Guardianes digitales para un crecimiento sostenible: ciberseguridad y protección ciudadana en la era de la transformación digital

Resumen ejecutivo

CONSEJO ECONÓMICO
Y SOCIAL **ESPAÑA**

CONSEJO ECONÓMICO Y SOCIAL **ESPAÑA**

Guardianes digitales para un crecimiento sostenible: ciberseguridad y protección ciudadana en la era de la transformación digital

Resumen ejecutivo

Premio de investigación del CES, convocatoria XXII

Director de la investigación: Alberto Vaquero García
Autores: María Bastida Domínguez, Alejandro Domínguez Lamela, Santiago Lago Peñas, Luis Alberto Otero González, Miguel Ángel Vázquez Taín, María Luisa del Río Araujo, Consuelo Ferreiro Regueiro, Luís Míguez Macho y Senén Barro Ameneiro.

En este trabajo se evalúa el impacto socioeconómico de la ciberseguridad en España desde una múltiple perspectiva, con el objeto de conocer su dimensión, situación, implicaciones y potenciales líneas de mejora. Esta investigación se presenta en un contexto actual en el que las personas (consumidoras y usuarias), las organizaciones, las empresas y los países presentan una clara dependencia –y cada vez con mayor intensidad– del mundo digital. En este nuevo marco, el desarrollo acelerado de las tecnologías de la información y la comunicación (TIC) y la incorporación de la inteligencia artificial (IA) ofrecen al tejido empresarial importantes oportunidades de mejora (y también nuevos retos) en aspectos fundamentales para su competitividad, como la automatización, la toma de decisiones estratégicas y la creación de soluciones innovadoras. Estas tecnologías suponen la irrupción y desarrollo de nuevos modelos de negocio, canales de distribución y estrategias empresariales –cada vez más flexibles y globales– facilitando la competitividad y el acceso a cualquier mercado y potenciando el crecimiento económico. Aquellas organizaciones y empresas que no sean capaces de adaptarse a estas transformaciones verán comprometida su sostenibilidad y competitividad en un entorno cada vez más cambiante y globalizado.

En consecuencia, y en base a los argumentos previamente señalados, la ciberseguridad se configura como un motor estratégico tanto directo, al generar empleo y actividad económica, como indirecto, por el impulso que supone su aplicación hacia otros sectores y actividades. Este estudio posibilita contar con un análisis aplicado de la situación actual del sector de ciberseguridad en España, analizando sus fortalezas, debilidades, oportunidades y amenazas, lo que permitirá identificar acciones que impulsen su crecimiento y competitividad.

Aunque existen trabajos previos sobre la ciberseguridad en España, no es menos cierto que sus resultados son limitados. Nuestra investigación presenta los siguientes factores diferenciales:

- La integración de estudios académicos con el análisis práctico empresarial.
- La inclusión de las necesidades estratégicas (adaptación y ajuste con los objetivos empresariales) y la posible obtención de ventajas competitivas por parte de las organizaciones ciberseguras.

- La sistematización de evidencia sobre la relación entre ciberseguridad y crecimiento sostenible.
- El análisis multinivel (global/organizativo/individual).
- La propuesta de políticas públicas orientadas a una estrategia general de ciberseguridad.

Esta investigación se estructura en siete apartados, cuyo contenido básico se relaciona a continuación. El **primer capítulo** ofrece una visión general de la ciberseguridad en España, evaluando su situación actual y su perspectiva a corto plazo. Se señala que la ciberseguridad es un tema transversal con impacto en personas (consumidores y usuarios), organizaciones, empresas, países y entorno. Se indica la necesidad de plantear un enfoque integral y de 360 grados. Este planteamiento sirve de base para estructurar el resto del informe.

El **segundo capítulo** analiza el marco general de la ciberseguridad y la ciberdelincuencia. En relación con la ciberseguridad, se realiza una aproximación conceptual, incluyendo su evolución histórica, las fases de aplicación y los niveles de protección asociados a cada una. Además, se estudian los niveles de adopción de medidas de ciberseguridad. Posteriormente se aborda la problemática de la ciberdelincuencia, siguiendo un esquema similar al planteado para la ciberseguridad. Por último, se integran ambos apartados desde una doble perspectiva –cualitativa y cuantitativa– completando este capítulo con una evaluación específica para España, para conocer su situación real y los potenciales retos.

El **tercer capítulo** se centra en el análisis del marco regulatorio del sector de la seguridad informática en el contexto europeo y español, para tener una visión comparada. El actual contexto digital ha impulsado los ciberataques. Los gobiernos y servicios públicos, así como las infraestructuras críticas de los países han sido los principales objetivos para los ciberdelincuentes por el daño –y la notoriedad– que pueden generar ir contra este tipo de servicios e infraestructuras. En este capítulo se examina la normativa española y se identifican las competencias de organismos y agencias responsables, además de señalar el papel de la colaboración público-privada en la gestión de ciberseguridad. También introduce una perspectiva legislativa comparada europea y, además, se señalan aquellas actuaciones normativas –a nuestro juicio– necesarias para garantizar un ciberespacio seguro.

El **cuarto capítulo** analiza la dimensión económica de la ciberseguridad, destacando sus implicaciones en términos de coste y beneficio. Se describen los costes directos, como la inversión en infraestructura tecnológica, contar con personal especializado y disponer de auditorías de seguridad. Se abordan los costes indirectos, como el daño reputacional, sanciones legales y pérdida de productividad. Se completa el análisis con los costes de oportunidad, como consecuencia de las interrupciones de actividad y pérdida de clientes por los ataques digitales.

En segundo lugar, se considera el impacto positivo de la ciberseguridad sobre el tejido económico, gracias a la creación de empleo técnico altamente cualificado y por el impulso a la innovación en un amplio conjunto de sectores y actividades. La ciberseguridad, al tratarse de un sector en claro crecimiento, genera una creciente demanda de profesionales altamente preparados, lo que provoca un efecto multiplicador sobre el resto de los sectores y actividades. La ciberseguridad, por lo tanto, debe entenderse como una actividad tractora.

Además, en este capítulo se destaca la importancia de valorar los costes de la ciberseguridad junto con los beneficios generados por un ecosistema socioeconómico colaborativo, público-privado, que transforme las amenazas en oportunidades de crecimiento económico sostenible. Así, y aunque la inversión en ciberseguridad sea significativa, creemos que compensa para reducir el impacto económico (y no económico) de los ciberataques, permite proteger las infraestructuras y servicios. Y, además, mejora la confianza global en la economía digital. Sin embargo, es preciso señalar que los altos costes y la posición dominante de ciertos agentes proveedores de servicios en ciberseguridad puede ser una barrera para el acceso a estas medidas, especialmente para las micropymes, pymes y para las personas con pocos recursos. Estas dificultades exigen el esfuerzo público adecuado –además de la necesaria colaboración del sector privado– para garantizar la accesibilidad y el fomento de las buenas prácticas para buscar actividades ciberseguras.

El **quinto capítulo** se ocupa de las implicaciones en materia de ciberseguridad para las personas, las organizaciones y las relaciones laborales. Se analizan los derechos de las personas usuarias, consumidoras y trabajadoras en el ámbito digital, sobre todo en lo relativo a la protección de datos personales y la necesidad de garantizar transacciones electrónicas sin riesgo. Una vez más, se procede a realizar un análisis comparado para identificar ejemplos de buenas prácticas.

Además, se remarca la importancia de integrar medidas de ciberseguridad de manera transversal. Solo así se garantizaría su alineación con la estrategia organizativa, considerando tanto los aspectos técnicos como de otra índole (psicológicos, sociales, etc.).

El **sexto capítulo** traslada el análisis teórico desarrollado en los apartados anteriores a la realidad práctica, sobre la base de dos encuestas que ofrecen una doble perspectiva: la de las empresas y la ciudadanía. La primera, diseñada específicamente para esta investigación, recoge las percepciones de las empresas sobre su grado de exposición a las herramientas digitales, el conocimiento de los problemas relacionados con la ciberseguridad, el nivel de protección frente a ciberdelitos, las certificaciones de seguridad con las que cuentan, su valoración del teletrabajo y el grado de concienciación organizacional en materia de ciberseguridad. Esta aproximación permite obtener una idea general de la forma en que las organizaciones españolas se enfrentan al actual entorno digital.

Las conclusiones obtenidas revelan importantes problemas en la ciberseguridad empresarial en España. Entre otras, la adopción de herramientas avanzadas sigue siendo limitada, dejando a las empresas vulnerables ante un número creciente de riesgos, especialmente por el uso intensivo de redes sociales, que son un objetivo frecuente de ciberataques. Además, la mayoría de las empresas almacena datos sensibles –como información personal, financiera y empresarial– lo que las convierte en blancos atractivos para la ciberdelincuencia. Sin embargo, pese a que el 90% de las empresas ha implantado recientemente medidas de protección, estas se centran en niveles básicos, indicando un amplio margen de mejora. Solo el 55% cuenta con un responsable específico de ciberseguridad, y menos del 60% dispone de una estrategia formal en este ámbito. Asimismo, se obtiene como el 15% de las empresas depende exclusivamente de apoyo externo para la gestión de la ciberseguridad. Estos resultados permiten inferir que la concienciación en materia de ciberseguridad si bien va aumentando paulatinamente, no va acompañada de implantación de medidas avanzadas.

La segunda encuesta se aproxima a los efectos que pueden generar los ciberdelitos sobre las personas a partir de información elaborada por el Centro de Investigaciones Sociológicas (CIS). De los resultados se desprende que Internet se ha consolidado como una herramienta esencial para la ciudadanía, aunque con una percepción generalizada de riesgo proveniente de estafas y fraudes en línea, especialmente entre los jóvenes y personas con mayor nivel educativo. No obstante, las tasas de denuncia son bajas; este resultado puede ser debido al escaso grado de confianza de los mecanismos de denuncia o bien a importantes dificultades con relación al acceso a estos mecanismos. Además, destaca la falta de formación específica en seguridad digital, lo que limita tanto la prevención como la capacidad de respuesta ante un ciberataque. También se observa una alta preocupación sobre los riesgos asociados al uso de la IA, sobre todo entre las personas jóvenes y con mayor nivel formativo.

El **séptimo capítulo** recoge las principales conclusiones de esta investigación, centradas en la necesidad de fortalecer la inversión en ciberseguridad y desarrollar una estrategia multidisciplinar para tratar que España se posicione adecuadamente en un entorno digital cada vez más complejo e interconectado.

Se destaca como la digitalización ha transformado a la economía y la sociedad, aunque estos cambios han provocado un incremento exponencial de la ciberdelincuencia. Este problema resulta cada vez más evidente, porque las amenazas son mucho más sofisticadas debido al uso intensivo y extensivo de tecnologías emergentes. Los ciberdelincuentes aprovechan un amplio abanico de herramientas digitales buscando atacar ordenadores y sistemas, comprometer datos sensibles y ejecutar delitos con mayor facilidad y rentabilidad. En particular, el desarrollo y expansión de IoT –con la interconexión masiva de múltiples dispositivos– puede suponer una puerta de entrada sin apenas control por la fragilidad –e incluso inexistencia– de protecciones digitales.

Esta situación se complica por la ausencia de un marco legal unificado y la falta de consenso internacional en ciberseguridad. Esta escasa –incluso nula– coordinación puede implicar una relativa impunidad de los ciberataques, incrementando tanto el impacto económico como la erosión de la confianza en los sistemas digitales, cercenando el comercio electrónico. Además, esta creciente sofisticación de los ciberataques no entiende de tamaño ni de sector empresarial. Debido a la interconexión, ninguna empresa, organización o persona está totalmente segura, ni siquiera aquellas de mayor tamaño y/o las que cuentan con medios económicos y tecnológicos suficientes.

El **octavo y último capítulo** presenta un conjunto de recomendaciones para mejorar las actuaciones en ciberseguridad.

Entre las *recomendaciones en materia de ciberseguridad y ciberdelincuencia* destacamos la necesidad de fortalecer las infraestructuras y adoptar tecnologías avanzadas para identificar y corregir vulnerabilidades y que estas actuaciones vengan acompañadas de políticas claras de seguridad.

La cooperación público-privada e internacional es imprescindible para atajar una ciberdelincuencia que no conoce fronteras y que se puede sentir impune cuando hay múltiples jurisdicciones. Además, resulta necesario proteger especialmente a quien más lo necesita. Para ello es preciso dedicar más recursos a las micropymes y pymes. La Administración pública debe llegar a donde estas entidades no siempre alcanzan para protegerse digitalmente; el sector privado también debe colaborar en todo este proceso.

En el *ámbito jurídico* se establecen diversas recomendaciones que buscan fortalecer el marco normativo en ciberseguridad y adaptarlo a las actuales necesidades. Entre otras, garantizar el cumplimiento de normativas existentes, como la Ley Orgánica de Protección de datos y las Directivas sobre la seguridad de redes y sistemas, la conveniencia de introducir elementos esenciales de la Estrategia Nacional de Ciberseguridad en la Ley 36/2015 de Seguridad nacional y la creación de una ley específica de ciberseguridad que integre la normativa derivada de la Directiva 2022/2555 con otros aspectos como la Estrategia Nacional y la ciberseguridad en la Administración pública. Finalmente, se recomienda que la Ley Orgánica 3/2018 incluya cláusulas de ciberseguridad en convenios colectivos.

Desde la *perspectiva económica*, se indica la importancia de fomentar la formación y capacitación profesional en ciberseguridad para cubrir la creciente demanda de especialistas, que en España podría superar los 80.000 empleos en 2024. Además, la ciberseguridad debe valorarse como una actividad tractora, con capacidad para fomentar el crecimiento económico, innovación y generación de empleo de calidad. También se remarca la necesidad de aumentar los servicios especializados de emergencia y asesoramiento en el campo de la ciberseguridad; solo así será posible responder con rapidez y eficacia a los ciberataques.

Entre las recomendaciones dirigidas a las *personas, organizaciones y relaciones laborales* destacan la importancia de fortalecer la concienciación y la formación en ciberseguridad como vía fundamental para la prevención y mitigación de amenazas. Es imprescindible contar con programas de formación continua que capaciten a las personas empleadas, ciudadanía y profesionales TIC para que reconozcan fácilmente los potenciales ataques digitales y, en caso de producirse, respondan a estos eficientemente y en el menor tiempo posible. Paralelamente y como no existe la seguridad absoluta, hay que fomentar una cultura organizativa de ciberseguridad que reduzca a la mínima expresión los daños en caso de incidentes digitales.

Además, todas las personas usuarias –individuales y organizativas– precisan adoptar medidas básicas y avanzadas en ciberseguridad. Asimismo, resulta necesario contar con programas adaptados a las necesidades específicas y los recursos disponibles, que sean útiles y fáciles de manejar. La implicación de las personas es vital para garantizar una efectiva primera línea de defensa, y su capacitación debe estar alineada con la misión de la organización.

Una vez más, es preciso señalar que resulta vital que las micropymes y pymes cuenten con el apoyo adecuado para su transformación digital de forma segura y rápida. Además, es necesario reducir la brecha educativa en ciberseguridad, asegurando un conocimiento básico –accesible y comprensible– para toda la población a través de programas y actuaciones educativas específicos.

En conclusión, en este informe insistimos en que la **ciberseguridad ha superado su concepción tradicional más técnica, para convertirse en una necesidad transversal que engloba varias dimensiones (entre otras, de naturaleza jurídica, económica, empresarial y social)**, cuestiones que han quedado patente en todo el documento.

Finalmente, queremos añadir que el aumento de las actividades delictivas digitales a todos los niveles, junto con el complejo espacio normativo –no siempre adecuado a la realidad a la que se enfrenta– exige una respuesta coordinada y estructurada en el campo de la ciberseguridad. En consecuencia, solo si es posible lograr un entorno digital seguro e inclusivo, que sea capaz de combinar innovación tecnológica, cooperación público-privada y formación continua, **se conseguirá que la ciberseguridad sea un pilar esencial para el desarrollo económico sostenible y la protección de los derechos de la ciudadanía en un entorno cada vez más digital.**