Anales
del Instituto de Actuarios Españoles

4ª Época, Número 31, Año 2025/1-18
DL M-3160-1961 – ISSN 0534-3232 – eISSN 2531-2308

CIBERSEGURIDAD EN PEQUEÑAS Y MEDIANAS EMPRESAS: VULNERABILIDADES, AMENAZAS Y DESARROLLO DEL CIBERSEGURO

CYBERSECURITY IN SMALL AND MEDIUM-SIZED ENTERPRISES: VULNERABILITIES, THREATS AND THE DEVELOPMENT OF CYBER INSURANCE

Ibtissame El Ferjani El Ferjani
Departamento de Econometría, Estadística y Economía Aplicada. Universitat de Barcelona. Barcelona, España.
ORCID: https://orcid.org/0009-0008-9035-9098
elferjani@ub.edu

Manuela Alcañiz Zanón
Departamento de Econometría, Estadística y Economía Aplicada. Universitat de Barcelona. Barcelona, España.
ORCID: https://orcid.org/0000-0002-5028-1926
malcaniz@ub.edu

Miguel Santolino Prieto
Departamento de Econometría, Estadística y Economía Aplicada. Universitat de Barcelona. Barcelona, España.
ORCID: https://orcid.org/0000-0002-0286-3673
msantolino@ub.edu
(Autor para correspondencia/Corresponding author)

Fecha de recepción/Date of reception: 24/04/2025
Fecha de aceptación/Date of acceptance: 15/07/2025

ABSTRACT

Small and medium-sized enterprises (SMEs) represent an essential pillar of the global economic structure. However, their increasing digitalisation also exposes them to an growing number of cyberattacks. Despite their vulnerability, many of these companies do not prioritise cybersecurity due to a lack of resources, knowledge and a misperception of risk. A review of the literature published between 2019 and 2025 is conducted to understand the current state of research in the field of SME cybersecurity and the development of cyber insurance. The results indicate that SMEs lack adequate protection measures, with phishing, ransomware and supply chain attacks being the most frequent types of attacks. Furthermore, while cyber insurance offers an effective solution for business protection and mitigation, its adoption remains low due to a lack of awareness and economic barriers. It concludes that there is a need to develop accessible cybersecurity strategies and promote the adoption of cyber insurance adapted to the reality of SMEs.

Keywords: Cybersecurity, SMEs, cyberattacks, cyber insurance.

DOI 10.26360/2025_01

RESUMEN

Las pequeñas y medianas empresas (pymes) representan un pilar esencial del tejido económico global, pero su creciente digitalización también las expone a un número cada vez mayor de ciberataques. A pesar de su vulnerabilidad, muchas de estas empresas no priorizan la ciberseguridad debido a la falta de recursos, conocimientos y percepción errónea del riesgo. Este estudio tiene como objetivo analizar los principales riesgos cibernéticos que enfrentan las pymes, los tipos de ciberataques más comunes y el papel del ciberseguro como estrategia de mitigación y protección. Se lleva a cabo una revisión de la literatura publicada entre 2019 y 2025 para conocer el estado actual de investigación en el ámbito de la ciberseguridad de las pymes y el desarrollo de los ciberseguros. Los resultados indican que las pymes carecen de medidas de protección adecuadas, siendo el *phishing*, el *ransomware* y los ataques a la cadena de suministro los ataques más frecuentes. Además, aunque los ciberseguros ofrecen una solución efectiva para la protección empresarial, su adopción sigue siendo baja debido a la falta de conocimiento y barreras económicas. Se concluye que es necesario desarrollar estrategias accesibles de ciberseguridad y promover la adopción de ciberseguros adaptados a la realidad de las pymes.

Palabras clave: Ciberseguridad, pymes, ciberataques, ciberseguros, seguros cibernéticos.

1. INTRODUCCIÓN

Las pequeñas y medianas empresas (pymes) tienen un papel fundamental en la sociedad, ya que contribuyen significativamente a las economías nacionales y a la generación de empleo (Al-Baldawi *et al.*, 2024). La Unión Europea define a la pyme como aquella entidad que emplea a menos de 250 personas y tiene un volumen de negocio anual inferior a 50 millones de euros o un balance anual menor a 43 millones de euros. En España las pymes representan el 99,8% del tejido empresarial, generan el 65% del PIB y proporcionan el 61.6% del empleo total (DGIP, 2025).

En los últimos años, la digitalización ha transformado la manera en que trabajan las pymes, mejorando su eficiencia y competitividad. La creciente dependencia de la tecnología también ha aumentado su exposición a riesgos cibernéticos (ciberriesgos). Por ciberriesgo nos referimos a la posibilidad de que ocurra un incidente cibernético que pueda interrumpir la actividad de la empresa, causarle daño reputacional y/o generarle pérdidas económicas. Sin embargo, muchas pymes carecen de recursos y conocimientos para protegerse adecuadamente de los ciberriesgos (Chidukwani *et al.*, 2022; Taskin *et al.,* 2025). Por ello, el estudio de la ciberseguridad de las pymes y el papel que pueden desempeñar los ciberseguros para este colectivo de empresas es de especial importancia para garantizar su estabilidad y, en general, la del conjunto de la economía.

La materialización de las amenazas cibernéticas se realiza mediante ciberataques. El Instituto Nacional de Ciberseguridad en España (INCIBE) define el ciberataque como un intento deliberado de acceder sin autorización a un sistema informático mediante diversas técnicas para fines maliciosos, como el robo de información, la extorsión o el daño al sistema. Dicho ataque es llevado a cabo por uno o varios ciberdelincuentes, definidos como las personas que realizan actividades delictivas en la red contra individuos o sistemas informáticos.

Los ciberataques pueden comprometer seriamente la viabilidad económica de las pymes. A pesar de ser objetivos recurrentes de ciberataques, muchas pymes siguen sin priorizar la ciberseguridad, bien por desconocimiento, por falta de presupuesto o porque subestiman su atractivo para los ciberdelincuentes (Chidukwani *et al.,* 2022; Soyer *et al.,* 2023). Esta percepción errónea no solo las hace vulnerables, sino que también pone en riesgo a otras empresas con las que mantienen relaciones comerciales, sirviendo como puerta de entrada para ataques de mayor escala (Taskin *et al.,* 2025).

En este contexto, resulta necesario analizar los riesgos concretos a los que se enfrentan estas

empresas, así como las estrategias que pueden adoptar para mejorar su seguridad digital y proteger su negocio.

La ciberseguridad en las pymes es un campo de investigación que, aunque en crecimiento, sigue presentando importantes vacíos en la literatura. Alahmari & Duncan (2020) concluyen que la investigación en este ámbito sigue siendo limitada y enfatizan la necesidad de estudios empíricos, especialmente en países en desarrollo. Sin embargo, esta carencia no se limita solo a estas regiones, sino que también se observa en países como España, donde la literatura existente es escasa. A pesar de la creciente digitalización de las pymes en España y su vulnerabilidad a los ciberataques, apenas existen estudios que aborden esta problemática de manera específica, lo que dificulta la comprensión en este campo.

Una de las áreas más desatendidas en la literatura relativa a ciberriesgos es el análisis del papel de los ciberseguros en la mitigación y protección de los riesgos digitales de las pymes. La investigación previa ha dado poca importancia a la conexión entre pymes, seguridad digital y ciberseguros, lo que implica que muchas de estas empresas no estén aprovechando los beneficios que estos productos pueden ofrecer. La escasez de estudios en este ámbito supone una barrera para la adopción de seguros, ya que, sin suficiente información sobre su efectividad, las pymes pueden no percibirlos como una herramienta viable dentro de su estrategia de ciberseguridad (Adriko & Nurse, 2024).

Este artículo realiza una revisión bibliográfica que tiene como objetivo facilitar una mejor comprensión de la situación actual de los riesgos cibernéticos y posibilidades de protección en las pymes. En concreto, los estudios previos de ciberriesgos en las pymes se agruparán en tres grandes bloques según el área de estudio, que son las siguientes: principales riesgos digitales, medidas de ciberseguridad y el ciberseguro o seguro cibernético. Aunque los términos "ciberseguro" y "seguro cibernético" son equivalentes, se opta por utilizar de forma preferente el término "ciberseguro" para mantener la uniformidad terminológica en el texto.

Esta agrupación de la bibliografía existente pretende aportar conocimiento sobre las siguientes cuestiones:

1. ¿Cuáles son las principales vulnerabilidades digitales en las pymes y sus causas? ¿Cuáles son los tipos de ciberataques más comunes?
2. ¿Cuáles son las medidas de ciberseguridad adoptadas por las pymes?
3. ¿Qué papel juegan los ciberseguros en la protección de las pymes?

Esta estructura permite avanzar desde la identificación del problema hasta la evaluación de soluciones potenciales. El objetivo principal de esta agrupación es proporcionar una herramienta útil tanto para investigadores como para profesionales, permitiéndoles identificar de manera rápida y eficaz qué artículos académicos pueden ser relevantes dependiendo del ángulo desde el que quieran abordar los ciberriesgos en pymes. Al organizar la literatura en tres grandes áreas, este estudio no solo simplifica la búsqueda de información, sino que también contribuye a una sistematización más clara del conocimiento existente.

Nuestro propósito es aportar una primera aproximación a la ciberseguridad y a los ciberseguros en las pymes españolas, abordando una laguna en la literatura científica al identificar áreas poco estudiadas y vacíos en la investigación. Se espera que este estudio proporcione una base que pueda guiar futuras investigaciones, facilitar comparaciones con otros países y contribuir al desarrollo del ciberseguro adaptado a la realidad de las pymes en España, además de funcionar como estrategia de protección frente a los riesgos cibernéticos.

Este artículo se organiza en las siguientes secciones, que estructuran un análisis progresivo de la ciberseguridad en pymes. En la sección 2 se establece el marco metodológico, describiendo el enfoque adoptado para la recopilación y análisis de la literatura. A continuación, se desarrolla la revisión de la literatura a partir de la triple perspectiva: en la sección 3 se analiza el contexto de vulnerabilidad de las pymes ante los ciberataques; en la sección 4 se detallan las principales amenazas que enfrentan estas empresas; y en la sección 5 se estudia el papel de los ciberseguros como estrategia de mitigación y protección. En la

sección 6 se discuten los principales desafíos del sector asegurador en materia de riesgos cibernéticos. La sección 7 sintetiza los principales resultados, destacando las conclusiones obtenidas y señalando futuras líneas de investigación sobre ciberseguridad en pymes. Finalmente, en el anexo se incluyen las Tablas 1 y 2 que clasifican los artículos consultados más relevantes para la explicación de las vulnerabilidades de las pymes ante ciberataques (Tabla 1) y los artículos relacionados con los ciberseguros para pymes (Tabla 2), especificando los enfoques y objetivos de cada uno.

2. METODOLOGÍA

Este estudio sigue el enfoque de revisión clásica de literatura según lo descrito en Wee & Banister (2016), centrándose en la recopilación y organización estructurada de la literatura existente. La revisión se desarrolla siguiendo un proceso de identificación, selección y análisis de artículos relevantes, asegurando una cobertura adecuada del tema tratado.

La búsqueda se centra en artículos publicados entre 2019 y 2025, una decisión basada en la necesidad de analizar un marco temporal reciente que refleje con mayor precisión la situación actual de la ciberseguridad en las pymes. La pandemia del COVID-19 ha supuesto un punto de inflexión en este ámbito, provocando un aumento significativo de los ciberataques (Kostyaeva & Chernyakov, 2020), lo que hace necesario estudiar las investigaciones recientes que abordan estos cambios.

Dado que la literatura específica sobre ciberseguridad en pymes en España es escasa, la búsqueda se centra en artículos internacionales para contextualizar y analizar tendencias globales aplicables al caso español. Para ello, se utilizan dos bases de datos académicas de amplio alcance, *Google Scholar* y *Web of Science*, ya que ambas ofrecen acceso a un alto volumen de publicaciones científicas en el ámbito de los ciberriesgos, permitiendo una cobertura suficiente para el propósito de este artículo. Dada la escasez de literatura para el caso español, se consultan los datos publicados por el INCIBE, ya que, como principal organismo público especializado en la materia, es una referencia en la generación de estudios adaptados al contexto nacional.

Para encontrar los artículos que permitan resolver las cuestiones planteadas, se llevan a cabo tres búsquedas distintas, combinando palabras clave, tanto en español como en inglés. En primer lugar, para delimitar el ámbito de estudio y garantizar la inclusión de investigaciones sobre pymes, se utilizan los términos: "SMEs" O "SME" O "s*mall and medium-sized enterprises*" O "pymes" O "pyme" O "pequeñas y medianas empresas". En segundo lugar, para abordar la temática de la ciberseguridad y riesgos digitales, se emplean las siguientes palabras: "*cybersecurity*" O "*cyberthreat*" O "*cyberattack*". Por último, con el objetivo de analizar el papel de los seguros en la protección contra ciberataques, se usan los términos: "*cyberinsurance*" O "*insurance for cyberattacks*". Asimismo, se excluyen palabras como "*digitalization*" O "*digital risks*", ya que generan resultados genéricos que no son relevantes o no se ajustan a los objetivos del estudio.

Además de la búsqueda directa en bases de datos, se aplican dos enfoques complementarios: el *snowballing* hacia atrás, que consiste en revisar las referencias bibliográficas de los artículos seleccionados en una primera fase, y el *snowballing* hacia adelante, en el que se analizan los estudios que citan los artículos encontrados (Wee & Banister, 2016). Gracias a estos procedimientos se pueden identificar publicaciones adicionales de interés que de otro modo podrían quedar fuera del análisis.

La selección de artículos académicos se realiza en varias fases. En primer lugar, se establecen criterios de inclusión con el fin de garantizar la relevancia de los artículos recopilados: se incluyen únicamente artículos publicados en español e inglés que traten específicamente la ciberseguridad en pymes, con especial atención a los riesgos cibernéticos, los tipos de ataques más comunes y la adopción de ciberseguros. No se establece una diferenciación entre artículos teóricos y empíricos, permitiendo la inclusión de ambos enfoques con la finalidad de obtener una visión más completa del estado del conocimiento en este campo. Sin embargo, dentro del conjunto de artículos seleccionados, se observa una mayor presencia de estudios

teóricos, lo que refleja la tendencia dominante en la literatura sobre ciberseguridad en pymes.

Tras la recopilación inicial de artículos, se realiza una fase de cribado en la que se excluyen aquellos trabajos que, aunque contienen términos relevantes en el título o resumen, no presentan una conexión clara con la ciberseguridad en pymes o se centran en grandes empresas sin referencia a negocios de menor tamaño. También se descartan artículos duplicados en distintas bases de datos y aquellos que, pese a tratar temas relacionados, carecen de suficiente información metodológica o no aportan datos relevantes para el análisis.

Una vez completada la recopilación y filtrado de los estudios, los artículos seleccionados se clasifican en función de la temática, organizándose en tres categorías principales: contexto general de los ciberriesgos en pymes y tipos de ciberataques más comunes, medidas de ciberseguridad adoptadas y los ciberseguros. Esta decisión responde a la necesidad de estructurar la literatura de manera ordenada, permitiendo identificar tendencias, vacíos en el conocimiento y futuras líneas de investigación. Cabe señalar que algunos artículos pueden abordar más de una temática, pero se clasifican según la categoría en la que presentan un mayor enfoque o desarrollo.

Este enfoque de agrupación no solo permite organizar el conocimiento de forma sistemática, sino que también facilita la comparación y el contraste de las diferentes perspectivas y enfoques de los autores sobre un mismo tema. De este modo, la clasificación temática contribuye a un mejor entendimiento de la ciberseguridad en pymes y proporciona una base de consulta útil para investigadores y profesionales interesados en este ámbito.

3. VULNERABILIDADES Y PRINCIPALES AMENAZAS

Para comprender el contexto de los ciberriesgos en las pymes, es fundamental tratar los factores que las hacen especialmente vulnerables. En este apartado se analizan los artículos que se centran en ofrecer una visión sobre los principales desafíos a los que se enfrentan estas organizaciones en materia de ciberseguridad (véase la Tabla 1, en Anexo). En conjunto, estos estudios proporcionan un primer acercamiento a los aspectos esenciales de los ciberriesgos en pymes, sirviendo como base para quienes buscan entender los riesgos, desafíos y oportunidades que implica la protección de estas empresas en el entorno digital actual.

3.1 Vulnerabilidades ante los ciberataques

La digitalización ha incrementado significativamente los riesgos de ciberseguridad en las organizaciones, especialmente en las pymes. Aunque la transformación digital ofrece numerosos beneficios, también introduce vulnerabilidades inevitables. En este contexto, un entorno empresarial cada vez más interconectado exige que las pymes cuenten con una estrategia sólida de seguridad de la información y un historial comprobado en ciberseguridad para fortalecer su resiliencia empresarial (Taskin *et al.,* 2025). Esto representa un dilema: ¿cómo pueden las pymes encontrar el punto medio entre la innovación y la protección de sus datos?

A pesar del aumento de amenazas cibernéticas, muchas pymes siguen subestimando la importancia de la ciberseguridad. Operan con medidas de protección insuficientes, bajo la errónea percepción de que su menor tamaño las hace menos atractivas para los atacantes (Ponsard *et al.,* 2019). Esta falta de preparación se traduce en que los ciberdelincuentes las convierten en objetivos frecuentes debido a su bajo nivel de protección y concienciación en ciberseguridad (Chidukwani *et al.,* 2022; Taskin *et al*., 2025). Además, muchas de estas empresas no son plenamente conscientes de los riesgos que enfrentan, incluso cuando trabajan con grandes volúmenes de datos sensibles (Chidukwani *et al*., 2022; Soyer *et al.,* 2023). Esta falta de conocimiento no solo incrementa su vulnerabilidad, sino que también compromete la seguridad de grandes corporaciones con las que están interconectadas, ya que pueden ser utilizadas como puntos de acceso para ataques de mayor escala (Taskin *et al.,* 2025).

El aumento de ciberataques contra pymes se debe, en gran medida, a la percepción de que estas empresas cuentan con menos barreras de seguridad y, por tanto, son objetivos fáciles (Arroyabe *et al.,* 2024). Esta situación se agrava por la creciente dependencia de las tecnologías que estas organizaciones adoptan con el fin de mejorar su competitividad (Ponsard *et al.,* 2019). Paradójicamente, la misma tecnología que impulsa su crecimiento es la que puede llevarlas a su colapso si no se utiliza adecuadamente.

Las pymes enfrentan dificultades adicionales para implementar medidas de ciberseguridad debido a la percepción de que este ámbito es excesivamente técnico y representa una inversión considerable. Esta percepción contribuye a que la ciberseguridad no sea priorizada dentro de sus estrategias empresariales (Chidukwani *et al.,* 2024).

3.2 Impacto económico y repercusiones en el ecosistema de las pymes

Las consecuencias de un ciberataque se consideran devastadoras para las pymes, no solo en términos financieros, sino también en lo que respecta a la pérdida de reputación y confianza de los clientes. Esta falta de confianza puede afectar gravemente la captación de nuevos negocios y dificultar la recuperación financiera de las empresas perjudicadas (Montiel, 2024; Taskin *et al.,* 2025). Además, estos incidentes no se limitan a la empresa directamente afectada, sino que pueden generar importantes repercusiones comerciales que afectan a terceros, evidenciando que la protección frente a ataques cibernéticos es fundamental para toda la red de negocios interconectados (Chidukwani *et al.,* 2022; Taskin *et al.,* 2025).

La pandemia de COVID-19 agravó la situación de las pymes, ya que muchas de ellas se vieron obligadas a adoptar nuevas tecnologías y a operar en entornos digitales sin contar con la preparación adecuada en ciberseguridad. Esta crisis también puso de manifiesto la fragilidad económica de estas empresas, lo que dificultó aún más su capacidad para invertir en estrategias de protección (Kostyaeva & Chernyakov, 2020). Esta situación subraya que la ciberseguridad no se considera un lujo, sino un requisito fundamental para la continuidad del negocio, especialmente en tiempos de crisis.

Como consecuencia de esta falta de preparación y recursos, el impacto económico derivado de los ciberataques en las pymes se percibe como considerablemente alto, llegando a comprometer gravemente su sostenibilidad financiera. No obstante, cuantificar este impacto con precisión resulta complejo debido a la falta de datos accesibles al público, lo que limita el análisis académico en este campo (Künzler, 2023).

Herath (2024) proporciona una de las estimaciones más completas disponibles, basada en investigaciones realizadas entre 2010 y 2021. Según este análisis, los costes directos para una pyme alcanzan, en promedio, 50.000 dólares en gastos de respuesta al incidente, 100.000 dólares en recuperación de datos, 75.000 dólares en honorarios legales y 150.000 dólares por pérdida de ingresos, sumando aproximadamente 375.000 dólares. A esto se suman 75.000 dólares por pérdida de productividad, 200.000 dólares por daño reputacional y 50.000 dólares en cumplimiento normativo, lo que eleva el coste total estimado a 2.4 millones de dólares. Sin embargo, estos datos podrían haberse visto alterados significativamente debido al auge de los ciberataques y la continua evolución del panorama tecnológico y del cibercrimen.

Estudios más recientes indican que, en el caso de las empresas españolas, el impacto económico puede variar según su tamaño: en las más pequeñas, el coste medio de un ciberataque ronda los 50.000 euros, mientras que en compañías más grandes puede superar los 5 millones de euros (Imízcoz, 2025). Además, estos costes tienden a incrementarse rápidamente, dificultando aún más la recuperación financiera de las empresas afectadas (Saha & Anwar, 2024).

Por otro lado, las empresas también pueden enfrentarse a sanciones económicas importantes si no garantizan la seguridad de los datos de sus clientes, con multas que pueden alcanzar los 20 millones de euros o el 4% de la facturación anual global de la compañía (Ordoñez, 2025).

Ante este panorama, invertir en medidas de protección resulta fundamental para mitigar estas pérdidas, ya que esto puede ser hasta 20 veces más económico que afrontar las consecuencias de un ciberataque exitoso (E&N, 2023). La dificultad para estimar con precisión estos costes, junto con la evolución constante de las amenazas cibernéticas, subraya la importancia de seguir investigando y obteniendo datos actualizados para evaluar mejor su impacto económico en las pymes.

3.3 Tipología de ciberataques en pymes

A pesar de que las pymes son un blanco frecuente de ciberataques, la literatura revisada no proporciona un análisis detallado de las amenazas específicas a las que se enfrentan. La mayoría de los artículos se centran en las barreras para implementar defensas en ciberseguridad, sin analizar de forma detallada los riesgos concretos.

La revisión literaria realizada por Junior *et al.* (2023) confirma esta brecha, señalando que los artículos existentes no identifican ni diferencian claramente las amenazas que afectan a las pymes en comparación con organizaciones más grandes. Lo anterior resalta la necesidad de investigaciones enfocadas en clasificar y entender los riesgos de este sector, facilitando así la implementación de soluciones más efectivas.

Dado este contexto, en lugar de clasificar artículos académicos dentro de este grupo temático, este apartado resalta la escasez de investigaciones sobre ciberataques en pymes y la necesidad de abordarlas en el futuro. Más que una limitación de esta revisión, esta ausencia en la literatura señala un área que requiere mayor atención, destacando la necesidad de realizar estudios específicos para comprender mejor los riesgos a los que se enfrentan las pymes.

No obstante, aunque la literatura académica no ofrece un marco detallado de los ciberataques más frecuentes en pymes, fuentes como el INCIBE (2024) proporcionan datos sobre los principales riesgos en el contexto español. Según este organismo, las amenazas más frecuentes incluyen el *phishing*, donde los atacantes suplantan identidades legítimas para obtener información confidencial; el *ransomware*, un tipo de *malware* que bloquea el acceso a los archivos y exige un rescate para su recuperación; y los ataques a la cadena de suministro, que comprometen la seguridad de una empresa a través de sus proveedores o socios comerciales. Además, la falta de formación y de políticas de seguridad agrava la vulnerabilidad de estas empresas, ya que el desconocimiento de buenas prácticas facilita la acción de los ciberdelincuentes. Otro riesgo común es el uso de contraseñas débiles, que permiten accesos no autorizados debido a su simplicidad y previsibilidad. Finalmente, la ausencia de actualizaciones de seguridad en sistemas y *software* incrementa la exposición a ataques, ya que las vulnerabilidades no corregidas pueden ser explotadas con facilidad.

4. CIBERSEGURIDAD

4.1 Barreras para la implementación de medidas de seguridad

Las soluciones actuales de ciberseguridad suelen estar diseñadas para grandes empresas, lo que les otorga ventajas en términos de accesibilidad y facilidad de implementación, dejando a las pymes en una posición de desventaja. Además, los pequeños empresarios no disponen del conocimiento necesario para abogar por sus necesidades en materia de ciberseguridad, lo que dificulta aún más su acceso a soluciones adecuadas (Tam *et al.,* 2021).

La falta de recursos económicos es el principal obstáculo para la adopción de medidas de ciberseguridad en las pymes, seguido por la escasez de habilidades técnicas en la materia. Muchas empresas desconocen por dónde empezar a implementar buenas prácticas de seguridad, lo que las deja en una situación de vulnerabilidad constante. Además, la percepción de que la ciberseguridad es un tema excesivamente técnico y complejo desincentiva su implementación (Chidukwani *et a*l., 2024). Esto revela una brecha preocupante: mientras que las amenazas cibernéticas evolucionan rápidamente, muchas pymes permanecen estancadas en un nivel de seguridad deficiente por falta de orientación

accesible.

No obstante, aquellas empresas que logren superar estas barreras y diferenciarse por su excelencia en ciberseguridad no solo estarán mejor protegidas, sino que también ganarán la confianza de clientes y socios comerciales, convirtiéndolo en un verdadero valor competitivo (Lloyd, 2020).

4.2 El factor humano y la brecha en investigación

Uno de los principales riesgos de seguridad proviene del comportamiento de los empleados, quienes, en muchos casos, adoptan prácticas inseguras de manera involuntaria. Dado que los trabajadores tienen acceso legítimo a la información de la empresa, los errores humanos pueden generar brechas de seguridad que comprometan la privacidad y la confianza de los datos (Gundu, 2019). Esto hace evidente la necesidad de priorizar la formación en ciberseguridad dentro de las organizaciones, dado que incluso las mejores herramientas de seguridad pueden ser ineficaces si los empleados no saben utilizarlas correctamente.

A pesar del aumento en la investigación sobre ciberseguridad en pymes, existen grandes lagunas en el conocimiento sobre cómo estas empresas gestionan los riesgos y responden ante amenazas cibernéticas. Gran parte de los artículos se han centrado en políticas de seguridad y aspectos operativos, dejando de lado áreas como la detección, respuesta y recuperación ante incidentes. Además, la mayor parte de la investigación en este ámbito se ha realizado en los Estados Unidos, a pesar de que otras regiones presentan dificultades similares en contextos regulatorios y económicos diferentes (Chidukwani *et al*., 2022).

Alahmari y Duncan (2020), uno de los principales estudios en la investigación sobre ciberseguridad en pymes, identifica cinco perspectivas principales en la gestión de riesgos: amenazas, comportamientos, prácticas, concienciación y toma de decisiones. Sin embargo, su trabajo no profundiza en cómo surgen estas problemáticas dentro del ecosistema empresarial de las pymes. Para mejorar la ciberseguridad en este sector, futuras investigaciones deben enfocarse en cómo estas variables interactúan y evolucionan con el tiempo.

4.3 Ciberseguridad en las pymes españolas

Una encuesta realizada a expertos en tecnología de la información y ciberseguridad en pymes (Aranda, 2024) revela que el 61% de los altos ejecutivos en España han sido objetivo de ciberataques al menos una vez en los últimos 18 meses, una cifra que ha aumentado un 57% en los últimos tres años. Este incremento se atribuye a prácticas descuidadas, como la descarga de archivos de origen no confiable (41%), contraseñas débiles (34%) y la falta de formación específica en ciberseguridad (38%). A pesar de que el 77 % de las empresas ofrecen a sus empleados formación en ciberseguridad al menos una vez al año, solo el 52 % de los altos ejecutivos recibe capacitación avanzada, lo que los deja en una posición vulnerable frente a amenazas sofisticadas.

En respuesta a estas amenazas, las pymes en España han empezado a incrementar sus esfuerzos en ciberseguridad y planean aumentar considerablemente sus presupuestos para 2025. Concretamente, el 30% de las empresas prevé aumentar su presupuesto en ciberseguridad entre el 6% y el 10% el próximo año, mientras que el 20% planea incrementarlo en un 11% o más (PwC, 2024). No obstante, la falta de una cultura sólida de ciberseguridad sigue siendo una preocupación. De acuerdo con una encuesta a 50 organizaciones sobre el estado en cultura de ciberseguridad en el entorno empresarial (PwC, 2020), el 86 % de las organizaciones considera que sus empleados no están adecuadamente preparados para enfrentar amenazas digitales.

5. CIBERSEGUROS EN PYMES

Esta sección reúne aquellos estudios que analizan la importancia y el impacto de los ciberseguros para las pymes. Los estudios en este grupo detallan desde los beneficios y

desafíos de su adopción hasta los factores que influyen en su implementación y desarrollo dentro del mercado asegurador (véase la Tabla 2, en Anexos).

Mientras algunos autores (Taskin *et al.,* 2025) presentan el ciberseguro como un mecanismo consolidado que no solo indemniza por pérdidas, sino que también fortalece la seguridad digital de las empresas, otros (Soyer *et al*., 2023) argumentan que este mercado sigue en una etapa de desarrollo y enfrenta problemas estructurales. Este punto presenta una aparente contradicción: si bien la exigencia de ciertas medidas de seguridad como requisito para contratar una póliza parece impulsar la madurez del sector, la falta de estandarización en términos de cobertura y la incertidumbre en la fijación de primas (Soyer *et al.,* 2023) sugieren que todavía no se ha alcanzado un nivel de estabilidad comparable al de otros mercados aseguradores.

El aumento de los ciberataques ha llevado a muchas pymes a considerar estrategias de gestión de riesgos, entre ellas la contratación de ciberseguros. A pesar de esto, varios factores limitan su adopción: el desconocimiento sobre los servicios de ciberseguridad, la falta de claridad en la cobertura de las pólizas y la percepción de un bajo riesgo de sufrir ciberataques (Soyer *et al.,* 2023).

Adriko & Nurse (2024) han sido los primeros en estudiar la interrelación entre ciberseguridad, ciberriesgos y ciberseguros específicamente en el contexto de las pymes. Estos autores destacan que, aunque los ciberseguros representan una estrategia para gestionar los riesgos digitales en pymes, existe una notable escasez de investigaciones que analicen estas interconexiones. Esta falta de estudios limita la capacidad de las pymes para aprovechar plenamente los beneficios de los ciberseguros, afectando su capacidad de recuperación ante incidentes de seguridad (Adriko & Nurse, 2024).

5.1 Beneficios del ciberseguro en pymes

El ciberseguro ofrece un respaldo financiero y operativo para las empresas que enfrentan incidentes de ciberseguridad, cubriendo desde la recuperación de datos hasta la asistencia legal y la mitigación de daños reputacionales (Adriko & Nurse, 2024; Soyer *et a*l., 2023; Taskin *et al*., 2025). Su adopción no solo protege ante ataques, sino que también impulsa una digitalización más segura, ya que muchas pólizas exigen la implementación de medidas de seguridad previas a la contratación (Taskin *et al.,* 2025). Esto contribuye a fortalecer la seguridad organizacional y fomenta una mayor inversión en tecnología (Salzberger, 2025; Taskin *et al*., 2025).

Uno de los aspectos más destacados de estos seguros es el acceso a recursos especializados en caso de incidente. Muchas pólizas incluyen asesoramiento de expertos en gestión de crisis, lo que resulta especialmente valioso para pymes sin capacidades internas avanzadas en ciberseguridad (Mott *et al*., 2023). Además, pueden incorporar servicios preventivos como evaluaciones de riesgo y revisiones de seguridad (Soyer *et al.,* 2023).

Más allá de la cobertura financiera ante brechas de seguridad, los ciberseguros ofrecen herramientas de ciberseguridad, *software* antivirus y evaluaciones de vulnerabilidad. Asimismo, muchas pólizas contemplan interrupciones operativas, multas regulatorias y honorarios legales, proporcionando un respaldo a las pymes ante incidentes cibernéticos (Taskin *et al.,* 2025).

Uno de los principales beneficios de adoptar ciberseguros es su contribución a un proceso de digitalización más seguro y ágil. Al mitigar el riesgo financiero asociado a los ciberataques, las pymes pueden invertir con mayor confianza en tecnologías y sistemas de información. Además, al establecer requisitos mínimos de autoprotección, estos seguros fomentan la adopción de prácticas de ciberseguridad más sólidas en las empresas (Taskin *et al.,* 2025).

5.2 Limitaciones en la adopción de ciberseguros en pymes

A pesar de sus ventajas, la adopción de ciberseguros en las pymes se ve limitada por múltiples

factores. Una de las principales limitaciones es la falta de conciencia sobre los riesgos cibernéticos y el impacto de éstos (Adriko & Nurse, 2024). Muchas pymes no priorizan la ciberseguridad, incluso cuando su actividad depende en gran medida de datos digitales, lo que reduce su interés en contratar una póliza de este tipo (Adriko & Nurse, 2024; Soyer *et al*., 2023).

Otro obstáculo relevante es la percepción de complejidad en la adquisición y gestión de estos seguros. La necesidad de contar con conocimientos técnicos para comprender las coberturas y evaluar los riesgos asociados puede generar incertidumbre y desincentivar su contratación (Taskin *et al.,* 2025). Además, los requisitos cada vez más estrictos para obtener cobertura dificultan el acceso a muchas pymes que no cumplen con los estándares mínimos de seguridad exigidos, limitando aún más su adopción (Mott *et al*., 2023). Este punto da paso a la siguiente cuestión: ¿son las pólizas actuales demasiado complejas para el perfil mayoritario de las pymes?

Por otro lado, el factor económico también juega un papel importante en la reticencia de las pymes a contratar estos seguros. Aunque pueden reducir el impacto financiero en caso de un ciberataque, su coste inicial es percibido como elevado, lo que dificulta su contratación para empresas con presupuestos ajustados (Adriko & Nurse, 2024). En muchos casos, el gasto se considera desproporcionado en relación con la percepción del riesgo, lo que lleva a muchas pymes a priorizar otros aspectos operativos en lugar de invertir en ciberseguridad (Salzberger, 2025). Esto lleva a reflexionar sobre si los modelos actuales de fijación de precios están alineados con la realidad financiera de las pymes o si se necesita una mayor segmentación para hacer que estos seguros sean más accesibles.

Algunos autores indican que la demanda de ciberseguros aumenta en función del tamaño de la empresa y la percepción subjetiva del riesgo cibernético, especialmente cuando se anticipa un impacto financiero significativo en caso de ataque. Asimismo, la forma en que las empresas acceden a la información sobre ciberseguros influye en su adopción: mientras que la consulta independiente en internet puede generar sobrecarga de información y reducir la probabilidad de contratación, el asesoramiento externo en la toma de decisiones aumenta la demanda de estos productos. Esto indica que las pymes podrían beneficiarse de un mayor asesoramiento especializado para comprender mejor el valor y los beneficios de los ciberseguros (Salzberger, 2025).

5.3 Los ciberseguros en España

En España, los ciberseguros dirigidos a pymes y autónomos ofrecen una variedad de coberturas diseñadas para mitigar y proteger los riesgos derivados de incidentes de seguridad digital. Las pólizas se estructuran en torno a dos ejes principales: la responsabilidad civil y los daños propios.

Dentro de las coberturas de responsabilidad civil, los seguros protegen a las empresas frente a reclamaciones derivadas de violaciones de privacidad, daños a terceros e incumplimiento de normativas como el Reglamento General de Protección de Datos (RGPD) y la Ley de Servicios de la Sociedad de la Información (LSSI). Algunas pólizas contemplan la responsabilidad civil por la violación de privacidad, la cobertura de daños ocasionados a terceros por subcontratistas, la responsabilidad civil multimedia y publicidad, así como los gastos de defensa, fianzas y conflictos de intereses. También pueden incluir el abono de sanciones administrativas cuando sea legalmente asegurable, lo que puede representar un respaldo financiero importante para las empresas que enfrentan consecuencias regulatorias tras un ciberataque.

Por otro lado, las coberturas de daños propios abarcan los costes de reparación y restauración de sistemas informáticos dañados, la indemnización por interrupción del negocio, y la gestión de amenazas de extorsión cibernética. Un aspecto relevante es la protección de datos, que incluye multas y sanciones por incumplimiento de la normativa, gastos de notificación y restitución de la imagen. Además, se cubren la pérdida y recuperación de datos y los gastos de relaciones públicas y atención al cliente. Las pólizas también pueden incluir la restauración

de datos, daños por extorsión cibernética y la pérdida de beneficios debido a interrupciones en la red.

Más allá de las coberturas básicas, las aseguradoras en España ofrecen servicios preventivos tecnológicos, como antivirus y análisis de vulnerabilidades, y asesoramiento en protección de datos. En caso de ciberincidente, las empresas pueden acceder a servicios de respuesta especializados, incluyendo respuesta a incidentes, gestión de extorsiones, relaciones públicas y asesoramiento legal. Estos servicios también abarcan la recuperación de datos, la descontaminación de código malicioso, la notificación a afectados y la gestión de crisis, con soporte 24/7 y líneas directas multilingües.

En este contexto, el mercado español de ciberseguros continúa en desarrollo, con productos que buscan adaptarse a un entorno digital en constante evolución. Sin embargo, la accesibilidad, el nivel de conocimiento de las empresas y la adecuación de las coberturas a las necesidades reales de las pymes siguen siendo aspectos que requieren un mayor análisis.

6. DESAFÍOS DEL SECTOR ASEGURADOR

El mercado de ciberseguros aún se encuentra en desarrollo y tiene dificultades para expandirse. La falta de estandarización en los términos de cobertura ha impedido una adopción más generalizada, a diferencia de otros sectores como el transporte o la energía, donde existen acuerdos establecidos entre aseguradoras y clientes (Soyer *et al.,* 2023).

Desde 2020, el mercado del ciberseguro se ha endurecido significativamente debido al aumento de reclamaciones, lo que ha llevado a la industria aseguradora a elevar sus estándares. Este endurecimiento se caracteriza por un incremento considerable en las primas, una reducción en las coberturas disponibles, la imposición de estrictos requisitos de seguridad como respaldo y mayores dificultades para acceder a pólizas, especialmente en sectores de alto riesgo (Mott *et al.,* 2023).

Otra problemática es la falta de información confiable sobre incidentes de ciberseguridad. Muchas empresas no declaran ataques debido al miedo a daños reputacionales, lo que dificulta a las aseguradoras evaluar correctamente los riesgos y fijar primas de manera precisa (Adriko & Nurse, 2024; Taskin *et al*., 2025). Esta falta de datos limita la capacidad del mercado para evolucionar y ofrecer coberturas más adaptadas a las necesidades de las pymes. Si la información sobre incidentes cibernéticos es limitada, ¿están las aseguradoras diseñando sus pólizas en base a datos suficientes y de calidad que les permite una correcta evaluación y segmentación de los riesgos o están estableciendo coberturas y precios basados en fuentes con datos infraregistrados? En este contexto, la aplicación de técnicas estadísticas dirigidas a cuantificar la gravedad de la información no registrada cobra una gran relevancia (Moriña *et al*., 2021).

Algunas propuestas para mejorar el mercado de los ciberseguros incluyen el desarrollo de un nuevo producto de ciberseguro que no solo ofrezca indemnización, sino también servicios de ciberseguridad como evaluaciones de riesgos y auditorías periódicas. Esto resultaría particularmente atractivo para las pymes que buscan mejorar su resiliencia cibernética. Asimismo, la colaboración entre aseguradoras y pymes para diseñar productos ajustados a sus necesidades específicas podría fortalecer el mercado de ciberseguros (Soyer *et al.,* 2023). Además, es necesario aumentar la educación y concienciación sobre la importancia del ciberseguro y su papel en la protección y mitigación de riesgos (Adriko & Nurse, 2024; Soyer *et al*., 2023).

Las aseguradoras también pueden ejercer un rol activo en la mejora de la seguridad de sus clientes, proporcionando guías y requisitos claros para la implementación de medidas de protección. Si bien el endurecimiento del mercado ha elevado los estándares de seguridad, también ha excluido a algunas empresas del acceso al seguro. Por ello, una mayor flexibilidad en los criterios de evaluación puede permitir un mejor equilibrio entre la protección del asegurado y la accesibilidad del producto (Mott *et al.,* 2023).

Finalmente, la toma de decisiones en torno a la contratación de ciberseguros está influenciada por el contexto personal de los dueños de las pymes y su percepción del riesgo. Evaluar adecuadamente las opciones de pólizas requiere comprender la naturaleza y el alcance del riesgo cibernético en la empresa, lo que puede resultar complicado si no se cuenta con personal especializado en riesgos cibernéticos (Taskin *et al*., 2025).

7. CONCLUSIONES

La literatura analizada indica que, aunque la digitalización ha favorecido el crecimiento de las pymes, estas continúan siendo vulnerables a los ciberataques. La falta de concienciación sobre los riesgos reales y la creencia errónea de que no son objetivos atractivos para los ciberdelincuentes han contribuido a que muchas de estas empresas operen con medidas de protección insuficientes.

A pesar de la creciente incidencia de ataques cibernéticos, la investigación específica sobre las pymes españolas es escasa, lo que dificulta una correcta comprensión del impacto real de estas amenazas en el contexto nacional. Esta ausencia de datos supone una barrera para la adaptación del mercado asegurador a sus necesidades reales. Sin datos concretos, las soluciones que se aplican podrían no ajustarse realmente a los problemas que enfrentan estas empresas.

En este sentido, el desajuste entre la percepción del riesgo por parte de las pymes y las condiciones del mercado asegurador genera un círculo problemático: las empresas no contratan estas pólizas porque las consideran innecesarias o complejas, y la baja demanda impide que las aseguradoras adapten sus productos a una realidad más viable para este sector. La falta de estandarización en las coberturas y la ausencia de incentivos agravan aún más el rechazo a invertir en estos mecanismos de protección.

Por otro lado, el factor humano sigue siendo una de las principales brechas de seguridad. La literatura indica que muchas amenazas se materializan debido a errores internos o a la falta de formación en prácticas básicas de ciberseguridad. Esto indica que la inversión en tecnología no es suficiente si no va acompañada de estrategias de concienciación y capacitación. Sin una cultura de seguridad bien establecida, cualquier esfuerzo en protección digital seguirá siendo insuficiente.

Para avanzar en el diseño de los ciberseguros es necesario aplicar técnicas cuantitativas que permitan modelizar la frecuencia y severidad de los ciberataques y estimar sus costes económicos. La utilización de dichas técnicas debe permitir desarrollar esquemas de tarificación más ajustados y segmentar el riesgo de forma más precisa. En relación con la modelización de la frecuencia de ocurrencia del ciberataque, dada la escasez de datos fiables respecto al número de ciberataques, resulta necesario aplicar métodos que estimen el riesgo asociado al subregistro (*misreporting*) de los eventos, como, por ejemplo, los propuestos por Moriña *et al.* (2021). Por otro lado, El Ferjani *et al.* (2025) sugieren que el riesgo de ciberataque a empresas se concentra en periodos concretos y no siempre responde a lógicas globales, sino que también puede responder a dinámicas locales. En este sentido, técnicas econométricas y de aprendizaje automático que permitan identificar picos en la frecuencia de los ataques (burbujas) pueden ser útiles para modelizar el riesgo de ciberataque en determinados sectores y regiones para un periodo concreto.

Respecto a la modelización de la gravedad de los ciberataques, técnicas de inferencia causal que permitan modelizar la distribución de la gravedad de los ciberataques, y no únicamente el valor medio esperado, pueden ser de gran interés. En concreto, la regresión de la distribución (Chernozhukov *et al.,* 2013, 2020) o la regresión cuantílica (Koenker & Bassett, 1978; Koenker, 2005; Machado & Santos Silva, 2005), nos permiten analizar el impacto de distintos factores de riesgo sobre el conjunto de la distribución de pérdidas económicas. En este contexto, el análisis contrafactual (Verma *et al.,* 2024; Chen *et al.,* 2016) puede aplicarse para estimar el efecto en la gravedad de un ciberataque de características específicas de las pymes, como el nivel de digitalización o las medidas de seguridad implementadas. Dicho análisis nos permite estimar el impacto del factor de interés sobre la gravedad de los

ciberataques, aislándolo de otros factores de confusión, como pueden ser el sector de actividad de la pyme o su volumen de negocio. Por último, la teoría de valores extremos y los modelos de aprendizaje profundo pueden desempeñar un papel muy importante en la modelización de los ciber riesgos (Beirlant *et al.,* 2004; Zhang *et al.,* 2021). Estos métodos son de especial utilidad para identificar y anticipar eventos poco frecuentes, que ocurren de forma intensa en periodos cortos de tiempo, con elevada dimensionalidad, y que son potencialmente muy dañinos, como es el caso de los ciberataques.

En resumen, la presente revisión refleja que, si bien es fundamental implementar soluciones tecnológicas y aseguradoras, también es necesario transformar la percepción del riesgo para adaptar las prácticas de seguridad a las necesidades reales de estas empresas.

8. AGRADECIMIENTOS

Esta investigación resulta del Proyecto Estratégico "Análisis de Riesgos" (C090/23), fruto del convenio de colaboración suscrito entre el Instituto Nacional de Ciberseguridad (INCIBE) y la Universidad de Barcelona. Esta iniciativa se realiza en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiados por la Unión Europea (Next Generation).

9. REFERENCIAS

Adriko, R., & Nurse, J. R. (2024). Cybersecurity, cyber insurance and small-to-medium-sized enterprises: A systematic review. *Information & Computer Security, 32*(5), 691–710. https://doi.org/10.1108/ICS-01-2024-0025

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 2020*, 1–5. https://doi.org/10.1109/CyberSA49311.2020.9139638

Al-Baldawi, Z. A., Kassam, A. H., & Al-Zubaidi, S. S. A. (2024). Assessment the Level of Importance of SME Lean Activities Using an Integrated Model Based on Fuzzy Logic. *Management and Production Engineering Review, 15.* https://doi.org/10.24425/mper.2024.149991

Aranda, A. (2024) "Los altos ejecutivos son objetivos codiciados por los hackers. Descubre cómo preparar y proteger los datos de los altos cargos en la empresa frente a los ataques cibernéticos" Capterra, https://www.capterra.es/blog/7564/ciberataques-empresas-espanolas

Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security, 141*, 103826. https://doi.org/10.1016/j.cose.2024.103826

Beirlant, J., Goegebeur, Y., Teugels, J., & Segers, J. (2004). *Statistics of extremes: Theory and applications*. Wiley. https://doi.org/10.1002/0470012382

Chen, M., Chernozhukov, V., Fernández-Val, I., & Melly, B. (2016). *Counterfactual analysis in R: A vignette*. arXiv. https://arxiv.org/abs/1610.07894v1

Chernozhukov, V., Fernández-Val, I., & Melly, B. (2013). Inference on counterfactual distributions. *Econometrica, 81*(6), 2205–2268. https://doi.org/10.3982/ECTA10582

Chernozhukov, V., Fernández-Val, I., Melly, B., & Wüthrich, K. (2020). Generic inference on quantile and quantile effect functions for discrete outcomes. *Journal of the American Statistical Association, 115*(529), 123–137. https://doi.org/10.1080/01621459.2019.1611581

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. *IEEE Access, 10*, 85701–85719. https://doi.org/10.1109/ACCESS.2022.3197899

Chidukwani, A., Zander, S., & Koutsakis, P. (2024). Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications. *Computers & Security, 145*, 104026. https://doi.org/10.1016/j.cose.2024.104026

Dirección General de Industria y de la Pyme (DGIP) (2025). Cifras PyME: Datos diciembre 2024. Ministerio de Industria y Turismo. https://ipyme.org/Publicaciones/Cifras%20PYME/CifrasPyme-diciembre2024.pdf

El Ferjani, I., Surroca, M., Santolino, M. (2025) Análisis regional de burbujas en el número de consultas sobre ciberseguridad de las empresas. *XLIX International Conference on Regional Science*, Navarra, 15-17 Octubre.

E&N. (2023). Recuperarse de ciberataques cuesta 20 veces más que invertir en protección. *Revista Estrategia & Negocios*. https://www.revistaeyn.com/empresasymanagement/recuperarse-de-ciberataques-cuesta-20-veces-mas-que-invertir-en-proteccion-GG13371250

Gundu, T. (2019). Acknowledging and reducing the knowing and doing gap in employee cybersecurity compliance. In *ICCWS 2019 14th International Conference on Cyber Warfare and Security* (pp. 94–102).

Herath, B.M.T.I.T. (2024). The economic impact of cyberattacks: A comprehensive analysis. *Social Science Research Network*. https://ssrn.com/abstract=4885666

Instituto Nacional de Ciberseguridad de España (INCIBE) (2024). Las principales vulnerabilidades de una pyme en materia de ciberseguridad. INCIBE. https://www.incibe.es/empresas/blog/las-principales-vulnerabilidades-de-una-pyme-en-materia-de-ciberseguridad

Imízcoz, J. (2025*).* Una pyme podría perder 50.000 euros de media tras un ciberataque*. El Mundo*. https://compartiendoconocimiento.elmundo.es/una-pyme-podria-perder-50-000-euros-de-media-tras-un-ciberataque

Junior, C. R., Becker, I., & Johnson, S. (2023). Unaware, unfunded and uneducated: A systematic review of SME cybersecurity. *arXiv preprint arXiv:2309.17186*. https://doi.org/10.48550/arXiv.2309.17186

Koenker, R., & Bassett, G. (1978). Regression quantiles. *Econometrica, 46*(1), 33–50. https://doi.org/10.2307/1913643

Koenker, R. (2005). Quantile regression. *Cambridge University Press*. https://doi.org/10.1017/CBO9780511754098

Kostyaeva, E. V., & Chernyakov, M. K. (2020). Factors of development of insurance of small and medium-sized businesses in the conditions of digitalization. In *2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020)* (pp. 417–423). Atlantis Press. https://doi.org/10.2991/aebmr.k.201205.070

Lloyd, G. (2020). The business benefits of cyber security for SMEs. *Computer Fraud & Security, 2020*(2), 14–17. https://doi.org/10.1016/S1361-3723(20)30019-1

Machado, J. A. F., & Santos Silva, J. M. C. (2005). Quantiles for counts. *Journal of the American Statistical Association, 100*(472), 1226–1237. https://doi.org/10.1198/016214505000000330

Montiel (2024) *Por qué las pymes también deben priorizar la ciberseguridad en 2025. Oficinas Montiel*. https://www.oficinasmontiel.com/blog/por-que-pymes-priorizar-ciberseguridad-2025/

Moriña, D., Fernández-Fontelo, A., Cabaña, A., Puig, P. (2021). New statistical model for misreported data with application to current public health challenges. Sci Rep 11, 23321 https://doi.org/10.1038/s41598-021-02620-5

Mott, G., Turner, S., Nurse, J. R., MacColl, J., Sullivan, J., Cartwright, A., & Cartwright, E. (2023). Between a rock and a hard (ening) place: Cyber insurance in the ransomware era. *Computers & Security, 128*. https://doi.org/10.1016/j.cose.2023.103162

Ordóñez, A. (2025). Los 'otros' costes que los ciberataques propinan a las pymes. *CESCE*. https://www.cesce.es/es/w/asesores-de-pymes/costes-ciberataques

Ponsard, C., Grandclaudon, J., & Bal, S. (2019). Survey and lessons learned on raising SME awareness about cybersecurity. *ICISSP*, 558–563. https://doi.org/10.5220/0007574305580563

PwC (2020). Informe del estado de cultura de ciberseguridad en el entorno empresarial. PricewaterhouseCoopers España, Cyber Risk Culture https://www.pwc.es/es/publicaciones/digital/informe-cultura-ciberseguridad.pdf

PwC (2024). Una de cada cinco empresas tiene previsto aumentar su presupuesto de ciberseguridad más de un 11% en 2025. PricewaterhouseCoopers España https://www.pwc.es/es/sala-prensa/notas-prensa/2024/empresas-aumento-presupuesto-ciberseguridad-2025.html

Saha, B. and Anwar, Z. (2024). A Review of Cybersecurity Challenges in Small Business: The Imperative for a Future Governance Framework. *Journal of Information Security*, 15, 24-39. https://doi.org/10.4236/jis.2024.151003

Salzberger, A. (2025). An empirical analysis of the behavioral influences and information sources affecting the cyber insurance decisions of German SMEs. *Journal of Risk Finance.* https://doi.org/10.1108/JRF-05-2024-0151

Soyer, B., Nicholas, A., & Leloudas, G. (2023). Cyber risk insurance – An effective risk management tool for SMEs in the UK? *Edinburgh Law Review, 27*(2), 157–184. https://doi.org/10.3366/elr.2023.0826

Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A narrative review of cyber-security implications for Australian small businesses. *Computers & Security, 109*, 102385. https://doi.org/10.1016/j.cose.2021.102385

Taskin, N., Özkeleş Yıldırım, A., Ercan, H. D., Wynn, M., & Metin, B. (2025). Cyber insurance adoption and digitalisation in small and medium-sized enterprises. *Information, 16*(1), 66. https://doi.org/10.3390/info16010066

Verma, S., Boonsanong, V., Hoang, M., Hines, K., Dickerson, J., & Shah, C. (2024). Counterfactual explanations and algorithmic recourses for machine learning: A review. *ACM Computing Surveys, 56*(12), Article 12. https://doi.org/10.1145/3677119

Wee, B. V., & Banister, D. (2016). How to write a literature review paper? *Transport Reviews, 36*(2), 278–288. https://doi.org/10.1080/01441647.2015.1065456

Zhang Wu, M., Luo, J., Fang, X., Xu, M., & Zhao, P. (2021). Modeling multivariate cyber risks: deep learning dating extreme value theory. *Journal of Applied Statistics*, 50(3), 610–630. https://doi.org/10.1080/02664763.2021.1936468

10.ANEXO

Alahmari & Duncan (2020)	
Título	*An empirical analysis of the behavioral influences and information sources affecting the cyber insurance decisions of German SMEs*
Objetivos	Realizar una revisión sistemática de la literatura para analizar la gestión de riesgos de ciberseguridad en las pymes y el papel de su dirección en la mitigación de amenazas.
Enfoque	Cualitativo
Contexto geográfico	Alemania
Chidukwani *et al.* (2022)	
Título	*A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations*
Objetivos	Revisar la investigación sobre ciberseguridad en pymes, evaluar su alineación con un marco de seguridad, identificar problemas y proponer recomendaciones.
Enfoque	Cualitativo
Contexto geográfico	-
Chidukwani *et al.* (2024)	
Título	*Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications*
Objetivos	Identificar los factores que influyen en la ciberseguridad de las pymes y evaluar su nivel de concienciación, barreras y fuentes de orientación en la materia.
Enfoque	Cualitativo
Contexto geográfico	Australia
Guy Lloyd (2020)	
Título	*The business benefits of cyber security for SMEs*
Objetivos	Resaltar los beneficios estratégicos de la ciberseguridad para las pymes, más allá de la prevención de riesgos, destacando su impacto en la generación de valor.
Enfoque	Cualitativo
Contexto geográfico	-
Ponsard *et al.* (2019)	
Título	*Survey and Lessons Learned on Raising SME, Awareness about Cybersecurity*
Objetivos	Analizar enfoques para mejorar la concienciación en ciberseguridad de las pymes belgas y proponer directrices basadas en experiencias previas.
Enfoque	Mixto
Contexto geográfico	Bélgica
Tam *et al.* (2021)	
Título	*The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses*
Objetivos	Analizar los desafíos de ciberseguridad que enfrentan las pequeñas empresas, considerando factores técnicos y no técnicos que afectan su protección.
Enfoque	Cualitativo
Contexto geográfico	Australia

Tabla 1: Vulnerabilidades de las pymes ante ciberataques. **Fuente**: Elaboración propia

Adriko & Nurse (2024)	
Título	*Cybersecurity, Cyber insurance, and Small-to-Medium-sized Enterprises: A Systematic Review*
Objetivos	Analizar los desafíos y beneficios de la ciberseguridad y el ciberseguro en las pymes
Enfoque	Cualitativo
Contexto geográfico	-
Mott *et al.* (2023)	
Título	*Between a rock and a hard(ening) place: Cyber insurance in the ransomware era*
Objetivos	Evaluar si el ciberseguro ayuda a mitigar el impacto del ransomware y analizar cómo el endurecimiento del mercado afecta su accesibilidad.
Enfoque	Cualitativo
Contexto geográfico	Reino Unido
Salzberger (2025)	
Título	*An empirical analysis of the behavioral influences and information sources affecting the cyber insurance decisions of German SMEs*
Objetivos	Analizar los factores conductuales e informativos que influyen en la decisión de contratar ciberseguros y determinar qué inhibe la demanda entre las pymes alemanas.
Enfoque	Cuantitativo
Contexto geográfico	Alemania
Soyer *et al.* (2023)	
Título	*Cyber risk insurance - an effective risk management tool for SMEs in the UK?*
Objetivos	Evaluar la eficacia con la que las pymes utilizan el seguro de riesgo cibernético como herramienta de mitigación de riesgos.
Enfoque	Mixto
Contexto geográfico	Reino Unido
Taskin *et al.* (2025)	
Título	*Cyber Insurance Adoption and Digitalisation in Small and Medium-Sized Enterprises*
Objetivos	Analizar cómo los ciberseguros ayudan a las pymes a gestionar los crecientes riesgos de ciberseguridad derivados de la digitalización.
Enfoque	Cuantitativo
Contexto geográfico	Turquía

Tabla 2: Ciberseguros para pymes**. Fuente**: Elaboración propia.