ISBN: 978-628-95207-8-1. ISSN: 2414-6390. Digital Object Identifier: 10.18687/LACCEI2024.1.1.639

How to evaluate the cyber risk of SMEs? An Academia strategy to create competitive advantages

Javier Rojas-Segura, Máster en Investigación Empresarial[1], Jose Martinez-Villavicencio, Doctor en Dirección de Empresas[2], Margie Faith-Vargas, Máster en Administración de Empresas[3], Susan Arce, Máster en Tecnología e Innovación Educativa[4], Mauricio Arroyo-Herrera, Doctor en Gobierno y Políticas Públicas[5], Guillermo Mateu, Doctor en Dirección de Empresas[6] and Cesar Rodriguez Bravo, Ingeniero Informático [7]

[1,2,3,4,5]Tecnológico de Costa Rica, Costa Rica, jarojas@tec.ac.cr, jomartinez@tec.ac.cr, mfaith@tec.ac.cr, sarce@tec.ac.cr, marroyo@tec.ac.cr [6]Universidad de Valencia, España, guillermo.mateu@uv.es [7]Kyndryl, Inc, Costa Rica, cesarrod@kyndryl.com

Abstract – Cyber risk refers to those risks generated using information and communication technologies (ICT), whether by individuals or organizations. The literature shows a gap between exposure, perception, and preparedness of small and medium-sized enterprises (SMEs) to mitigate cyber risk. The lack of qualified personnel in cybersecurity exacerbates this situation, placing SMEs in a vulnerable position against cyber attacks. However, developing an active and resilient stance allows them to manage these risks adequately, enhancing growth and fostering innovation, leading to more valuable organizations. This research aims to develop a methodology that enables an assessment tool for evaluating SMEs' cyber risk and to design a strategy for Academia to transfer knowledge to SMEs for mitigating cyber attack risks, thereby enabling them to gain a competitive advantage. The topic is relevant since through a comprehensive methodology, risks could be identified, and recommendations could be made so that SMEs can create a plan to prioritize and implement the most appropriate improvements for each case.

Keywords—Cybersecurity, cyber risk, SMEs, cyber maturity, cyber resilience.

¿Cómo evaluar del riesgo cibernético de las PYMEs? Una estrategia de la Academia para crear ventajas competitivas

Javier Rojas-Segura, Máster en Investigación Empresarial[1], Jose Martinez-Villavicencio, Doctor en Dirección de Empresas[2], Margie Faith-Vargas, Máster en Administración de Empresas[3], Susan Arce, Máster en Tecnología e Innovación Educativa[4], Mauricio Arroyo-Herrera, Doctor en Gobierno y Políticas Públicas[5], Guillermo Mateu, Doctor en Dirección de Empresas[6] and Cesar Rodriguez Bravo, Ingeniero Informático[7]
[1,2,3,4,5]Tecnológico de Costa Rica, Costa Rica, jarojas@tec.ac.cr, jomartinez@tec.ac.cr, mfaith@tec.ac.cr, sarce@tec.ac.cr, marroyo@tec.ac.cr [6]Universidad de Valencia, España, guillermo.mateu@uv.es [7]Kyndryl, Inc, Costa Rica, cesarrod@kyndryl.com

Abstract*– El riesgo cibernético hace referencia a aquellos riesgos que se generan por el uso de las tecnologías de información y comunicación (TIC), sea por parte de las personas o de las organizaciones. La literatura muestra una brecha entre la exposición, la percepción y la preparación de las pequeñas y medianas empresas (PYMEs) para mitigar el riesgo cibernético. Situación agravada por la falta de personal calificado en ciberseguridad. Todo esto coloca a las PYMEs en una situación vulnerable ante los ataques cibernéticos. Pero al desarrollar una postura activa y resiliente les permite gestionar adecuadamente estos riesgos, potenciando no solo el crecimiento sino la innovación dando lugar a organizaciones más valiosas. Por lo que el objetivo de esta investigación es plantear la metodología para habilitar un instrumento que permita evaluar el riesgo cibernético de las PYMEs, así como diseñar la estrategia para que la Academia transfiera el conocimiento a las PYMEs para mitigar el riesgo por ciberataques, permitiéndoles crear una ventaja competitiva. El tema es relevante ya que mediante una metodología integral se podrían identificar los riesgos y sugerir recomendaciones para que las PYMEs puedan crear un plan para priorizar e implementar las mejoras más apropiadas para cada caso.

Palabras clave—Ciberseguridad, riesgo cibernético, PYMEs, madurez cibernética, resiliencia cibernética.

I. Introducción

El uso de tecnologías digitales ha dado paso a un proceso que tiene como objetivo mejorar la sociedad, desencadenando cambios significativos en el modelo de negocio de las empresas [1], dentro de esta transformación digital que estamos viviendo el papel que desempeñan las TIC es muy relevante. Si bien estos avances tecnológicos brindan numerosas ventajas y oportunidades, se sabe que enfilan a las organizaciones con nuevos desafíos, como los ataques cibernéticos. Esto es especialmente importante para las PYMEs que se consideran las menos maduras y altamente vulnerables a los riesgos de ciberseguridad [2].

En la última década, las olas de transformación digital han obligado a las PYMEs a adoptar y equipar sus modelos de negocio con tecnologías en constante evolución [3]. Sin embargo, para la dirección, la ciberseguridad no ha sido una alta prioridad para la mayoría de las PYMEs, pocos ejecutivos entienden los riesgos y no se ven a sí mismos como objetivos probables [4]. Se considera que las PYMEs enfrentan los mismos niveles de problemas de ciberseguridad que sus contrapartes más grandes, sin embargo, los recursos y capacidades limitadas las hicieron frágiles frente a los riesgos cibernéticos [5], [3].

La Agencia de la Unión Europea para la Ciberseguridad [6] encuestó a 249 PYMEs europeas sobre su estado de seguridad digital, donde el 80% afirmó que los problemas de seguridad cibernética tendrían un impacto negativo grave en su negocio, mientras que el 57% reveló que, en la eventualidad de un ciberataque, muy probablemente su negocio quebraría o cerraría. Lo cual concuerda con [7] quien indica que más de la mitad de las PYMEs hackeadas no pueden recuperarse y van a la quiebra en los seis meses posteriores al ataque.

En la Estrategia Nacional de Ciberseguridad definida por [8], a través de la aplicación sistemática de las líneas de acción, se pretendía que Costa Rica continuara siendo un líder en el área de la investigación y desarrollo en tecnologías de información (TI), como también una fuente de recursos humanos calificados en el ámbito de la seguridad cibernética y la información. Sin embargo, en la Revisión de la Estrategia Nacional de Ciberseguridad [9] se observó un menor nivel de implementación en la línea estratégica sobre temas de ciberseguridad dirigida a las PYMEs. Por lo que se hace necesario el desarrollo y traslado de documentos de buenas prácticas a las partes interesadas, así como implementar programas, cursos de capacitación y especialización en donde participe la Academia, proponiendo diferentes iniciativas de trabajo conjunto entre el sector público y privado, empezando por la promoción de una cultura de ciberseguridad [9].

La existencia de buenas prácticas de ciberseguridad en una PYME crea una ventaja competitiva para ellas en el mercado, creando oportunidades para contratos lucrativos de la cadena de suministro [10], esto requiere un esfuerzo continuo en educación, procesos e inversión y se ve afectada por la madurez de TI de las organizaciones [11].

El desafío es encontrar una metodología efectiva de evaluación de riesgos de ciberseguridad de las PYMEs [4]. Si bien existen muchos marcos y recursos de gobernanza de seguridad de la información, tales como la norma ISO 27001, estas pueden ser complicadas de interpretar y evaluar, así como costosas de implementar [12]. El problema por resolver se traduce en las preguntas: ¿Cómo construir una metodología efectiva para la evaluación del riesgo cibernético de las PYMEs? y ¿Cómo podría la Academia implementar estrategias de reducción del riesgo que le permita a las PYMEs desarrollar una ventaja competitiva? Siendo el objetivo de esta investigación plantear la metodología para habilitar un instrumento que permita evaluar el riesgo cibernético de las PYMEs, así como diseñar la estrategia para que la Academia transfiera el conocimiento a las PYMEs para mitigar el riesgo por el uso de TIC, potenciando el crecimiento y la innovación dando lugar a organizaciones más valiosas y rentables.

II. Marco Teórico

Las PYMEs juegan un papel destacado en el desarrollo económico de los países [13], son consideradas la columna vertebral de las economías en el mundo [14]. En América Latina conforman el 99,0% del parque empresarial, generando cerca de dos tercios del empleo de la región [15].

En Costa Rica las PYMEs representan el 97.5% del parque empresarial, aportan el 35.7% del PIB y contribuyen con el 33.0% del empleo formal [16]. A pesar de lo anterior, estas organizaciones empresariales, en Latinoamérica, no están exentas de limitaciones, por ende, de enfrentar diversos desafíos [17]. La dependencia de las PYMEs a la tecnología e Internet abre la puerta a vulnerabilidades frente al cibercrimen, estas debilidades ocasionan que la seguridad de la información sea un tema crítico para todas las PYMEs [18], especialmente al considerar errores humanos mediante técnicas de manipulación, como la ingeniería social, para obtener información y accesos no autorizados. Estas empresas también suelen ser las menos capaces de abordar los temas de ciberseguridad, lo cual las coloca en una posición donde necesitan de actividades de concientización sobre ciberseguridad [19].

Existe un reconocimiento generalizado entre los líderes en la mayoría de las industrias de que el papel de la tecnología digital está cambiando rápidamente, de ser un impulsor de la eficiencia marginal a un fundamental facilitador de la innovación y de la disrupción [20]. La necesidad de competitividad e innovación de las PYMEs las convierte en grandes adoptadores de tecnologías digitales, lo que aumenta su exposición a los ciberataques [7]. Estas empresas se encuentran entre las menos maduras y más vulnerables en términos de riesgo y resiliencia en materia de ciberseguridad [4]. Enfrentan muchos de los mismos problemas de ciberseguridad que las grandes empresas, pero no cuentan con los recursos correspondientes para abordar los riesgos de manera efectiva [21].

En una investigación realizada por el Foro Económico Mundial [4], el 88.0% de los encuestados expresaron estar preocupados por la resiliencia cibernética de las PYMEs en su ecosistema, considerándolas una amenaza clave en las cadenas de suministros, las redes de socios y los ecosistemas. Para el Gobierno de Japón los ataques cibernéticos se han vuelto cada vez más complejos y sofisticados, por lo que se deben tomar medidas de seguridad considerando la cadena de suministro completa, donde las PYMEs, pueden no tomar las medidas adecuadas y ser blanco de ataques [23]. Para [4] las empresas medianas se encuentran en el punto óptimo del cibercrimen, ya que son los suficientemente grandes como para tener cuentas bancarias significativas, pero a menudo no utilizan las últimas defensas de ciberseguridad y frecuentemente son la puerta de entrada a objetivos más grandes para los ciberdelincuentes. Ref. [24] externa su inquietud por la vulnerabilidad de las Startups Tecnológicas, ya que en muchos casos son proveedores y vendedores de grandes organizaciones como multinacionales, instituciones gubernamentales y financieras, almacenando incluso información confidencial de sus grandes clientes, como estados financieros, datos personales e información patentada. Convirtiéndose estas en un vector de ataque para que los *hackers* maliciosos ingresen a las grandes empresas.

Estas situaciones exigen que en la región existan las suficientes capacidades humanas para la gestión adecuada y oportuna de riesgos inherentes de ciberseguridad, de forma tal que, aunque exista mayor nivel de exposición a los riesgos por el uso incremental del entorno digital, las acciones que se adelanten reduzcan los incidentes digitales para evitar consecuencias de tipo económico o social derivadas de amenazas, ataques e incidentes cibernéticos que deterioran la confianza digital y ralentizan la adaptación para el futuro digital [25]. Sin embargo, la cantidad de profesionales adicionales que las organizaciones necesitan para defender adecuadamente sus activos críticos es escaza, lo que crea una brecha de la fuerza laboral de ciberseguridad [26]. Esta brecha varía según la realidad de cada región, pero en América del Norte, Europa y Latinoamérica está creciendo rápidamente. Pero no solo la escasez de talento genera riesgos en las organizaciones sino también la escasez de habilidades en la fuerza laboral [25].

Para combatirlo este flagelo adecuadamente, debemos entender que es el riesgo cibernético. Para [27] es el riesgo empresarial de estar conectado a Internet. Sin embargo, la definición que más se ajusta a las PYMEs dada su realidad comercial, es cualquier riesgo que surja del uso de TIC que comprometan la confidencialidad, disponibilidad o integridad de los datos o servicios [28], [29].

Las deficiencias en la cultura de riesgo, así como la brecha en el mercado laboral de ciberseguridad son los principales obstáculos con respecto a la implementación de la gestión del riesgo cibernético en las PYMEs, estos desafíos son similares en todos los países [29]. Las PYMEs parecen necesitar más apoyo de terceros, como la Academia, para acumular conocimiento y fomentar la sensibilización con el fin de eliminar el exceso de confianza y mejorar la gestión del riesgo cibernético [30]. Es decir, la gestión y preparación ante el riesgo cibernético, emergen como competencias cruciales no solo para la supervivencia sino también para el crecimiento de las pequeñas empresas [31].

Acorde a [29] la literatura sugiere una brecha entre la exposición al riesgo cibernético, la percepción del riesgo cibernético y la preparación percibida por las PYMEs para resistir los riesgos cibernéticos. Por lo que se debe garantizar que la gestión del riesgo cibernético se vea como un problema corporativo y no se delegue en el departamento de TI [30]. Tal como lo recomienda [4] los lideres de las PYMEs deben tener la posibilidad de identificar sus mayores vulnerabilidades al riesgo cibernético; comparar su madurez con la de sus pares con base en un conjunto de medidas estándar; y elegir los esfuerzos de mejora más valiosos. En sintonía con las cinco dimensiones más citadas por la literatura respecto al riesgo cibernético: identificar, proteger, detectar, responder y recuperar [10].

La investigación en seguridad cibernética rara vez se centra en las PYMEs, a pesar de que representan una gran proporción de las empresas [10], en su investigación [11] muestra que algunas características de las PYMEs, como la agilidad, el gran tamaño de la cohorte y la arquitectura de TI fragmentada, podrían permitir una mayor ciberseguridad. Una estrategia de seguridad cibernética eficaz con la gestión de riesgos adecuada proporciona el trampolín para innovar, diferenciarse y en última instancia, generar un crecimiento de los ingresos [32].

Ref. [10] muestra que el 70.0% de las investigaciones en ciberseguridad de las PYMEs han sido cualitativas, un 25.0% cuantitativas y solamente un 5.0% mixtas. Siendo el método de recolección de datos más utilizado, la revisión de literatura (43.0% del total). Esto indica que la investigación mediante encuestas, casos de estudio y experimentos, ha sido limitada. Por lo que investigaciones originales utilizando estos métodos serían altamente deseadas para una mayor comprensión de la problemática, brindando mejores soluciones a este relevante segmento de empresas.

III. Metodología

Es preciso que las PYMEs desarrollen competencias para mejorar la gestión del riesgo cibernético y eliminen el exceso de confianza [28], [29], por lo que se hace necesario conocer su nivel de madurez en ciberseguridad y desarrollar estrategias de concientización para mitigar el riesgo por ciberataques, lo que le permitiría crear una ventaja competitiva.

Como metodología integral, se planteó un estudio sistemático del estado del arte, para el cumplimiento del objetivo de esta investigación, siendo plantear la metodología para habilitar un instrumento que permita evaluar el riesgo cibernético de las PYMEs, así como diseñar la estrategia para que la Academia transfiera el conocimiento a las PYMEs, siguiendo los siguientes pasos:

1) Utilizando la base de datos Scopus, se realizó una busqueda, mediante la cadena de busqueda "*SME**" AND "*cybersecurity*" OR "*cyber risk*" OR "*cyber resilience*".
2) De todos los artículos obtenidos se leyó el *abstract* para verificar que estuvieran dentro del alcance de esta investigación.
3) La base de datos de los artículos se exportó al software Bibliometrix, para obtener a través de la bibliometría, datos cuantitativos que permitieron conocer el estado del arte.
4) Luego se procedió a la lectura completa de las publicaciones con mayor cantidad de citas, al igual que las publicaciones dentro de la espectroscopía o raíces históricas de estas publicaciones, en busca de un instrumento para evaluar la ciberseguridad de las PYMEs y de ubicar en la literatura estrategias para la transferencia de conocimiento a las PYMES.

Dada la experiencia de los autores en la transferencia de conocimiento a las PYMEs, se les solicitó su criterio experto sobre los resultados de la literatura para generar las estrategias.

IV. Resultados

Los resultados para el primer objetivo de esta investigación, en el que se plantea construir una metodología efectiva para la evaluación del riesgo cibernético de las PYMEs, se detallan a continuación:

A. Instrumento para evaluar la ciberseguridad de las PYMEs

1) Se seleccionó la herramienta en idioma inglés propuesta por [4], denominada *Cybersecurity Evaluation Tool* (CET), la cual se compone de 35 preguntas mediante una encuesta en línea a lideres de IT de la empresa, para obtener una auto calificación de la madurez, acorde al marco de ciberseguridad de National Institute of Standards and Technology's (NIST), la cual considera las cinco categorías de identificar, proteger, detectar, responder y recuperar, tal como se muestra en Fig. 1

2) Traducción de la herramienta CET para ser utilizada por empresas hispanoparlantes.

3) Validación de contenido a través de entrevistas cognitivas a cinco empresas del país para validar el contenido de la encuesta. Debido a las diferencias lingüísticas que se dan de un país a otro dada su cultura y costumbres, este paso es necesario de hacer en cada país donde se vaya a implementar.

4) Aplicación del instrumento validado a la unidad de análisis. Definiendo la estrategia de muestreo desde la perspectiva científica, acorde a las medidas tomadas para garantizar la confiabilidad y validez de los resultados.

B. Determinar el nivel de madurez ideal

Consulta a cinco expertos académicos y de la industria con conocimientos en ciberseguridad, en donde por medio de su criterio se determinará el nivel de madurez ideal de ciberseguridad para cada estándar. Seguidamente se calcula un promedio de las puntuaciones de madurez obtenida de las respuestas brindadas por las empresas para cada estándar.

C. Reporte de evaluación para las PYMEs del país

Basado en el nivel de madurez ideal y promedios establecidos para cada estándar, se determinan los niveles por categoría y se generará una tarjeta de reporte CET individual para cada PYME. Con los datos obtenidos se elaboran las conclusiones sobre el estado de ciberseguridad y se brindan recomendaciones para mejorar el nivel de madurez en cada categoría para todas las PYMEs. La Fig. 1 presenta el detalle de las categorías y subcategorías según la herramienta de evaluación CET que se utiliza en el estudio.

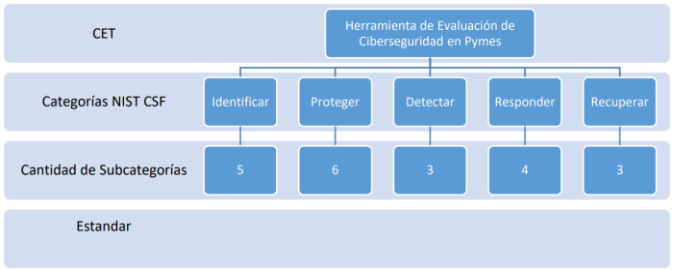

Fig. 1 Categorías y Subcategorías según la herramienta de evaluación CET.

Nota figura adaptada de [4]

Para el segundo objetivo de esta investigación, donde se planteó diseñar la estrategia para que la Academia transfiera el conocimiento a las PYMEs mitigando el riesgo por el uso de TIC, los resultados fueron:

A. Profundizar en las prácticas de ciberseguridad de las PYMEs en el país de estudio, según su nivel de implementación de la transformación digital

A partir de las conclusiones obtenidas en la etapa anterior, construir una guía de temas y preguntas para grupos focales que permita profundizar en la comprensión de los resultados obtenidos. Llevando a cabo grupos focales, divididos en empresas según su nivel de implementación de la transformación digital. Los resultados obtenidos se analizan con el apoyo del software de análisis cualitativo NVivo.

B. Analizar los riesgos de ciberseguridad mediante un enfoque mixto.

Mediante un enfoque mixto se identifican los principales riesgos de ciberseguridad que están presentando las PYMEs del país de estudio, en cada una de las categorías evaluadas y se explican a profundidad con la información proporcionada en los grupos focales.

C. Divulgación de los resultados.

1. Crear un documento con las recomendaciones obtenidas al aplicar estos procedimientos, incluyendo las recomendaciones para minimizar los riesgos de ciberseguridad en las PYMEs del país de estudio. Este documento entregaría al ente regulador de las PYMEs en el país y a las cámaras o asociaciones que reúnan a estas empresas.

2. Talleres de divulgación y seminarios WEB, impartidos por docentes expertos de la Academia a los gerentes de las PYMEs.

3. Divulgación en redes sociales de la universidad.

4. Participación en congresos académicos y publicaciones científicas de los resultados de un sector o país, para que los estudios puedan ser replicados en diversas zonas geográficas.

V. Discusión y Conclusiones

Ref. [33] indica que es necesario sensibilizar a las PYMEs sobre la importancia de la ciberseguridad y prepararlas no solo para defenderse contra un ciberataque, sino también para una rápida y oportuna recuperación ante un posible incidente, por lo que el tema desarrollado en esta investigación es relevante ya que mediante una metodología integral pretende evaluar los riesgos identificados y sugerir recomendaciones para que las PYMEs puedan crear un plan para priorizar e implementar las mejoras más apropiadas para cada caso. Así como desarrollar

y transferir buenas prácticas a las partes interesadas para propiciar una cultura de ciberseguridad, contextualizada en la realidad de cada país, ya que en los programas de concientización se deben de tomar en cuenta los contextos culturales y nacionales [34].

Esta es una investigación novedosa ya que según [10] solamente el 5.0% de las investigaciones en el campo de la ciberseguridad para PYMEs utilizan un enfoque mixto. Además, propone una forma de trabajo conjunto entre la Academia y el sector privado para la promoción de una cultura de ciberseguridad, acorde a lo indicado por [35], las alianzas público-privadas-académicas juegan un papel importante en un plan de acción para la educación en ciberseguridad.

Acorde a [36] para construir una cultura de ciberseguridad, es conveniente que las PYMEs y la Academia trabajen de forma conjunta, porque la ciberseguridad se aborda desde un enfoque interdisciplinario y holístico, con aplicación multilateral. Es por ello que como línea futura se recomienda generar una propuesta de investigación académica, con la participación de escuelas de ingeniería y de administración de empresas, en la cual se aplique la metodología acá expuesta, dado que en un mundo cada vez más interconectado y digitalizado, la creación de un ciberespacio seguro se ha convertido en una prioridad ineludible para la sociedad moderna [37], potenciando el crecimiento y la innovación de las empresas, dando lugar a organizaciones más valiosas y rentables.

REFERENCIAS

[1] J. Rojas-Segura, M. Faith-Vargas, y J. Martinez-Villavicencio, «Conceptualizing digital transformation using semantic decomposition», *Tec Empresarial*, vol. 17, n.º 3, pp. 63-75, dic. 2023, https://doi.org/10.18845/te.v17i3.6850

[2] A. Sukumar, H. A. Mahdiraji, y V. Jafari-Sadeghi, «Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors», *Risk Analysis*, 2023, doi: 10.1111/risa.14092.

[3] V. Jafari-Sadeghi, A. Garcia-Perez, E. Candelo, y J. Couturier, «Exploring the impact of digital transformation on technology entrepreneurship and technological market expansion: The role of technology readiness, exploration and exploitation», *Journal of Business Research*, vol. 124, pp. 100-111, ene. 2021, doi: 10.1016/j.jbusres.2020.11.020.

[4] M. Benz y D. Chatterjee, «Calculated risk? A cybersecurity evaluation tool for SMEs», *Business Horizons*, vol. 63, n.º 4, pp. 531-540, jul. 2020, doi: 10.1016/j.bushor.2020.03.010.

[5] S. S. Baggott y J. R. Santos, «A Risk Analysis Framework for Cyber Security and Critical Infrastructure Protection of the U.S. Electric Power Grid», Risk Analysis, vol. 40, n.o 9, pp. 1744-1761, 2020, doi: 10.1111/risa.13511.

[6] ENISA, «Cybersecurity for SMEs - Challenges and Recommendations». The European Union Agency for Cybersecurity, junio de 2021. https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

[7] C. Ponsard, J. Grandclaudon, y S. Bal, «Survey and Lessons Learned on Raising SME Awareness about Cybersecurity.», en *ICISSP*, 2019, pp. 558-563. doi: 10.5220/0007574305580563.

[8] MICITT, «Estrategia Nacional de Ciberseguridad de Costa Rica 2017», Ministerio de Ciencia, Tecnología y Telecomunicaciones, San Jose, Costa Rica, ISBN: 978-9968-732-52-9, 2017. https://www.micitt.go.cr/wp-content/uploads/2022/05/Estrategia-Nacional-de-Ciberseguridad-Costa-Rica-Oficial.pdf

[9] MICITT, «Revisión de la Estrategia Nacional de Ciberseguridad de Costa Rica (2017)», Ministerio de Ciencia, Tecnología y Telecomunicaciones, San Jose, Costa Rica, 2021. https://www.micitt.go.cr/wp-content/uploads/2022/05/Revision-de-la-Estrategia-Nacional-de-Ciberseguridad-de-Costa-Rica-2017.pdf

[10] A. Chidukwani, S. Zander, y P. Koutsakis, «A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations», *IEEE Access*, vol. 10, pp. 85701-85719, 2022, doi: 10.1109/ACCESS.2022.3197899.

[11] T. Tam, A. Rao, y J. Hall, «The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses», *Computers & Security*, vol. 109, p. 102385, oct. 2021, doi: 10.1016/j.cose.2021.102385.

[12] C. Abraham, D. Chatterjee, y R. R. Sims, «Muddling through cybersecurity: Insights from the U.S. healthcare industry», *Business Horizons*, vol. 62, n.º 4, pp. 539-548, 2019, doi: 10.1016/j.bushor.2019.03.010.

[13] T. Semrau, T. Ambos, y Sascha Kraus, «Entrepreneurial orientation and SME performance across societal cultures: An international study», *Journal of Business Research*, vol. 69, n.º 5, pp. 1928-1932, may 2016, doi: 10.1016/j.jbusres.2015.10.082.

[14] F. Eggers, «Masters of disasters? Challenges and opportunities for SMEs in times of crisis», *Journal of Business Research*, vol. 116, pp. 199-208, ago. 2020, doi: 10.1016/j.jbusres.2020.05.025.

[15] M. C. Fernández y P. Puig, «Los Desafíos del Comercio Electrónico para Las PyME Principales Claves en El Proceso de Digitalización», BID, Whashington, DC, ene. 2022. https://publications.iadb.org/es/los-desafios-del-comercio-electronico-para-las-pyme-principales-claves-en-el-proceso-de

[16] M. Faith, J. C. Leiva, y R. Mora, «Las Pymes en Costa Rica», en *Los efectos de la digitalización, inteligencia artificial, big data e industria 4.0 en el trabajo de las Pymes en Latinoamérica*, Konrad-Adenauer-Stiftung e.V y la Universidad Católica del Uruguay., I. Bartesaghi y W. Weck, Eds., en Primera edición. , Panamá, 2022. https://www.kas.de/en/web/regionalprogramm-adela/single-title/-/content/los-efectos-de-la-digitalizacion-inteligencia-artificial-big-data-e-industria-4-0-en-el-trabajo-de-l

[17] I. Bartesaghi y W. Weck, Los efectos de la digitalización, inteligencia artificial, big data e industria 4.0 en el trabajo de las Pymes en Latinoamérica, Konrad-Adenauer-Stiftung e.V y la Universidad Católica del Uruguay. en Primera edición. Panamá, 2022. https://www.kas.de/en/web/regionalprogramm-adela/single-title/-/content/los-efectos-de-la-digitalizacion-inteligencia-artificial-big-data-e-industria-4-0-en-el-trabajo-de-l

[18] Mi. de Bruycker y C. Darville, «Cyber Security Guide for SME, Foreword». Centre for Cyber Security Belgium, 20 de enero de 2017. https://ccb.belgium.be/en/document/guide-sme

[19] ITU, «Global Cybersecurity Index 2020», International Telecommunication Union, U.N., Geneve, Switzerland., 2022. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

[20] B. Weinelt, «Digital Transformation of Industries». World Economic Forum, 2016. www.accenture.com/_acnmedia/accenture/conversion-assets/wef/pdf/accenture-digital-enterprise.pdf

[21] A. Horn, «Cybersecurity Should Be a Top Concern for Middle-Market Companies», SmallBizDaily. https://www.smallbizdaily.com/cybersecurity-middle-market-companies/

[22] WEF, «Global Cybersecurity Outlook 2022», 2022. https://www.weforum.org/reports/global-cybersecurity-outlook-2022/

[23] The Government of Japan, «Cybersecurity for All». Setiembre de 2021. https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf

[24] M. N. Y. Marican, S. Abd Razak, A. Selamat, y S. H. Othman, «Cyber Security Maturity Assessment Framework for Technology Startups: A

Systematic Literature Review», *IEEE Access*, vol. 11, pp. 5442-5452, 2023, doi: 10.1109/ACCESS.2022.3229766.
[25]OEA y CISCO, «Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades». Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo, 2023. https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf
[26](ISC)², «A Resilient Cybersecurity Profession Charts the Path Forward (ISC)2 CYBERSECURITY WORKFORCE STUDY, 2021», International Information System Security Certification Consortium, 2021. https://www.isc2.org/About/~/-/media/F829F79ADBDC4F6391432B7D122DA32E.ashx
[27]L. A. Gordon, M. P. Loeb, y T. Sohail, «A framework for using insurance for cyber-risk management», *Commun. ACM*, vol. 46, n.º 3, pp. 81-85, mar. 2003, doi: 10.1145/636772.636774
[28]M. Eling y W. Schnell, «What do we know about cyber risk and cyber risk insurance?», *The Journal of Risk Finance*, vol. 17, n.º 5, pp. 474-491, ene. 2016, doi: 10.1108/JRF-09-2016-0122.
[29]F. Hoppe, N. Gatzert, y P. Gruner, «Cyber risk management in SMEs: insights from industry surveys», *The Journal of Risk Finance*, vol. 22, n.º 3/4, pp. 240-260, ene. 2021, doi: 10.1108/JRF-02-2020-0024.
[30]P. Ferreira de Araújo Lima, M. Crema, y C. Verbano, «Risk management in SMEs: A systematic literature review and future directions», *European Management Journal*, vol. 38, n.º 1, pp. 78-94, feb. 2020, doi: 10.1016/j.emj.2019.06.005.
[31]D. Chatterjee, «Should executives go to jail over cybersecurity breaches?», *Journal of Organizational Computing and Electronic Commerce*, vol. 29, n.º 1, pp. 1-3, 2019, doi: 10.1080/10919392.2019.1568713.
[32]G. Lloyd, «The business benefits of cyber security for SMEs», *Computer Fraud & Security*, vol. 2020, n.º 2, pp. 14-17, ene. 2020, doi: 10.1016/S1361-3723(20)30019-1.
[33]O. Bustillos Ortega y J. Rojas Segura, «Protocolo básico de ciberseguridad para pymes», *Interfases*, n.º 016, Art. n.º 016, dic. 2022, https://doi.org/10.26439/interfases2022.n016.6021
[34]R. Herkanaidu, S. M. Furnell, y M. Papadaki, «Towards a cross-cultural education framework for online safety awareness», *Information & Computer Security*, vol. 29, n.º 4, pp. 664-679, ene. 2021, doi: 10.1108/ICS-11-2020-0183.
[35]OEA y AWS, «Alfabetización y Seguridad Digital: La importancia de mantenerse seguro e informado». Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo, 2020. https://www.oas.org/es/sms/cicte/docs/20200925-ESP-White-Paper-Educacion-en-Ciberseguridad.pdf
[36]O. Bustillos Ortega y J. Rojas Segura, «Cómo promueven los estados la ciberseguridad de las PYMEs», *Interfases*, n.º 017, Art. n.º 016, 2023, https://doi.org/10.26439/interfases2023.n017.6246
[37]O. Bustillos Ortega, J. Rojas Segura, y J. Murillo-Gamboa, «Ciberseguridad y desarrollo de habilidades digitales: propuesta de alfabetización digital en edades tempranas», *Interfases*, n.º 018, Art. n.º 018, dic. 2023, https://doi.org/10.26439/interfases2023.n018.6626