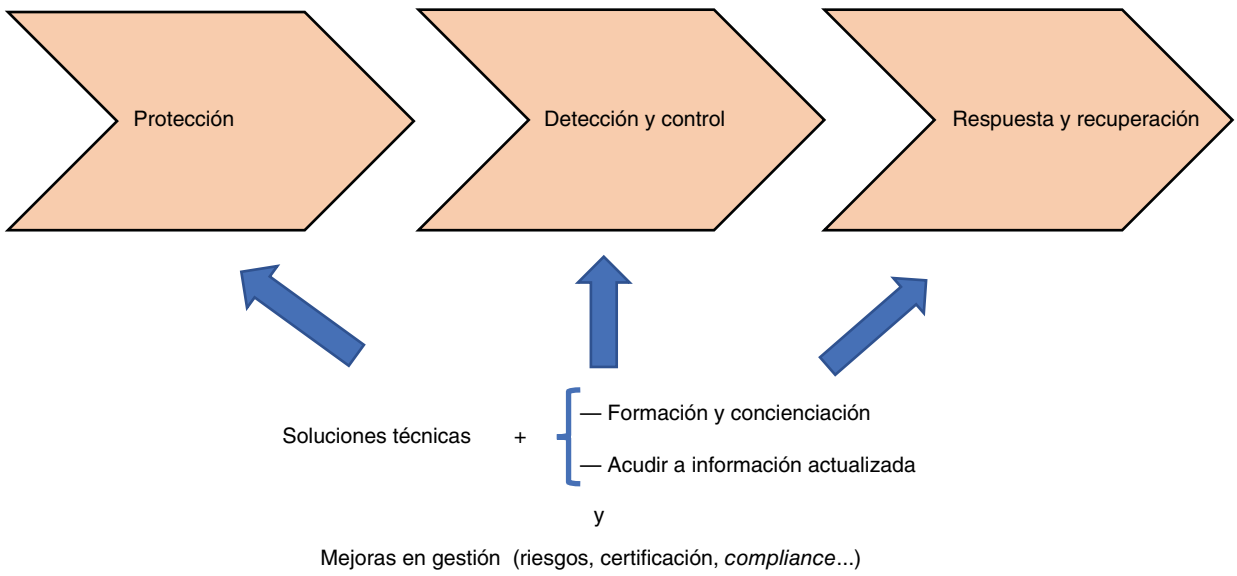
Adicionalmente, resulta un apoyo importante poder acceder a redes o fuentes de información especializada que alerten de nuevos riesgos o de incidentes que estén teniendo lugar en entornos de trabajo similares, y de las lecciones aprendidas de estas experiencias.

Y, por último, la dirección de la empresa, o institución, debe incorporar la ciberseguridad dentro de la gestión. Esto implica incorporar una gestión de riesgos y considerar otros elementos como el *compliance*, la certificación ISO, etc.

En definitiva, hay que actuar con la tecnología, las personas y los procesos. La Figura 2 recoge de modo esquemático este enfoque. No se menciona el caso de los ciudadanos, pues sería una aplicación muy simplificada de este.

De este modo mejoran su ciberseguridad las empresas y las instituciones en todos los países más avanzados. Según los resultados de la encuesta realizada con directivos de empresa de veinte países, recogida en el *Global Cibersecurity Outlook 2020* elaborado por el World Economic Forum, un 87 % de los ejecutivos están trabajando en mejorar su *cyber resilience*, reforzando sus políticas, sus procesos y sus estándares sobre el trabajo con terceros. Se entiende por *cyber resilience* o ▷

FIGURA 2
MEJORAR LA CIBERSEGURIDAD EN EMPRESAS E INSTITUCIONES



Fuente: Elaboración propia.

ciberresiliencia la capacidad de una organización para superar (anticipándose, resistiendo, recuperándose y adaptándose) las tensiones, los fallos, las incidencias y las amenazas con sus ciberrecursos dentro de su ecosistema para que pueda cumplir con su misión, preservar su cultura y mantener su forma de operar (World Economic Forum, 2022a).

Pero obviamente esto no se da en todas las empresas. En el caso de las grandes o medianas, los requisitos que mencionábamos de personal con formación e integración dentro de la gestión son más fáciles de cumplir. De hecho, suelen tener en su organigrama un puesto de responsable de seguridad de la información o CISO (Chief Information Security Officer)[1]. Sin embargo, no es así en las pymes. Para éstas es crítico poder contar con el apoyo de la Administración en ambas funciones y con ayudas para implementar soluciones técnicas. Y no digamos ya para los profesionales autónomos.

Pero, además, las propias características del sector hacen que sea la Administración a la que le corresponda jugar un papel relevante, más activo que en otros sectores en los que una actuación similar sería considerada como un exceso de intervencionismo. Ello es debido claramente a varios factores. En primer lugar, a que los incidentes y ataques a la seguridad de la información son provocados, hoy en día, fundamentalmente por la delincuencia organizada o por individuos que rentabilizan su actividad ilegal vendiendo la información que obtienen a estas redes organizadas. Los ciberdelincuentes explotan las vulnerabilidades o fallos que puedan tener los diferentes programas informáticos o aplicaciones que se utilizan en la actividad empresarial o privada, y que ellos mismos han identificado tras un trabajo concienzudo, o han adquirido de otros en el mercado negro. De hecho, es sabido que existe un importante mercado negro de datos personales, identidades, ▷

[1] Estos CISO suelen mantener de modo informal redes de contacto y reuniones periódicas para intercambiar información, además de los foros o eventos en los que coinciden.

vulnerabilidades de programas, etc., de la misma manera que hay profesionales y empresas de *hackers* «éticos» que trabajan buscando posibles vulnerabilidades de los programas que se venden o van a salir al mercado, para, una vez encontradas, si las hay, «parchearlas», esto es, corregir las vulnerabilidades.

En segundo lugar, en este sector la confidencialidad, e incluso una cierta opacidad en la información, es un hecho y, por ello, no siempre es sencillo conocer el impacto real de lo que está sucediendo en un momento determinado. Cuando una empresa de ciberseguridad desarrolla un programa o una solución tecnológica, o descubre un «parche» a un problema, prefiere no hacerlo público para protegerlo más; por su parte, cuando una empresa o institución ha sufrido un ciberataque, prefiere, si es posible, ocultarlo y no contarlo por razones de imagen ante clientes y proveedores. Por tanto, debe ser la Administración la que establezca mecanismos para que se puedan conocer los incidentes y sus consecuencias.

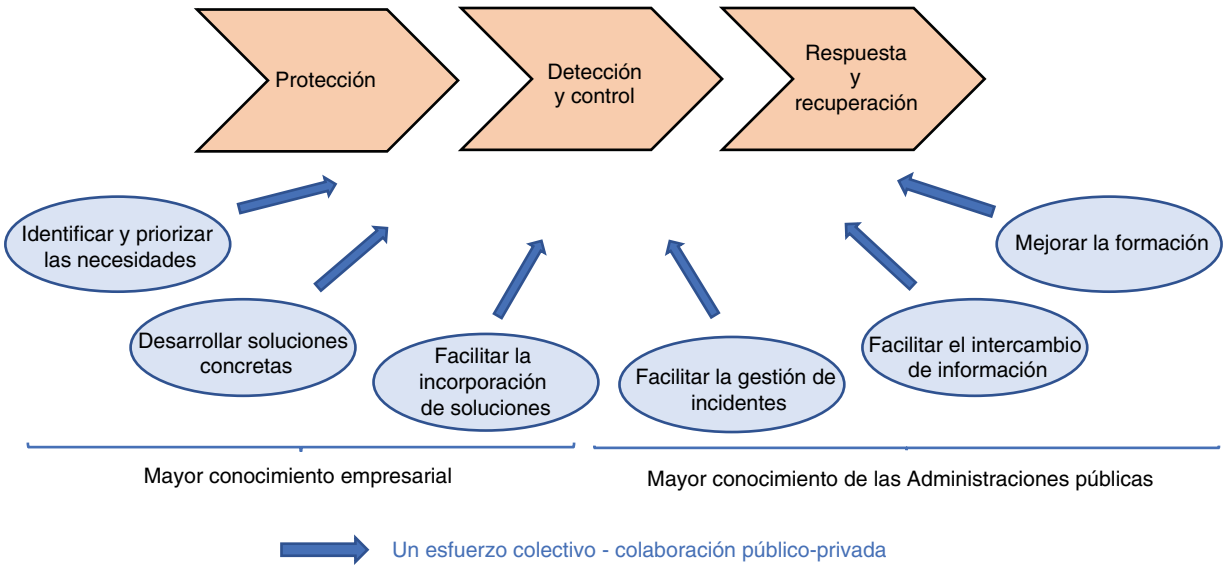
En definitiva, para conseguir una mejora de la ciberseguridad en el conjunto del país, las Administraciones públicas tienen un papel imprescindible que jugar. Son actores importantes en un esfuerzo colectivo, ya que las propias empresas deben colaborar activamente en ello, aportando principalmente su visión y su *know how*, sobre todo en el caso de empresas proveedoras de soluciones.

Como puede verse en la Figura 3, hay ámbitos en los que el conocimiento por parte de las empresas es más elevado, y otros en los que las Administraciones públicas tienen una mejor visión y capacidad. De ahí que una buena colaboración activa entre ambos tipos de agentes aporte valor y sea muy necesaria.

3. El papel del Estado y la colaboración público-privada en el campo de la ciberseguridad

Creemos que las razones expuestas son suficientemente sólidas, pero podemos ▷

FIGURA 3
CÓMO MEJORAR LA CIBERSEGURIDAD EN EL CONJUNTO DE UN PAÍS



Fuente: Elaboración propia.

mencionar que en el ámbito académico hay incluso autores que van más allá, considerando que la ciberseguridad puede ser calificada como un «bien público» que genera externalidades, y que, por tanto, el Estado debe jugar un papel más activo en este sector[2].

De hecho, y sin tener que acudir a este tipo de enfoques, es evidente que en el momento actual hay un claro consenso de apoyo público activo al desarrollo del sector. De un apoyo público no intervencionista en el mercado, de un apoyo por parte de instituciones u órganos públicos muy especializados que aportan soporte y ayudan al desarrollo del sector dejando, a su vez, que el mercado juegue de modo competitivo. Afortunadamente, no es necesario ya, como hace algunos años, buscar ejemplos de apoyo por parte de Gobiernos, referirse a casos como el de Israel o EE. UU., sino que hoy basta citar las políticas de la UE y sus Estados miembros, o las recomendaciones de la Organización para la Cooperación y el Desarrollo Económicos (OCDE).

En todos los casos, se trata de políticas de apoyo basadas en una colaboración público-privada y, por ello, a efectos de clarificación, es conveniente recordar brevemente qué hay detrás de este concepto.

Como recogen expertos de la OCDE, no hay una definición estandarizada de qué se entiende por colaboración público-privada, o más concretamente, en su terminología inglesa, por *public-private partnership*. En general, se considera colaboración público-privada a los acuerdos a medio o largo plazo entre la Administración pública y socios privados. La fórmula se aplica tanto a obras de infraestructura como a provisión de servicios, y es considerada dentro de los principios de lo que se conoce como «buen gobierno» (OCDE, 2012; Ruiz Rivadeneira y Schuknecht, 2019).

Pues bien, podemos decir que las políticas de mejora de la ciberseguridad en la UE y en sus Estados miembros se han desarrollado con ese enfoque.

4. La política de apoyo a la ciberseguridad en España y el marco institucional

Llegados a este punto conviene hacer un breve repaso a la política de apoyo que se lleva a cabo en España y al marco institucional en el que se desarrolla.

4.1. La Estrategia Nacional de Ciberseguridad y el Plan Nacional de Ciberseguridad

El interés y la importancia por la ciberseguridad en España, por parte de la Administración del Estado, se remonta a la creación de las unidades de delitos informáticos de la Policía Nacional y la Guardia Civil, a mediados de los años noventa. En 2005 se dio un paso fundamental con la creación del INTECO (Instituto de Tecnologías de la Comunicación), que años más tarde pasaría a denominarse INCIBE (Instituto Nacional de Ciberseguridad).

Pero, aparte de estas acciones específicas, no fue hasta 2011 cuando se aprobó la Primera Estrategia de Seguridad Nacional, incluyendo en esta la seguridad de la información y de las redes. En ese año también se aprobó la Ley Reguladora de las Infraestructuras Críticas. Sin embargo, por estar al final de la legislatura no hubo un desarrollo de la estrategia, como ▷

[2] Pueden verse, en este sentido, trabajos como Asllani *et al*. (2013) o Kianpour *et al.* (2022).

debería haberse hecho. Sería un año después, ya en 2012, cuando se crearía el DSN, o Departamento de Seguridad Nacional, dentro de Presidencia del Gobierno, como órgano de asesoramiento al presidente del Gobierno en materia de seguridad nacional, y, entre otras funciones, impulsar el desarrollo e integración del Sistema de Seguridad Nacional[3].

Poco después, en 2013, se creó el Consejo de Seguridad Nacional o Comisión Delegada del Gobierno, que encabeza el propio presidente del Gobierno y en la que participan los ministros competentes. Su Secretaría Técnica la ejerce la DSN. Es el Consejo el que ha aprobado la última actualización de la estrategia, en diciembre de 2021, hoy vigente (Real Decreto 1150/2021).

Dentro de este marco, el 29 de marzo de 2022 se aprueba también el Plan Nacional de Ciberseguridad. Este incluye más de 130 actuaciones, cuya implementación asciende a 1.000 millones de euros. Una parte importante de ellas ya tienen adjudicada su financiación. El resto se ejecutarán una vez se disponga de los recursos económicos necesarios. Una gran parte de las medidas incluidas en el plan están vinculadas al Plan de Recuperación, Transformación y Resiliencia, que más adelante comentamos.

4.2. La organización dentro de la Administración del Estado

A la hora de implementar estas acciones, y dejando fuera de nuestro análisis el área de defensa, hay cuatro departamentos o unidades operativas que juegan un papel central clave: el DSN de Presidencia del Gobierno, el CCN, el CNPIC y el CCO, y el INCIBE. Cada uno tiene asignadas unas competencias específicas.

Así, el DSN es el órgano de asesoramiento al presidente del Gobierno en materia de seguridad nacional. Y, dentro de ella, la ciberseguridad ocupa una parte relevante. Precisamente, con el objeto de mantener un contacto directo y una relación de colaboración en este ámbito, impulsó la creación del Foro Nacional de Ciberseguridad, constituido en 2020 con el objetivo de fomentar la cultura de ciberseguridad y promoverla a través de un entorno de colaboración público-privada. Son miembros del foro asociaciones empresariales, otras entidades y expertos. Su presidente es el del DSN.

El CCN (Centro Criptológico Nacional), dependiente del CNI (Centro Nacional de Inteligencia), es el órgano responsable de la ciberseguridad del sector público. A través de su unidad CCN-CERT[4] gestiona la acción ante los ciberincidentes que afectan a las Administraciones públicas, incluyendo tanto las alertas como la detección, los análisis forenses y las auditorías.

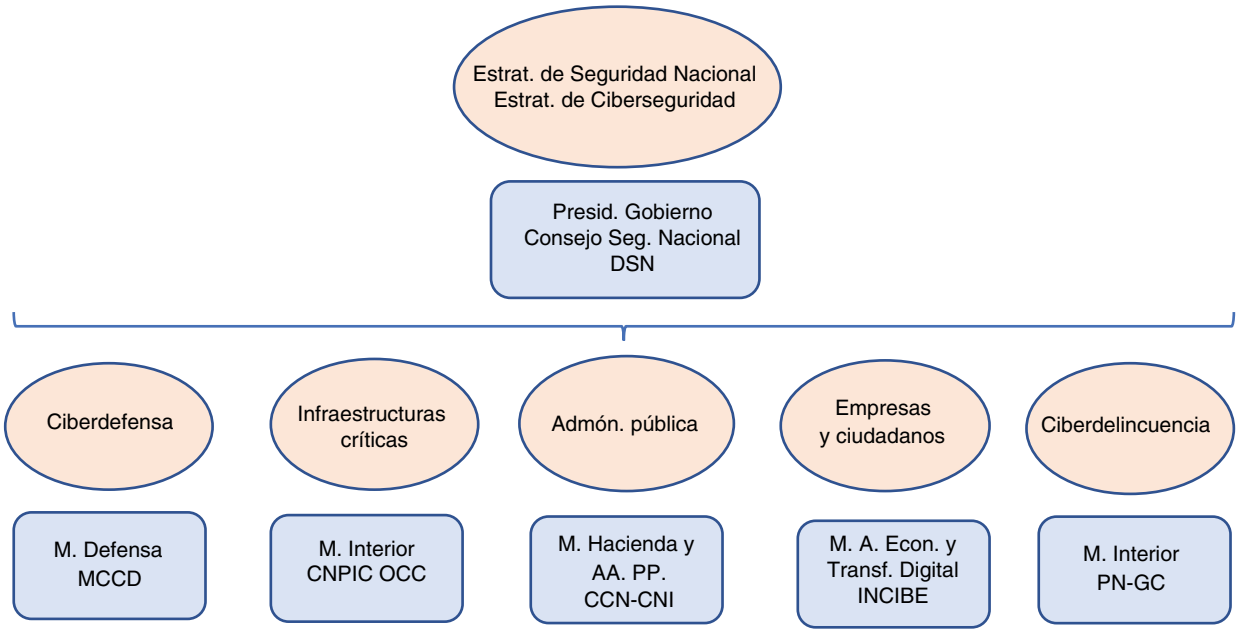
Dentro de la Secretaría de Estado de Seguridad, del Ministerio del Interior, se encuentran dos unidades: el CNPIC (Centro Nacional de Protección de las Infraestructuras Críticas), que es el órgano responsable de la ▷

[3] En concreto sus funciones son:

El Departamento de Seguridad Nacional es el órgano de asesoramiento al presidente del Gobierno en materia de seguridad nacional. Mantendrá y asegurará el adecuado funcionamiento del Centro de Situación del Departamento de Seguridad Nacional para el ejercicio de las funciones de seguimiento y gestión de crisis, e impulsará el desarrollo e integración del Sistema de Seguridad Nacional. (Real Decreto 634/2021) En https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-17340

[4] El término CERT (Computer Emergency Response Team) define a un equipo de personas dedicado a la implantación y gestión de medidas preventivas, reactivas y de gestión de la seguridad con el objetivo de mitigar el riesgo de ataques contra las redes y sistemas. El término fue creado y registrado por la Universidad Carnegie Mellon de EE. UU. en 1988, quien valida el uso del nombre, existiendo en la actualidad muchos en todos los países. También se usan las siglas CSIRT (Computer Security and Incident Response Team). Por su parte, un SOC es algo más amplio y no centrado como los anteriores en la gestión de incidentes. Es un Centro de Operaciones de Seguridad (Security Operations Center) desde donde se gestiona y monitoriza la ciberseguridad de una empresa o institución.

FIGURA 4
DEPARTAMENTOS DE LA ADMINISTRACIÓN CENTRAL RESPONSABLES EN CIBERSEGURIDAD



Fuente: Elaboración propia.

coordinación y supervisión de las infraestructuras críticas, gestionando el catálogo de infraestructuras y el plan de seguridad que estas deben seguir; y la OCC (Oficina de Coordinación de Ciberseguridad), que coordina los CSIRT o equipos de respuesta a incidencias de seguridad que tienen estas infraestructuras, y es también punto de contacto y enlace en estos ámbitos, con la Comisión Europea y los Estados miembros.

Por último, el INCIBE dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital, de empresas, profesionales autónomos, red académica y de investigación, y ciudadanos. Dispone también de un CERT para gestión de incidentes de ciberseguridad (INCIBE-CERT), aporta información y tiene un servicio de ayuda en ciberseguridad, el 017, por teléfono, WhatsApp y Telegram.

La gran profesionalidad de todas estas unidades de la Administración hace que todas ellas sean órganos muy importantes para obtener información y apoyo.

Asimismo, algunas comunidades autónomas han impulsado sus propios CERT o CSIRT.

A ello podemos sumar el papel de la Agencia Europea de Ciberseguridad, ENISA, con sede en Grecia, cuyo objetivo es velar para que la UE mantenga un nivel alto de ciberseguridad. Para ello realiza análisis e informes, impulsa la cooperación dentro de la Unión y contribuye a una mayor concienciación[5].

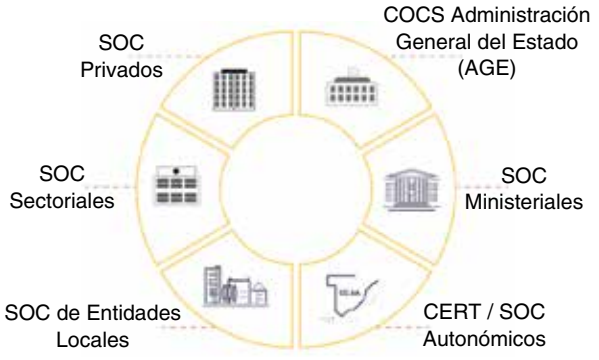
Ahora bien, aunque el marco dibujado en estas líneas refleja un claro apoyo de las Administraciones públicas a que se desarrolle la ciberseguridad, hay también un aspecto que ▷

[5] Ver https://www.enisa.europa.eu

hay que poner de manifiesto. A diferencia de otros países de nuestro entorno, en España no hay, de hecho, una centralización jerárquica en materia de ciberseguridad. Esto puede dificultar en la práctica una aplicación estricta e integral de la Estrategia de Ciberseguridad Nacional. Así, el órgano máximo responsable de la aprobación de la Estrategia de Seguridad Nacional es el Consejo de Seguridad Nacional, siendo el DSN el que coordina la elaboración de esta estrategia. Pero, en la práctica, la eficacia en la implementación depende mucho de que haya una colaboración estrecha y efectiva entre las instituciones que operan en los diferentes ámbitos. La Figura 4 recoge un esquema resumen de las competencias que ejercen cada uno de los actores dentro de la Administración General del Estado, en línea con lo que hemos dicho antes.

A esta distribución de competencias hay que añadir que, como antes mencionábamos, hay comunidades autónomas que han montado sus propios CERT o CSIRT, y adicionalmente hay empresas privadas y entidades que mantienen centros de gestión o SOC. Este panorama queda resumido en la Figura 5, recogida en el *Informe Anual de Seguridad Nacional 2021.* Según indica este informe, el Centro Criptológico Nacional (CCN-CERT) está llevando a cabo el desarrollo de la Red Nacional de Centros de Operaciones de Ciberseguridad (SOC), que permitirá una mayor coordinación y un mejor y más fluido intercambio de información entre todos sus miembros (Departamento de Seguridad Nacional, 2021).

FIGURA 5
RED NACIONAL DE CENTROS DE OPERACIONES DE CIBERSEGURIDAD (SOC)



Fuente: Centro Nacional de Inteligencia.

4.3. Otros agentes del ecosistema de ciberseguridad en España

El ecosistema de ciberseguridad

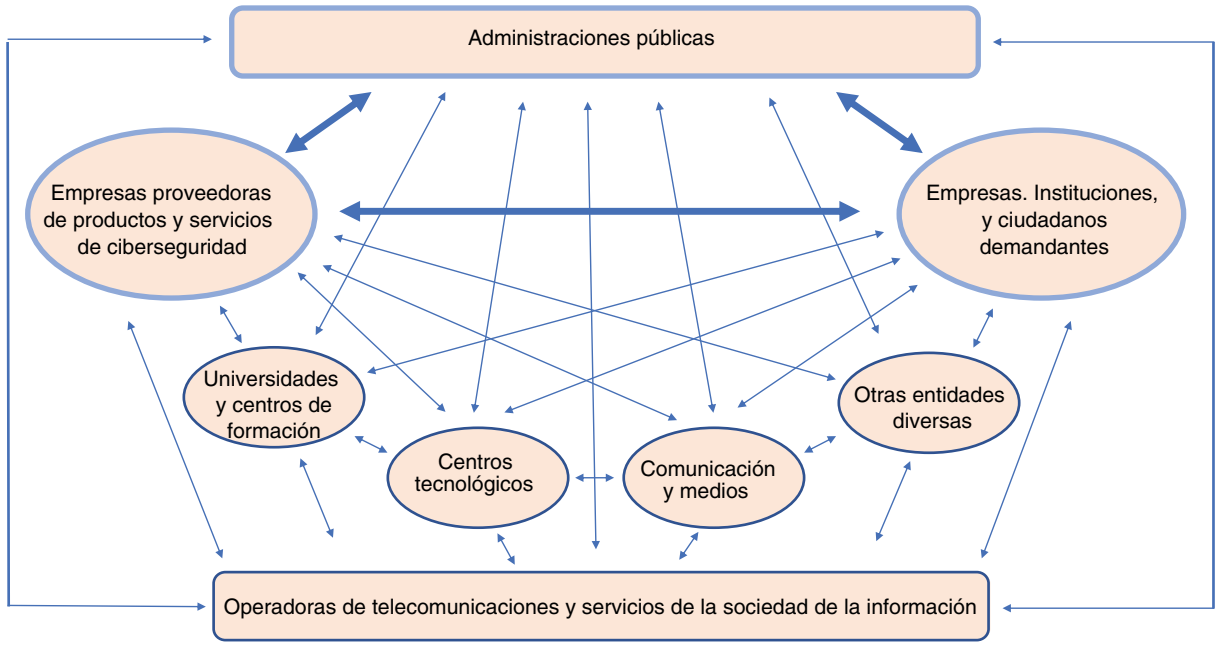
Si dejamos los aspectos de regulación, control y seguimiento de los incidentes, y nos centramos en la actividad del sector desde una óptica más económica, esto es, centrada en diferenciar los proveedores de soluciones o servicios de ciberseguridad de los usuarios o demandantes, así como otras instituciones o entidades que juegan un papel en el desarrollo de la ciberseguridad en España, vemos que el ecosistema podría representarse como en la Figura 6.

Los diferentes clústeres y su efecto tractor

Por último, en distintos territorios de nuestra geografía se han ido desarrollando clústeres que agrupan instituciones y empresas de ciberseguridad, con el objetivo de impulsar el desarrollo del sector en el entorno y que cuentan con el apoyo de las Administraciones autonómicas y locales. Los más destacados son:

– La AEI de Ciberseguridad con sede en León. La Agrupación Empresarial Innovadora en Ciberseguridad y Tecnologías Avanzadas nació con el apoyo del ▷

FIGURA 6
EL ECOSISTEMA DE CIBERSEGURIDAD



Fuente: Elaboración propia.

INCIBE, que tiene su sede en esta ciudad. Cuenta también con el apoyo de la Comunidad de Castilla y León.

– Basque Cybersecurity Centre, con sede en el Parque Tecnológico de Álava, es el centro para el desarrollo de la ciberseguridad en el País Vasco, siendo sus socios instituciones de la Administración autonómica y centros tecnológicos. Vinculado a él está CyBasque, la asociación de industrias de ciberseguridad del País Vasco. Una de sus áreas de especialización es la ciberseguridad en la industria.
– CyberMadrid (Clúster de Ciberseguridad de Madrid) fue creado en el periodo de la pandemia y formado por empresas e instituciones, a iniciativa del Ayuntamiento de Madrid, y cuenta con el apoyo de la comunidad autónoma y del INCIBE.
– El caso de Málaga, ciudad dinámica con el Proyecto Málaga Valley, impulsado, hace más de diez años, por el Ayuntamiento y el Parque Tecnológico de Andalucía (PTA), con la colaboración de la universidad, operadores de telecomunicaciones y empresas; alberga hoy el centro para desarrollo de ciberseguridad de Google.
– Otro caso a considerar es el que se está desarrollando en la Comunitat Valenciana, y en especial en Alicante. Esta ciudad se ha convertido en sede de empresas tecnológicas innovadoras, particularmente en el ámbito de las aplicaciones de la inteligencia artificial.

Hay que decir que, aunque las grandes empresas del sector operan, en general, por toda la geografía nacional, en estos entornos han ido surgiendo empresas pequeñas también muy innovadoras. ▷

5. El Plan de Recuperación y los fondos Next Generation EU. Una oportunidad

En plena pandemia del coronavirus, el Consejo Europeo adoptó, el 21 de julio de 2020, una decisión sin duda histórica. Ante la situación que se estaba viviendo, y con el objeto de ayudar a la recuperación de la economía, la convergencia y la resiliencia, la Unión Europea acordó un paquete de medidas de gran alcance, un instrumento europeo de recuperación, Next Generation EU, por valor de 750.000 millones de euros, que se sumaba al marco financiero plurianual (MFP) para 2021-2027 reforzado.

Este instrumento europeo de recuperación, que supone para España poder recibir unos 140.000 millones de euros en forma de transferencias y préstamos para el periodo 2021-2026, se basa en tres pilares: apoyar los esfuerzos de los Estados miembros por recuperarse, reparar los daños y salir reforzados de la crisis; impulsar la inversión privada y apoyar a las empresas en dificultades; hacer que el mercado único sea más fuerte y resiliente, y acelerar la doble transición ecológica y digital.

Desde el punto de vista operativo, su puesta en marcha en los Estados miembros exige que estos presenten un plan nacional de recuperación, con medidas concretas, dentro de los criterios marcados por la UE. Aprobado ese plan, la Comisión Europea, como medida de control, irá liberando fondos en función del cumplimiento del plan que presente cada Estado miembro y de los resultados eficaces que se considere puedan generar los fondos ya concedidos. En definitiva, si se implementan y financian proyectos sólidos y eficaces, la probabilidad de que haya más fondos en esa zona o sector es más alta.

En el caso de España, el Gobierno ha elaborado el Plan de Recuperación, Transformación y Resiliencia, que fue aprobado por la Comisión Europea en abril de 2021 y cuyo contenido puede verse con detalle en la web creada al efecto (Gobierno de España, 2021).

El plan establece cuatro ejes básicos (transición ecológica, transformación digital, cohesión social y territorial, e igualdad de género), y para desarrollarlos se definen diez políticas consideradas palancas, que a su vez incluyen, en conjunto, treinta componentes o áreas de actuación. Los proyectos que se presenten para ser apoyados deberán enmarcarse dentro de, al menos, uno de los componentes.

Pues bien, uno de esos componentes, dentro de la política de «modernización y digitalización del tejido industrial y de la pyme», es el de «conectividad digital, impulso a la ciberseguridad y despliegue del 5G». Adicionalmente, el reforzamiento de la ciberseguridad figura también de modo explícito dentro del componente de «modernización de las Administraciones públicas», que se encuadra dentro de la política de lograr «una Administración para el siglo XXI».

Desde el punto de vista de la implementación práctica del plan, y más concretamente de los criterios que se deberán seguir para aprobar proyectos dotándolos de recursos, la colaboración público-privada es un factor relevante. Es más, el Real Decreto-ley 36/20, por el que se aprueban medidas urgentes para la modernización de la Administración pública y para la ejecución del Plan de Recuperación, Transformación y Resiliencia, incorpora un nuevo instrumento de colaboración público-privada, los PERTE, o proyectos tractores, que viene a sumarse a otras vías o instrumentos ya existentes. En este sentido, la disposición, en su preámbulo, afirma que «… dado el efecto ▷

multiplicador que implica en la economía una movilización de recursos de esta dimensión, la CPP será clave para la ejecución de los distintos proyectos tractores contemplados en el Plan…» (Gobierno de España, 2021).

La figura de los PERTE es realmente innovadora y se está empezando a aplicar a varios sectores: vehículo eléctrico, salud de vanguardia, energías renovables, agroalimentario, microelectrónica… A la fecha de escribirse este artículo no hay un PERTE para ciberseguridad, aunque ha habido alguna consulta pública en esa línea. No obstante, hay otros instrumentos ya existentes en la legislación española que, siendo poco utilizados, podrían utilizarse mucho más, como es el caso de la Compra Pública Innovadora, que es una fórmula muy adecuada para buscar soluciones de seguridad en el sector público (Álvarez Rubio, 2021; Ministerio de Ciencia e Innovación, 2011).

En definitiva, la mejora de la ciberseguridad es un objetivo recogido en el Plan de Recuperación y, por tanto, estamos ante una oportunidad de aprovechar para España la iniciativa puesta en marcha por la UE recibiendo recursos europeos para contribuir a su mejora. La cuestión es si seremos capaces de aprovechar de modo óptimo esta oportunidad.

6. Cómo se puede optimizar esta oportunidad

Decíamos antes que la mejora de la ciberseguridad en España requiere un esfuerzo colectivo. Pero ¿dónde debe focalizarse esa necesaria colaboración público-privada?

Hemos visto que para mejorar la ciberseguridad de las empresas e instituciones hay que actuar en las tres fases que se recogían en la Figura 2, y que, adicionalmente, es un requisito imprescindible para la formación de profesionales, así como un buen sistema de seguimiento y aportación de información. Pero vimos también que para conseguir una mejora de la ciberseguridad a nivel de país hay que actuar en línea con el enfoque recogido en la Figura 3. Por tanto, la clave para conseguir el objetivo es desarrollar una serie de acciones, y hacerlo en un marco de clara colaboración público-privada. Se trataría de impulsar acciones como las siguientes:

- Mejorar la oferta de servicios y aplicaciones que aporten soluciones.
  - Facilitando la I+D+i para desarrollar soluciones concretas.
  - Apoyando a las *startup* y pequeñas empresas con proyectos innovadores.
  - Impulsando la creación de servicios de monitorización y protección externos a las empresas, como los SOC o centros de operaciones de seguridad.
  - Impulsando el desarrollo de soluciones para la recuperación tras incidentes.
- Apoyar la implantación por parte de las empresas de soluciones de seguridad.
  - Facilitando la implantación de medidas y soluciones de protección de equipos.
  - Facilitando la mejora de la protección de entornos de trabajo.
  - Facilitando la realización de diagnósticos técnicos de seguridad y de controles.
  - Facilitando la realización de *pentest*, de presencia en internet.
  - Facilitando la modernización de equipos, cuando sea imprescindible para implantar las soluciones de seguridad requeridas. ▷

  - Facilitando la realización de auditorías de seguridad y, en casos de incidentes, los análisis forenses necesarios que ayuden a solucionar mejor el problema,
- Impulsar el desarrollo y uso de seguros de ciberriesgos.
- Reforzar la formación, a todos los niveles, pero fundamentalmente en el nivel técnico operativo (en España hay un elevado número de universidades y centros superiores que imparten cursos, másteres y programas especializados, pero, sin embargo, se imparten muy pocos cursos en Formación Profesional).

Todas estas son acciones que cualquier experto recomendaría llevar a cabo. Pero lo importante es que las acciones se adecúen a las necesidades reales de cada colectivo o sector, y al nivel de partida en que estos se encuentran. Por eso, resulta imprescindible que las Administraciones públicas que vayan a establecer las convocatorias y los programas de ayuda colaboren previamente de modo activo con los diferentes sectores a efectos de que las acciones elegidas sean las adecuadas. No podemos olvidar, además, que la ciberdelincuencia organizada es muy innovadora, por lo que van incorporando elementos de sofisticación que es necesario ir detectando para protegerse. Los clústeres y *hubs* existentes, con el *know how* y conocimiento de las empresas e instituciones que participan, pueden ser un buen instrumento de apoyo a la Administración en este sentido.

En cuanto al sistema de seguimiento y aportación de información, y el papel de los CERT públicos, poco puede decirse. Las instituciones que trabajan en este ámbito están jugando un papel crítico y deben seguir jugándolo.

Por último, hay una cuestión que deben tener en cuenta los responsables de la Administración pública en el ámbito de la ciberseguridad, si quieren realmente que tras cuatro o cinco años hayamos maximizado los fondos europeos que podemos recibir, y estos se hayan utilizado de una manera eficiente. Y tiene que ver con un problema estructural que lamentablemente tiene la Administración pública española y que para hacerle frente requiere una voluntad clara de los gestores responsables.

Me refiero a que no existe, en general en nuestro país, una práctica ni una cultura de evaluación del gasto público y de las políticas públicas. En general, se planifican los presupuestos, incluso se hacen memorias con justificación económica de las propuestas de acciones, pero, una vez que el control de legalidad *ex ante* autoriza el gasto, luego no hay un seguimiento ni una verificación de si el gasto ha servido realmente para alcanzar los objetivos de la política en cuestión y si lo ha hecho de un modo eficiente.

Ha habido intentos de cambiar esta situación. La más notable, la creación en enero de 2007 de la Agencia Estatal de Evaluación de Políticas Públicas, que, tras empezar su tarea con entusiasmo, languideció, y diez años más tarde, en 2017, otro Gobierno decidió suprimir. Tras ello, la Autoridad Independiente de Responsabilidad Fiscal (AIReF) ha ido trabajando en la evaluación del gasto, asumiendo tareas, y en estos meses hemos visto renacer algo el optimismo con el Proyecto de Ley de Institucionalización de la Evaluación de las Políticas Públicas en la Administración General del Estado, aprobado por el Consejo de Ministros el pasado 24 de mayo. Propone, incluso, volver a crear la Agencia Estatal de Evaluación de Políticas Públicas[6]. ▷

[6] Ver un resumen en la referencia del Consejo de Ministros de ese día. En https://www.lamoncloa.gob.es/consejodeministros/referencias/Paginas/2022/refc20220524.aspx#evaluar

Era una exigencia de la OCDE desde hace años y, en consecuencia, también de la UE. De hecho, el proyecto de ley se enmarca, como se recoge en su texto, dentro de las medidas de reforma incluidas en el Plan de Recuperación, Transformación y Resiliencia.

En cualquier caso, si se implementa de modo eficaz y empieza a imponerse una cultura de evaluación en la Administración pública española, puede facilitar que los gestores responsables de la política de ciberseguridad incorporen este instrumento para optimizar la eficacia de las acciones. Ante ello, la Comisión Europea será, sin duda, más favorable a seguir incrementando dotación para esta política de mejora de la ciberseguridad.

7. Reflexión final

Hemos visto que las ciberamenazas generan un riesgo elevado importante al que las sociedades deben hacer frente, y de modo especial tras el uso generalizado e intenso de las comunicaciones *online* y el uso de internet como consecuencia de la pandemia. Mejorar la ciberseguridad es hoy, sin duda, un objetivo claro de todas las Administraciones públicas. Pero para mejorar la ciberseguridad en un país es imprescindible trabajar en un entorno de colaboración público-privada. Estamos ante un sector peculiar.

Pero justamente tenemos delante la iniciativa del programa de apoyo a la recuperación de la UE Next Generation, por la que se van a destinar cuantiosos fondos de ayuda para la transformación digital y la modernización de las Administraciones públicas. Para beneficiarse de esta iniciativa el Gobierno lanzó el año pasado el Plan de Recuperación, Transformación y Resiliencia, en el que la idea de colaboración público-privada es un criterio relevante.

En España tenemos ya, en el ámbito de la ciberseguridad, un marco institucional adecuado, aunque requiera esfuerzos de colaboración estrechos entre todas las instituciones del ecosistema. Por el contrario, según el último informe del Foro de Seguridad Nacional, la conciencia del tema es aún baja en pymes y autónomos. Aquí impulsar más formación, sobre todo en un nivel más técnico y operativo, es fundamental.

La clave del éxito, por tanto, es que empresas y Administraciones públicas trabajen conjuntamente en los próximos años para ir definiendo las acciones más adecuadas que deben ser impulsadas ahora y en estos próximos años para mejorar el nivel de ciberseguridad en toda España. El seguimiento continuo de lo que se vaya haciendo es muy importante, pues la sofisticación de los ciberdelincuentes es alta y hay que saber dar respuesta a los cambios y a nuevas modalidades de amenazas que vayan surgiendo. Ir haciendo una evaluación, en paralelo, de las políticas aplicadas, sería una garantía de eficiencia en las decisiones y en su implementación.

En definitiva, una gran oportunidad, y unos primeros pasos ya en marcha. El éxito dependerá de que seamos capaces de desarrollar ese trabajo conjunto. Y la historia nos dice que sí puede hacerse. Cuando España como país se enfrentó a la gran oportunidad de transformar su economía, con la adhesión a la UE, y dejar atrás una economía encorsetada, fue posible un esfuerzo colectivo que consiguió hacer de la oportunidad un éxito: nos incorporamos a un espacio europeo abierto y competitivo y recibimos muchísimos fondos para modernizar el país. Ahora toca el esfuerzo para acabar de digitalizar nuestra economía y hacerla más robusta y menos vulnerable. ▷

Bibliografía

Álvarez Rubio, B. (2021). La colaboración público-privada, palanca del Plan de Recuperación, Transformación y Resiliencia. *Economía Industrial*, (420). https://www.mincotur.gob.es/es-ES/Publicaciones/Paginas/detallePublicacionPeriodica.aspx?numRev=420

Asllani, A., White, C. S., & Ettkin, L. (2013). Viewing cybersecurity as a public good. The role of governments, businesses, and individuals. *Journal of Legal, Ethical and Regulatory Issues, 16*(1), 7-14.

Ballestero, F. (2020). La ciberseguridad en tiempos difíciles. ¿Nos ocupamos de ella o nos preocupamos por ella? *Boletín Económico de ICE,* (3122). https://doi.org/10.32796/bice.2020.3122.6993

Deloitte. (2022). *El estado de la ciberseguridad en España. Post pandemia: un camino inexplorado.* https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html

Departamento de Seguridad Nacional. (2021). *Informe Anual de Seguridad Nacional 2021*. https://www.dsn.gob.es/es/documento/informe-anual-seguridad-nacional-2021

Gobierno de España. (2021). *Plan de Recuperación, Transformación y Resiliencia*. https://planderecuperacion.gob.es/plan-espanol-de-recuperacion-transformacion-y-resiliencia

Instituto Nacional de Ciberseguridad. (2021). *Balance de ciberseguridad 2021.* https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2021_incibe.pdf

Kianpour, M., Kowalski, S. J., & Overby, H. (2022). Advancing the concept of cybersecurity as a public good. *Simulation Modelling Practice and Theory*, *116*.

Ministerio de Ciencia e Innovación. (2011). *Guía sobre Compra Pública Innovadora*. https://www.mineco.gob.es/stfls/MICINN/Innovacion/FICHEROS/Politicas_Fomento_Innv./Guia.CPI.pdf

Organisation for Economic Co-operation and Development. (2012). *Recommendation of the Council on Principles for Public Governance of Public-Private Partnerships. May 2012*. https://www.oecd.org/governance/budgeting/PPP-Recommendation.pdf

Real Decreto 634/2021, de 26 de julio, por el que se reestructura la Presidencia del Gobierno. *Boletín Oficial del Estado,* n.º 178, de 27 de julio de 2021, pp. 90436 a 90446. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-12549

Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021. *Boletín Oficial del Estado,* n.º 314, de 31 de diciembre de 2021, pp. 167795 a 167830. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-21884#:~:text=Art%C3%ADculo%20%C3%BAnico.,texto%20se%20incluye%20a%20continuaci%C3%B3n

Real Decreto-ley 36/2020, de 30 de diciembre, por el que se aprueban medidas urgentes para la modernización de la Administración Pública y para la ejecución del Plan de Recuperación, Transformación y Resiliencia. *Boletín Oficial del Estado,* nº 341, de 31 de diciembre de 2020, pp. 126733 a 126793. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-17340

Ruiz Rivadeneira, A. M., & Schuknecht, L. (2019). Ensuring effective governance of Public-Private Partnerships. *Journal of Infrastructure, Policy and Development, 3*(2).

World Economic Forum. (2022a). *Global Cybersecurity Outlook 2022*. *Insight Report January 2022*. https://www.weforum.org/reports/global-cybersecurity-outlook-2022/

World Economic Forum. (2022b). *The Global Risks Report 2022*. https://www.weforum.org/reports/global-risks-report-2022

Páginas Web

European Union Agency for Cybersecurity. https://www.enisa.europa.eu

La Moncloa. https://www.lamoncloa.gob.es/consejodeministros/referencias/Paginas/2022/refc20220524.aspx#evaluar