ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

Buenas Prácticas de Ciberseguridad para PYMES: Revisión de Experiencias Internacionales

Best Cybersecurity Practices for SMEs: A Review of International Experiences

Hercilia Cerrud de Dominguez
Universidad de Panamá. Centro Regional Universitario de Azuero. Panamá
Hercilia.cerrud@gmail.com
https://orcid.org/0009-0006-2719-330X

Diana Maritza Mendoza Ávila
Universidad de Panamá. Centro Regional Universitario de Azuero. Panamá
mendozadiana454545@gmail.com
https://orcid.org/0000-0001-9402-166X

Diana Valdés Mendoza
Dell Technologies. Panamá
diana.valdes25@gmail.com
https://orcid.org/0009-0008-8784-0913

Recibido: 9/05/2025 *Aprobado: 20/06/2025*

DOI: https://doi.org/10.48204/2992-6629.7637

Resumen

En el presente trabajo, se reúne una revisión de la literatura sobre las buenas prácticas de ciberseguridad que utilizan las pequeñas y medianas empresas (pymes) en el ámbito internacional. En base a la investigación de documentos académicos, informes de instituciones y estudios de caso en América Latina, Europa y Asia, se determinan las mejores prácticas de ciberseguridad que realizan estas organizaciones. La toma de contraseñas, la capacitación periódica del personal, las copias de seguridad y la aplicación de marcos normativos como el ISO/IEC 27001 y el NIST son algunas prácticas que merecen ser enfatizadas. También se estudian los factores que favorecen su adecuada implementación, ya sea el compromiso de la alta dirección, la disponibilidad de recursos adaptados o las ayudas de las organizaciones que puedan realizar su promoción. Los resultados muestran que las pymes, a pesar de sus limitaciones, pueden mejorar su ciberseguridad mediante prácticas que son perfectamente realizables. El trabajo finaliza con recomendaciones prácticas y propuestas para políticas públicas que tiendan la mano a la digitalización segura de este tipo de empresas.

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

Palabras clave: gestión de la ciberseguridad, pequeñas y medianas empresas, buenas prácticas en seguridad de la información, transformación digital empresarial, gestión de riesgos cibernéticos.

Abstract
The current article provides a literature review on cybersecurity best practices used by small and medium-sized enterprises (SMEs) around the world. Through the assessment of academic literature, institutional reports, and case studies from Latin America, Europe and Asia, the article explores the best cybersecurity practices adopted by SMEs. The best cybersecurity practices identified were: password management; constant user training; enforce regular data backups; and, using cybersecurity regulations like ISO/IEC 27001, and NIST. In addition, the article critically analyzed success factors like executive leadership, availability of scaled resources, and working with cybersecurity institutions. Overall, while SMEs often have limited resources, it was determined that the many ways they can enhance their cybersecurity posture are strategic and easily accessibility. The article concludes with practical strength recommendations and public policy recommendations for enabling SMEs to assist their secure digital transformation.
Keywords: cybersecurity management, small and medium-sized enterprises, information security best practices, digital business transformation, cyber risk management.

Introducción

En la actualidad, en un entorno digital caracterizado por una conectividad constante, acceso remoto a los datos y una creciente dependencia de las plataformas tecnológicas, la ciberseguridad se ha convertido en una cuestión crítica para la sostenibilidad y la competitividad de las organizaciones, cualquiera sea su tamaño. Y las pequeñas y medianas empresas (PYMES), que constituyen la espina dorsal de la economía internacional, ya que representan cerca del 90 % de las empresas y que producen más del 50 % del empleo formal (Banco Mundial, 2021), se enfrentan a situaciones concretas a tal respecto. Bueno, su escasa capacidad económica, escasa disponibilidad de personas especializadas y también la falta de

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

marcos normativos adaptados a su realidad les hace ser especialmente vulnerables frente a las amenazas cibernéticas.

De toda manera, las PYMES no son organismos pasivos frente al riesgo las experiencias internacionales demuestran que con el enfoque adecuado y con la aplicación de buenas prácticas adaptadas puede fortalecer la postura en ciberseguridad de las PYMES. A tal efecto, las buenas prácticas en ciberseguridad —entendidas como estrategias, políticas, procedimientos y tecnologías encaminadas a prevenir, detectar, responder y recuperarse ante incidentes informáticos— se convierten en herramientas clave para poder promover la resiliencia de la empresa.

El propósito de este artículo es, mediante una revisión bibliográfica sistemática, analizar qué experiencias internacionales existen sobre la implementación de buenas prácticas de ciberseguridad en las PYMES. A partir de la consulta de estudios académicos, informes técnicos y documentos institucionales correspondientes a lo publicado entre 2018 y 2024 se han podido identificar los mejores enfoques aplicados en las distintas regiones del mundo (América Latina, Europa; Asia) y en los distintos sectores económicos, así como los factores que ayudan o dificultan su implementación o los resultados al que se les ha llegado y las lecciones aprendidas que pueden ser replicadas o adaptadas a otros contextos.

El análisis no se limita a realizar una simple descripción de aquellas prácticas que pueden ser consideradas exitosas, sino que se busca dotarla de un sentido crítico y propositivo, donde se intenten analizar las condiciones sobre el compromiso organizacional, la formación continua, la colaboración multisectorial, la contextualización, como condicionantes del éxito para estas prácticas. Asimismo, se presentan las discusiones sobre

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

la implementación de los resultados obtenidos en relación al diseño de políticas públicas o de los programas que se deben desarrollar para el fortalecimiento de la ciberseguridad de las PYMES. En definitiva, el presente artículo ayuda a comprender el estado de la ciberseguridad en las empresas de menor tamaño y propone una base sólida de conocimiento para la toma de decisiones en términos de protección digital. Y su último objetivo es aportar a la construcción de una cultura organizacional que incorpore la ciberseguridad como eje transversal del desarrollo empresarial sostenible en la era digital.

Contextualización

Las pequeñas y medianas empresas (PYMES) representan un grupo significativo en las economías mundiales. El Banco Mundial (2021) indica que las PYMES son en torno al 90% de las empresas en el mundo y que crean más del 50% de los puestos de trabajo formal. Son especialmente importantes en los países en desarrollo, donde constituyen el motor del crecimiento económico, la innovación y la inclusión social; a pesar de su importante papel, no están exentas de ser especialmente frágiles a nuevas amenazas, entre ellas, los riesgos de la seguridad de la información.

En un contexto en que la transformación digital avanza en un proceso continuamente creciente, las PYMES también deben realizar o facilitar la integración de las tecnologías de información para poder competir. Esta tarea, sin embargo, puede ser compleja cuando se empezaran a incluir las tecnologías de información y los activos digitales en el proceso de digitalización de las PYMES, así como también en su proceso de adopción de servicios de nube, plataformas digitales y software especializado. Por ello, este nuevo proceso digitalización puede conllevar también nuevos, y complejos, retos en relación a la protección

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

de sus activos digitales. Las PYMES están expuestas a nuevas y recientes amenazas cibernéticas como son el ransomware, el phishing, las violaciones de datos y los ataques de denegación de servicio que les pueden llegar a crear grandes pérdidas de negocio en relación a sus activos digitales y su seguridad (Luján Rodas et al., 2023).

La problemática se desarrolla con mayor intensidad en el sentido de que las PYMES poseen menos recursos técnicos y financieros que las grandes empresas, de modo que resultan incapaces de adoptar medidas de seguridad que sean potentes. En este sentido, Díaz Chantre (2023) señala que la escasa inversión en sistemas de ciberseguridad en las empresas del sector industrial en Colombia pone de manifiesto la gran distancia que existe entre las necesidades de protección y las capacidades efectivas de las entidades. En muchas ocasiones las empresas no poseen personal especializado en Tecnologías de la información y no tienen políticas internas claras en relación a la protección de los datos, por lo que están constantemente expuestas al riesgo.

En América Latina, la situación se torna realmente compleja. Muchas PYMES operan en contextos regulatorios debidamente poco desarrollados en ciberseguridad, lo que les terminará impidiendo alinearse con estándares internacionales como ISO/IEC 27001 o NIST. Esto transcurre en el cuadro de esfuerzos regionales llevados a cabo por entidades como la OEA, que ha promovido marcos de ciberseguridad y programas de formación, no obstante, los niveles de madurez en ciberseguridad siguen siendo desiguales (OEA, 2020). En Ecuador, por ejemplo, se ha podido observar a partir de los trabajos de López-Anchala y Ordóñez-Parra (2024), una baja frecuencia de auditorías de seguridad de la información en empresas comerciales, lo que da cuenta de una no cultura preventiva frente las amenazas digitales.

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

Junto a ello, otros estudios realizados en Paraguay concluyeron sin embargo, que el bajo nivel de capacitación del personal y la no existencia de estrategias de protección de datos son dos de los principales factores que explican los obstáculos a la transformación digital de las PYMES (Luján Rodas et al., 2023), situación que también se replicará en otros países de la región. En el propio México, Hernández et al. (2018) nos comentan que las PYMES suelen ser objetivos de ataques y que muchas no cuentan con protocolos para responder a incidentes de ciberseguridad.

Por el contrario, hay algunos modelos que han sido implementados con éxito por algunas diferentes partes, que pueden servir de ejemplo. El programa "Cyber Essentials" en Singapur ha sido configurado específicamente para las necesidades de ciberseguridad de las pequeñas empresas mediante una guía práctica y la obtención de la certificación para que estas mismas PYMES creen una buena base de la que poder partir en la ciberseguridad (CSA 2022). Y en el caso de Europa, la ENISA produce recomendaciones en función de la realidad de las pequeñas empresas, para la formación del personal, la gestión de las contraseñas o la actualización de sistemas (ENISA 2021).

Es fácil suponer que, en este contexto, la ciberseguridad debería dejar de considerarse una carga que fatiga aún más a las PYMES, para pasar a ser tratada como una ventaja competitiva para el sostenimiento de éstas mismas. Las enseñanzas internacionales ponen de relieve que llegar a un nivel razonable de protección no necesita una infraestructura referente a la cuestión costosa, al contrario, se exige la voluntad de la propia organización, el conocimiento de las buenas prácticas adaptadas y acciones de políticas públicas sobre esta cuestión que sirvan para fomentar la producción y la interacción de los sectores.

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

De este modo, el conocimiento del contexto concreto de desarrollo de las PYMES y los retos estructurales que estas deben afrontar en el ámbito de la ciberseguridad permite diseñar soluciones efectivas y sostenibles que garanticen la integridad, confidencialidad y disponibilidad de su información, así como de la información con la que interactúan en el marco de la economía digital contemporánea. De esta forma, logramos entender mejor los retos de la economía digital contemporánea.

Pregunta de Revisión

La formulación de una pregunta de revisión clara, específica y contextualizada es fundamental para guiar un estudio bibliográfico de manera efectiva. En el marco de este trabajo, la pregunta central planteada es: ¿Qué buenas prácticas han demostrado efectividad en la protección cibernética de las PYMES a nivel internacional?

Esta cuestión se origina en una necesidad real y urgente. Las PYMES han sido claramente protagonistas en las últimas décadas de todo un proceso de transformación digital sin precedentes; un proceso de transformación digital que es fruto del aumento gradual de usos de herramientas tecnológicas que, si bien mejoran tanto su productividad como sus posibilidades comerciales, las vuelven también más vulnerables a las amenazas cibernéticas. Como evidencian, en sus resultados, López-Anchala y Ordóñez-Parra (2024) muchas de estas organizaciones no cuentan con ningún tipo de controles formales de seguridad y no llevan a cabo auditorías de ciberseguridad de manera periódica, lo que llega a comprometer su propia resiliencia ante o frente incidentes digitales.

De esta manera, se deberá identificar alguna práctica que sea efectiva y viable para empresas con limitaciones económicas, con contados técnicos y con escasa infraestructura.

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

La pregunta de investigación no tiene como objetivo exclusivo conocer qué prácticas existen, sino en última instancia saber cuáles de éstas han dado buenos resultados en la vida real, sobre todo en aquellos contextos que se asemejan a las PYMES de América Latina y otras regiones emergentes.

Diferentes investigaciones han evidenciado que la comprensión del impacto de una práctica de ciberseguridad no tiene que ver con las posibilidades técnico-instrumentales que la propia práctica de ciberseguridad ofrece, sino con la capacidad de la práctica para adecuarse a las características del entorno organizacional, la cultura institucional y la normativa en la que inscribe la práctica de ciberseguridad. Por caso, en Colombia, el autor Díaz Chantre (2023) ha puesto de manifiesto el hecho de que, gracias a la progresiva adopción de estándares tales como ISO 27001 o NIST y aún en empresas medianas dentro del sector industrial, disminuyen significativamente los incidentes de seguridad, siempre que, y cuando las prácticas vengan acompañadas, a su vez, de un compromiso por la dirección y de la formación del personal.

De igual modo, en relación a la realidad del país del Paraguay, Luján Rodas et al. (2023) reseñan que una de las barreras más importantes para llevar adelante buenas prácticas no es la falta de herramientas, como podría pensarse, sino la falta de instrumentación de una estrategia formativa sostenida y adaptada a las capacidades de las pequeñas y medianas empresas del lugar. Esta situación también es típica en muchos países de América Latina y evidencia la necesidad de un compendio validado de buenas prácticas no solo a nivel técnico, sino también a nivel implementación y sustentable.

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

Por otra parte, el interés por prácticas "efectivas a nivel internacional" es también consecuencia del ida y vuelta entre el reconocimiento de que si bien la ciberseguridad es un fenómeno mundial, su abordaje requiere enfoques adaptativos. Así, la experiencia europea ilustra que la promoción de guías de acción concretas como las del ENISA (2021) permite a las PYMES el acceso a medidas básicas —gestión de contraseñas, actualización de sistemas, formación continua— que disminuyen drásticamente la exposición al riesgo.

Por la misma razón, iniciativas como "Cyber Essentials" en Singapur son ejemplos de la exitosa implementación de programas de transferencia del conocimiento, combinados con el apoyo institucional hacia empresas pequeñas que necesitan directrices sencillas pero efectivas (CSA, 2022). Este tipo de modelos centrados en la accesibilidad y en la certificación del cumplimiento ofrecen un modelo que se puede replicar y que es adaptable en países latinoamericanos y en otras áreas en vías de desarrollo.

La correspondiente formulación de esta pregunta permite hacer preguntas complementarias a modo de subpreguntas que contribuyen a tal análisis como son las siguientes: ¿Qué sectores (comercio, manufactura, servicios) dan cuenta de un avance mayor en la implementación de prácticas seguras? ¿Qué factores del contexto (cultural, económico, normativo) facilitan o dificultan la implementación de prácticas seguras para las empresas? ¿Qué indicadores se usan para dar cuenta de la efectividad de una práctica de ciberseguridad en una PYME?

Por ello, la pregunta central no solamente da cuerpo a la búsqueda y selección de fuentes, sino que articula los objetivos del estudio con una necesidad concreta de conocimiento aplicable: la de facilitar a las pymes disponer información verificada,

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

contextualizada y útil para mejorar su contexto frente a los desafíos impuestos por la ciberseguridad propia de una era moderna.

Metodología

La investigación que se presenta se sitúa en un tipo de metodología cualitativa de tipo descriptiva y exploratoria, centrada en el análisis de experiencias documentadas sobre la implementación de buenas prácticas de ciberseguridad en pequeñas y medianas empresas (PYMES) a escala internacional; la cual permite aprehender las buenas prácticas implementadas por distintos países y sectores a la hora de mitigar los riesgos cibernéticos en organizaciones de menor tamaño, así como su efectividad y aplicabilidad en otras contextos.

Diseño de investigación

La metodología utilizada fue una revisión bibliográfica sistematizada basada en la recopilación y la organización del análisis y de la interpretación de fuentes informáticas y académicas. Se partió del reconocimiento de una problemática recurrente en distintas regiones que han realizado estudios similares: la vulnerabilidad de las PYMES ante las cada vez más crecientes amenazas digitales y su escasa implementación de medidas de seguridad efectivas. Por lo expuesto, la revisión fue orientada a la identificación de aquellas prácticas que bien pueden ser recomendadas por instituciones especializadas, pero que, además, la comunidad científica ha abordado con unos resultados que pueden ser medidos en las distintas realidades nacionales.

Selección de fuentes

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

Las fuentes que fueron consultadas comprenden publicaciones académicas, documentos institucionales y técnicos de organismos internacionales. Se incluyen, a modo de ejemplo, informes provenientes de la Agencia de la Unión Europea para la Ciberseguridad (ENISA); de la Organización de los Estados Americanos (OEA); de la Agencia de Seguridad Cibernética de Singapur (CSA); así como artículos extraídos de revistas científicas indexadas en bases como Scopus, Scielo o Latindex. Se integraban, además, estudios de caso que formaban parte de trabajos de grado universitarios que trataban la implementación de marcos de seguridad como TOGAF, ISO/IEC 27001, COBIT y NIST, en especial en el caso colombiano (Díaz Chantre, 2023; Bolaño Rocha & Amaya Corredor, 2023).

Para asegurar la actualización y pertinencia de la información, se seleccionaron documentos cuya publicación oscilara entre los años 2018 y 2024, priorizando los documentos que describen prácticas en el contexto de PYMES y que a su vez incluyen evidencias de resultados, indicadores o análisis comparados. El criterio de inclusión fundamental es el de la pertinencia del tema de ciberseguridad y su aplicación en pequeñas empresas. En sentido opuesto, se han excluido documentos que se centran exclusivamente en grandes empresas o que no cuenten con sustento empírico en base a evidencia.

Procedimiento de Análisis

Una vez elegidas las fuentes, la información se codificó de manera temática, es decir que se categorizaron los datos a través de categorías analíticas predefinidas: (1) prácticas de ciberseguridad documentadas; (2) marcos normativos y técnicos; (3) sectores económicos; (4) resultados y (5) barreras y facilitadores de implementación. Esta forma de hacer categorización se trató de un proceso manual siguiendo los principios de análisis cualitativo

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

que establecían Miles y Huberman (1994), facilitando así el poder descubrir patrones repetidos entre categorías, relaciones causales y discrepancias entre experiencias.

Además, también se vis-to un proceso de triangulación de fuentes institucionales y de trabajos académicos para comprobar la consistencia de los hallazgos y enriquecer el análisis desde diferentes visiones. De la misma forma, con los trabajos de América Latina, como el estudio de López-Anchala & Ordóñez-Parra (2024) en Ecuador y el estudio de Luján Rodas et al. (2023) en Paraguay, se verificaron los hallazgos de los trabajos con políticas promovidas por organismos como la OEA y con las guías para la implementación que se promovían con ENISA y con CSA.

Consideraciones éticas y limitaciones

Dado que el estudio se realiza exclusivamente a partir de fuentes secundarias, ni entrevistas ni encuestas a personas resulta un instrumento de recolección de datos necesario. No obstante, se han respetado los principios de la integridad académica, a través de la correcta citación de cada fuente y la adecuada utilización de los contenidos analizados. Se reconocen a modo de principales limitaciones del estudio depender de la información previamente publicada, la escasa disponibilidad en algunos de los estudios consultados de indicadores cuantitativos específicos e incluso la heterogeneidad de ciertos contextos analizados, lo que puede dar lugar a una difícil comparación entre ellos.

Conclusión metodológica

La metodología que se usa facilita la posibilidad de construir un armazón analítico muy completo y variado que reúne conocimientos académicos y/o conocimientos técnicos, desde planteamientos normativos hasta experiencias prácticas en diferentes lugares del

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

mundo. Esta metodología da lugar a una construcción muy completa del armazón analítico y, a su vez, a poder dar respuesta a la cuestión de investigación, generar recomendaciones adaptadas a las realidades de las PYMES, y en particular para situaciones de escasez de recursos y de elevada exposición a los riesgos digitales.

Revisión de buenas prácticas por Región o Sector

La revisión regional y sectorial de las buenas prácticas en ciberseguridad implementadas por PYMES permite entender las diferencias en la adopción de medidas según los contextos culturales, económicos y regulatorios. En este apartado revisamos algunas experiencias concretas desde América Latina, Europa o Asia, así como notables diferencias entre sectores, como el sector de servicios o el de manufactura. Esta revisión permite tener una lectura comparativa para saber cómo implementar las prácticas efectivas en ciberseguridad en cada entorno empresarial.

América Latina

En el territorio de América Latina, las pequeñas y medianas empresas (PYMES) deben afrontar una situación caracterizada por sus presupuestos limitados, su baja capacitación técnica, debilidad institucional en materia de ciberseguridad. Sin embargo, varias naciones han implementado iniciativas que analizan sus experiencias positivas. La Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) han fomentado el desarrollo de competencias a través de talleres, diagnósticos de madurez cibernética y alianzas público-privadas (OEA, 2020). De esta forma, han puesto en manifiesto la posibilidad de poder adoptar marcos normativos simplificados, orientados a las capacidades reales de las PYMES.

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

En el país sudamericano Colombia, han aparecido avances significativos en la integración de marcos propuestos como ISO/IEC 27001 e NIST (National Institute of Standards and Technology) pero que están especialmente relacionados con sectores industriales y de servicios que han descrito a la ciberseguridad como factor estratégico. Investigaciones como las de Díaz Chantre (2023) registran la práctica de controles mínimos como la gestión de contraseñas, la realización de copias de seguridad de forma automatizada, el establecimiento de políticas de acceso y la formación continua, que han permitido mejorar, de forma significativa, la postura de seguridad de empresas de tamaño medio del sector productivo.

En el país de Ecuador, por otro lado, las empresas que pertenecen al sector comercial han mantenido una baja frecuencia en auditorías de seguridad cibernética, ya que incluso algunas organizaciones han empezado a implementar medidas básicas de protección, entre las que cabe mencionar la implementación de firewalls, antivirus actualizados y la capacitación del personal. Con esto, se comprobará que, tal y como lo afirman López-Anchala & Ordóñez-Parra (2024), solo un 16,67% de las empresas encuestadas llevaban a cabo auditorías anuales, hecho que nos muestra una necesidad urgente de institucionalizar dichas auditorías.

El caso de Paraguay es otro ejemplo de carácter ilustrativo. Luján Rodas et al. (2023) abordan que la formación del personal en habilidades digitales es una de las prácticas más efectivas para que las organizaciones avancen en materia de seguridad informática. Las PYMES que invirtieron en los procesos formativos y la sensibilización de sus trabajadores

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

mostraron mejoras en la detección de amenazas o en las buenas prácticas, como puede ser el uso de autenticación multifactor o actualización oportuna del software.

Europa

Europá, por otro lado, ha sido la principal impulsora de las políticas inclusivas de ciberseguridad para las pequeñas empresas. La Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha emitido muchos documentos de buenas prácticas dirigidos de forma específica a PYMES. Entre las prácticas recomendadas están la identificación y la catalogación de los activos digitales, los planes de respuesta a incidentes, la realización de auditorías internas periódicas, así como el cumplimiento normativo del Reglamento General de Protección de Datos (GDPR) (ENISA, 2021).

Un elemento destacable del enfoque europeo es la normalización de los procedimientos. Muchas empresas gravan sus procedimientos alineándose a marcos como ISO/IEC 27001 o COBIT, no como requisitos complejos, sino como marcos bases adaptables por tamaño y sector de la empresa. Esas recomendaciones involucran por ejemplo un comienzo usando controles básicos que incluyen revisión periódica de accesos, educación de los funcionarios y soluciones anti-malware automáticas.

Asia

En Asia es importante mencionar el caso de Singapur con la Cyber Security Agency (CSA) ha desarrollado el modelo “Cyber Essentials” que va dirigido a empresas de pequeña y mediana dimensión con un marco práctico de cinco pilares: actualización de sistemas, control de accesos, respaldo de datos, protección contra malware y concienciación de los empleados. La estrategia incluye la certificación para aquellas empresas que cumplan los

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

requerimientos mínimos según los cuales no sólo mejora su seguridad, sino que incrementa la confianza de sus socios comerciales y también la de sus clientes (CSA, 2022).

La perspectiva asiática da gran importancia la colaboración entre gobierno y sector privado, como por ejemplo, la que se lleva a cabo en Singapur, donde se otorgan subvenciones a las PYMES para que accedan a soluciones de seguridad y formación, lo cual ha promovido la participación activa de las mismas en programas de empoderamiento digital.

Sector Servicios vs. Manufactura

Las diferencias existentes en los sectores también determinan la forma de aplicar buenas prácticas. En el sector servicios, las PYMES apuestan en primer lugar por la protección de los datos personales y la privacidad del cliente, todo ello en función del contenido del tipo de información que se suele manejar. Las medidas más comunes en este sector son las que aplican el uso de cifrado de las comunicaciones, la firma digital de los documentos, y las que han formalizado la adopción de normativas como el GDPR y la Ley de Protección de Datos Personales en los países de América Latina. La formación del personal por capacidad para detectar ataques phishing o ransomware es una medida que cobra especial fuerza, dado que el personal puede ser el primer eslabón de defensa (López-Anchala & Ordóñez-Parra, 2024).

Aunque en otros entornos de trabajo dentro de la manufactura se buscan sobre todo, la protección de los sistemas industriales, la red interna y cualquier otro servicio asociado al propio sector, resultarían ser las preocupaciones principales la continuidad operativa y la integridad de los procesos productivos, llevarían a fomentar criterios como los controles de acceso físico, la segmentación de redes industriales (OT) y el uso de mecanismos de

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

monitoreo en tiempo real. En términos de lo que indican Bolaño Rocha & Amaya Corredor (2023), la combinatoria de marcos de arquitectura empresarial como TOGAF resulta ser efectivo para la identificación de los riesgos, la elaboración de planes de transición, la mejora de las capacidades de respuesta a incidentes en el entorno de la producción.

Análisis de resultados

La recolección de experiencias internacionales y sectoriales permite constatar regularidades y líneas de trabajo puestas en práctica por las buenas prácticas de ciberseguridad en las PYMES. La recolección de experiencias internacionales y sectoriales está estructurada a partir de tres subdimensiones: las prácticas emergentes, los resultados reportados y los indicadores de éxito, lo cual permite identificar el contenido de las acciones a implementar y su impacto resumido y concretado en las organizaciones.

Prácticas más recurrentes

Un uso habitual de la protección contra la entrada de atacantes es la creación de políticas de contraseñas fuertes, las cuales son vistas como una primera línea de defensa a accesos no autorizados. Esta política se lleva a cabo mediante requerimientos de combinaciones complejas, mediante autenticación de múltiples factores (MFA), buscando la rotación de claves durante un tiempo impuesto, mientras que trabajos como, por ejemplo, el de Díaz Chantre (2023), el cual pone de manifiesto que muchas entidades en Colombia, apuestan por estas herramientas como parte de un paquete mínimo de controles básicos siguiendo las pautas que marcan los marcos como NIST e ISO/IEC 27001.

Una práctica igualmente importante es la de la actualización de software y sistemas operativos, que se utiliza para corregir vulnerabilidades previamente conocidas que puedan

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

ser utilizadas por los atacantes. Dicha práctica necesita tratar la gestión de parches, escanear vulnerabilidades del sistema, la automatización de procesos de la actualización... mientras que ENISA (2021) y CSA (2022) la resaltan como una de las mejores prácticas que puede emplearse para reducir la exposición al riesgo, especialmente en sistemas heredados o aquellos que cuentan con algún tipo de conectividad.

La formación y la concienciación del personal, también se encuentran entre las prácticas que se repiten constantemente. En la medida en que el factor humano aparece con frecuencia entre los vectores más comunes involucrados en los incidentes de seguridad —por ej., el phishing, la ingeniería social, los errores de gestión de la configuración—, numerosos trabajos de investigación destacan la necesidad de realizar formaciones para reducir los incidentes maliciosos. En el estudio que desarrollaron López-Anchala y Ordóñez-Parra (2024) indicaban que el factor humano es un factor necesario para la gran mayoría de empresas ecuatoriana, dando la circunstancia de que son escasas en su implementación.

Finalmente, realizar copias de seguridad periódicas, así como practicar planes de recuperación ante la caída del sistema, pertenecen a estas prácticas mínimas de fortalecimiento, siendo este tipo de prácticas que suelen repetirse con mayor frecuencia. Realizar estas acciones permite garantizar la disponibilidad de la información y la recuperación de los sistemas operativos frente a ransomware o fallos graves. ENISA (2021) y CSA (2022) concluyen que las empresas que cuentan con un respaldo local y en la nube son las que mejor preparadas están para responder ante incidentes e impactar en la menor medida a su productividad.

Resultados reportados

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

Las ventajas que se podrían obtener de la gestión de la arquitectura empresarial de los diferentes tipos de las organizaciones que han gestionado de forma continua. Dispuesto a esto, por la parte de las organizaciones colombianas cuya investigación de aplicación para la arquitectura empresarial, siendo esa TOGAF, se ha traducido en que se ha logrado un proceso seguro de manejo documental digital en plataformas de SaaS. La cifra que ha expuesto ibid. es que se han podido reducir hasta en un 40% las incidencias provocadas entre el no acceso permitido y los riesgos de pérdida de información. La cifra que han presentado representa que se ha llegado a disminuir un 40% incidencias originadas por el no acceso permitido y por pérdida e información.

En Paraguay, la investigación de Luján Rodas et al. (2023) informa que las PYMES que capacitaron a su personal en competencias digitales permiten una mejora en la detección de ataques y una disminución de los errores humanos del 25%, lo cual reduce eficazmente la brecha de seguridad.

En Ecuador y dado que las auditorías cibernéticas son poco llevadas a la práctica, las empresas que sí la aplicaron indican que tienen una mejora en la velocidad de respuesta para la resolución de los incidentes, e igualmente consideran que sus clientes tienen mejor percepción de la seguridad (López-Anchala & Ordóñez-Parra, 2024). Este efecto reputacional también es mencionado por entidades internacionales, como es el caso de la ENISA y la OEA, para las cuales la visibilidad y la trazabilidad de todas las acciones de Ciberseguridad nos ayudan a generar confianza con los socios comerciales.

Indicadores de éxito

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

Entre los principales indicadores utilizados para evaluar la efectividad de las buenas prácticas se encuentran:

- Reducción de incidentes de seguridad reportados (ataques bloqueados, intentos de phishing detectados, infecciones de malware).
- Tiempo de respuesta ante incidentes, especialmente en eventos críticos como caídas de sistema o ransomware.
- Disponibilidad de sistemas clave, medida en términos de continuidad operativa.
- Nivel de cumplimiento normativo en relación con estándares locales e internacionales (por ejemplo, ISO 27001, GDPR).
- Percepción de confianza por parte de los clientes, evaluada mediante encuestas internas o métricas de satisfacción.

Del mismo modo y apoyado en estudios como el que ha llevado a cabo Díaz Chantre (2023), se revela que las organizaciones que han estructurado un modelo de gestión del sistema de la seguridad de la información (SGSI) disminuyen su nivel de documentación y seguimiento, así como el de mejora continua lo que favorece, a su vez, la resiliencia institucional.

Por norma general, la combinación de una serie de prácticas básicas acompañadas de un modelo organizacional, pero con una aptitud normativa flexible, es la combinación que ha demostrado ser más efectiva para garantizar resultados sostenibles en materia de ciberseguridad; la clave no está solo en el ámbito técnico, sino en el modo de apoderarse de la cultura, de la operativa de la seguridad como parte del ADN de las organizaciones.

Factores Clave para la Implementación Exitosa

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

Las buenas prácticas en ciberseguridad de las PYMES no son sólo el hecho de contar con herramientas de ciberseguridad o marcos normativos, sino que vienen por una serie de factores que determinan el éxito del buen funcionamiento de las estrategias de ciberseguridad de las pequeñas y medianas empresas. En la revisión documental llevada a cabo se han obtenido cuatro factores que determinan que el éxito del funcionamiento de dichas estrategias son el compromiso de la alta dirección, la disponibilidad de recursos adaptados, la colaboración institucional y la cultura estructural de las organizaciones.

Compromiso de la alta dirección

Uno de los componentes más restrictivos para la adopción de la ciberseguridad efectiva en las PYMES, es el propio compromiso genuino de la dirección de la empresa. Las organizaciones que entienden la seguridad de la información como un componente de la maquinaria estratégica y no como un elemento puramente técnico se desempeñan mejor y obtienen una mejor puntuación en cuanto a la gestión de los riesgos derivados del proceso de digitalización. Paralelamente a ello, y por este motivo, esta clase de liderazgo se concreta de manera formal y explícita en la implementación de presupuestos específicos, en la identificación de políticas de seguridad de la información en el propio plan estratégico de la organización y, por último, también en la propia promoción de una cultura de la prevención (Díaz Chantre, 2023).

Los datos evidencian que cuando la alta dirección asigna importancia a la ciberseguridad, la adopción de marcos como ISO/IEC 27001, NIST o arquitecturas empresariales que se basen en TOGAF es considerablemente más asequible. En Archivos y Sistemas S.A.S en Colombia, por ejemplo, esto fue precisamente el sustento de la alta

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

dirección lo que permitió diseñar y poner en marcha una arquitectura de seguridad robusta en su plataforma de gestión documental SIGED, lo que a su vez fortaleció la postura de seguridad a través de unos procesos organizativos bien definidos (Bolaño Rocha & Amaya Corredor, 2023).

Recursos y soluciones adaptadas a la escala de la empresa

Las PYMEs tienen afrontando limitaciones muy notorias en cuanto a sus recursos financieros, infraestructura tecnológica o personal calificado. Por tanto, la disponibilidad de herramientas y soluciones acordes a su tamaño es fundamental. Las buenas prácticas de mayor éxito son aquellas que no requieren inversiones excesivas ni personal muy especializado para su aplicación.

La experiencia internacional nos dice que muchas empresas han llevado a cabo una correcta seguridad con soluciones de baja complejidad pero bien instaladas: antivirus con administración centralizada, firewalls, backups en la nube y plataformas de formación asequibles. Un programa como el de Cyber Essentials en Singapur representa un buen ejemplo de cómo la puesta a disposición de guías prácticas y de certificaciones mínimas puede facilitar la adopción de medidas de seguridad, incluso entre las empresas con escasa infraestructura tecnológica (CSA, 2022).

De la misma forma, las guías de ENISA para PYMES europeas (2021) confirman que el acceso a manuales, guías con pasos a seguir y la posibilidad de acceder a plantillas de políticas de seguridad tengo cabida a la diferencia. La cuestión radica en la sencillez, la claridad y la contextualización de los recursos existentes.

Colaboración con entidades especializadas

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

Otro elemento determinante lo constituye la capacidad de establecer sinergias con aquellas entidades expertas en ciberseguridad que estén a la vez en el ámbito público y privado; lo cual no sólo permite cubrir el déficit de personal de la organización, sino que también se puede llegar a adoptar diagnóstico y modelos probados sin la necesidad de implementar capacidades desde cero.

La OEA promueve dicho tipo de cooperación en América Latina mediante los programas de fortalecimiento institucional, auditorías externas y sinergias con universidades e institutos técnicos (OEA, 2020). En Ecuador, López-Anchala y Ordóñez-Parra (2024) llevan a la luz el poder provenido de las auditorías regulares, de los planes de recuperación ante incidentes y de los sistemas de monitorización de amenazas alcanzado por las empresas que, por otra parte, han recibido apoyo externo, siendo el poder conseguido superior al medio alcanzado.

Por otro lado, en naciones como Paraguay, las universidades han desempeñado una labor relevante en el desarrollo del talento humano y la asistencia técnica a empresas en formación (Luján Rodas et al., 2023), lo que pone de manifiesto la necesidad de crear ecosistemas colaborativos entre el sector académico, estatal y privado.

Cultura organizacional y formación continúa

Por último, la sostenibilidad de cualquier estrategia de ciberseguridad en las PYMES depende de la inclusión de la seguridad digital como uno de los aspectos propios de la cultura organizacional. Para ello es necesario que la totalidad de la plantilla de la organización (no sólo el personal técnico) conozca los riesgos y habitualice a patrones seguros en su tarea diaria.

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

La formación continúa del personal, la práctica de simulacros, las campañas internas de concienciación, la existencia de canales claros de reporte de incidentes,… constituyen algún componente básico para el buen desarrollo de esa cultura. Los hallazgos que recogen López-Anchala & Ordóñez-Parra (2024) muestran que aquellas organizaciones que invierten en formación continuada consiguen reducir sustancialmente la tasa de incidentes por fallos humanos.

Igualmente, acoger modelos de gobernanza en los que todo el mundo tenga bien definida su existencia y el alcance para el que existe facilita la implementación de controles y evita ambigüedades que pudieran derivar en incidentes operativos.

Discusión

La literatura revisada pone de manifiesto que a pesar de las diferencias económicas, culturales y tecnológicas bastante pronunciadas, se percibe una clara convergencia en la necesidad de que las pequeñas y medianas empresas (PYMES) implanten buenas prácticas de la ciberseguridad. La discusión en este sentido de las experiencias ha de tener en cuenta la transferibilidad de las prácticas pero también los obstáculos estructurales que pueden dificultar su despliegue pero también las oportunidades que puedan surgir para que surjan ecosistemas más seguros y resilientes.

Transferibilidad de buenas prácticas

Uno de los hallazgos de mayor valor para la identificación de buenas prácticas es que muchas de las buenas prácticas identificadas —por ejemplo, la autenticación multifactorial, la formación continua del personal, la existencia de copias de seguridad y la monitorización de las amenazas— son altamente replicables, adaptándolas, sí, pero a las capacidades y al

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

contexto de cada organización. En este sentido, se entiende que la ciberseguridad no es un conjunto de soluciones a aplicar universales, sino una forma de aplicar soluciones a partir de la consideración de otros factores como la madurez digital, el nivel educativo del personal, la capacidad económica de la organización o el marco legislativo en el que opera cada organización.

Por poner un ejemplo, en Europa la ENISA impulsó marcos estructurados y guías prácticas de alta repercusión para las PYMES gracias a ser simples, accesibles y en normativa (ENISA, 2021); en cambio las prácticas, a diferencia de la amplitud de la infraestructura y de la formación en América Latina exigen ajustes contextuales y apoyo institucional para ser efectivas. Así es el caso del Ecuador que, dado el escaso porcentaje de empresas que llevan ciber seguimiento, confirma la carencia de cultura de prevención, pero la necesidad también de estar orientado técnicamente y de tener que financiarse ofreciendo fondos desde el exterior (López-Anchala & Ordóñez-Parra, 2024).

De igual manera, Colombia y Paraguay han llegado a observar experiencias relativas a la implementación de marcos de trabajo como puede ser TOGAF o la inversión en mejorar las capacidades de las personas, lo que ha llevado a la obtención de importantes avances en la seguridad de la organización (Bolaño Rocha & Amaya Corredor, 2023; Luján Rodas et al., 2023). Lo que les ha mostrado es que, justamente, la transferencia de buenas prácticas implica mucho más que la mera operación del procedimiento a replicar, sino que se requiere también la construcción de capacidades adecuadas para asegurar su sostenibilidad.

Limitaciones estructurales

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

No obstante el reconocimiento de las adecuadas prácticas, la gran mayoría de las PYMES están en condiciones de atravesar barreras estructurales que dificulten su implementación. Entre estas, destaca la falta de presupuesto, la escasez de personal técnico, el desconocimiento de marcos normativos, reconocer los riesgos cibernéticos como un proceso de toma de riesgo y la falta de 'latencia' en los incentivos del gobierno. En muchos casos, las empresas dan mayor importancia a las necesidades operativas urgentes por encima de las inversiones preventivas, lo que entonces incrementa su vulnerabilidad.

En Latinoamérica, los estudios revisados indican que un 80% de las empresas del sector comercial no realizan auditorías periódicas de seguridad, lo que muestra este gap tan crítico entre la percepción del riesgo y la acción preventiva (López-Anchala & Ordóñez-Parra, 2024). Esta situación refleja también la falta de políticas públicas específicas y esquemas de financiamiento que den la posibilidad a las empresas de invertir en ciberseguridad.

A lo anterior se añade la dificultad de que no existen métricas estándar que permitan a las PYMES verificar su mejora en la cuestión de la medida de la seguridad. A diferencia de las grandes empresas, que disponen de unidades de trabajo y instrumentos de medida complejos, las pequeñas empresas no poseen métricas a las cuales recurrir que les permitan conocer su propio nivel de exposición o la eficacia de las medidas puestas en marcha.

Oportunidades de mejora y colaboración

No obstante, la creciente disponibilidad de recursos gratuitos, marcos simplificados, programas de certificación puede presentar también una nueva oportunidad para las PYMES. Ejemplos como Cyber Essentials en Singapur, las guías de ENISA o los programas dentro de

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

las iniciativas de cooperación de la OEA muestran cómo gobiernos y/o las organizaciones internacionales pueden facilitar el acceso a conocimientos prácticos y fomentar la adopción de estándares mínimos.

También el fortalecimiento de las redes colaborativas entre las empresas, las universidades y las administraciones puede hacer frente a gran parte de las limitaciones individuales que pueden tener unos, las empresas, que a menudo no obtendrán el respaldo suficiente de unas administraciones que, además, no han puesto el foco en las empresas, sino en otras instituciones que no son empresas. En Paraguay, por ejemplo, la vinculación establecida entre las PYMES y el sector académico para poder dotar a las empresas de capacidad técnica, ha dado resultados eficaces de empresas con poca capacidad técnica y con unos costes ajenos muy altos. (Luján Rodas et al., 2023).

En el ámbito de la política pública se pueden llegar a considerar propuestas enfocadas a integrar con las PYMES las estrategias nacionales de ciberseguridad, que pueden incluir incentivos tributarios a la contratación, formación gratuita, asesoramiento técnico especializado, y campañas de concientización para gerentes y el personal operativo de las organizaciones, de forma que la ciberseguridad no sea una preocupación aislada sino que pase a formar parte del sistema de gestión global de la organización.

Conclusiones

La revisión bibliográfica realizada ha permitido identificar, comparar y analizar una serie de buenas prácticas en ciberseguridad que se han desarrollado a nivel de PYMEs en diferentes contextos internacionales y, a partir del análisis de casos de PYMEs en América Latina y Europa y Asia, y de experiencias sectoriales, se ha podido elaborar un mapa de

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

prácticas de buenas estrategias que podrían ser adecuadamente adaptadas y que, en virtud de su adecuación, podrían ayudar a mejorar la postura de ciberseguridad en este tipo de organizaciones.

Conclusión general

El hallazgo primordial del informe es que las PYMES, a pesar de sus limitaciones estructurales, pueden llegar a un nivel de protección cibernética adecuado mediante la implementación de unas prácticas básicas, pero bien ejecutadas: las de gestión de contraseñas, la formación del personal, la actualización periódica del software, la realización de backup y auditorías. Son unas medidas sencillas, pero son muy eficaces si son implementadas dentro una estrategia organizacional coherente, con liderazgo gerencial y continuación en el tiempo.

Las prácticas que han sido recopiladas en el informe correspondiente a la ENISA (2021) y en el programa de Cyber Essentials correspondiente a Singapur (CSA, 2022) así como en diversos trabajos académicos revisados (Díaz Chantre, 2023; López-Anchala & Ordóñez-Parra, 2024; Luján Rodas et al., 2023) muestran que tener grandes inversiones económicas no es estrictamente necesario para mejorar la ciberseguridad, pero teniendo una clara visión, herramientas accesibles y un adecuado acompañamiento técnico.

Síntesis de hallazgos clave

1. Las prácticas más efectivas son transferibles, pero requieren adaptación. Medidas como la autenticación multifactorial, la segmentación de redes, la gestión de accesos o los planes de respuesta ante incidentes son útiles en diversos contextos, siempre que se ajusten a la realidad operativa, financiera y cultural de la empresa.

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

2. El compromiso de la alta dirección es indispensable. Las empresas que lograron avances significativos en su postura de seguridad digital tienen en común la participación activa de sus directivos, quienes lideraron procesos de cambio, asignaron recursos y promovieron una cultura de prevención.
3. La capacitación continua del personal es una inversión clave. La concienciación y formación de los colaboradores permite reducir errores humanos, mejorar la capacidad de respuesta ante incidentes y fortalecer el cumplimiento de políticas internas de seguridad.
4. La colaboración institucional y el apoyo técnico externo marcan la diferencia. Las PYMES que establecen vínculos con entidades gubernamentales, universidades o asociaciones gremiales acceden a conocimiento especializado, programas de formación y mecanismos de certificación que facilitan la implementación de estándares.
5. La falta de auditorías y métricas es una debilidad crítica. Muchos de los estudios revisados evidencian que las PYMES no cuentan con sistemas de monitoreo ni indicadores que les permitan evaluar su nivel de madurez en ciberseguridad, lo cual limita la toma de decisiones y la mejora continua.

Recomendaciones para las PYMES

A partir de lo anterior planteamos recomendaciones de interés para empresas de pequeña y mediana dimensión que deseasen mejorar su postura en ciberseguridad:

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

- Centrar su modelo en fases, iniciando por controles básicos y avanzando hacia gestiones más completas de gestión de la seguridad de la información (como ISO/IEC 27001 o NIST).
- Designar personas responsables de la ciberseguridad, incluso no siendo especialistas en ciberseguridad, pero las cuales pudiesen promover la coordinación de acciones a través de asesorías con especialistas de forma externa.
- Valerse de recursos gratuitos y marcos simplificados (como guías de ENISA o Cyber Essentials) para estructurar su práctica de una forma ordenada y comprensible.
- Crear sinergias estratégicas con universidades, asociaciones, administraciones públicas, proveedores tecnológicos que proporcionasen formación y soporte.
- Entrar en la ciberseguridad como parte de su modelo de negocios, no como un coste sino como un modelo que les permita generar confianza y competitividad.

Propuestas para Políticas Públicas

- Los organismos internacionales y los gobiernos además tienen un papel importante. En este sentido, se propone que:
- Se desarrollen programas nacionales de ciberseguridad para PYMEs, introduciendo financiamiento, formación y apoyo técnico,
- Se dispongan de marcos regulatorios flexibles que reconozcan las especificidades de las pequeñas empresas, sin poner en riesgo estándares mínimos de protección,

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

- Se promueva la certificación por niveles, de modo que las PYMEs puedan avanzar por etapas en su madurez cibernética, sin que hayan barreras técnicas o económicas insalvables.

Cierre

El resumen de lo anterior es que la ciberseguridad no debe ser analizada o considerada como un privilegio exclusivo de las grandes corporaciones, dado que las PYMES, a través de los enfoques correctos y el debido apoyo, pueden llegar a ser consideradas incluso como organizaciones resilientes y de confianza en la economía digital. La clave se encuentra en la democratización del conocimiento, en la facilitación del acceso a recursos ajustados, junto con la promoción de una cultura empresarial a la que le otorguemos valor a la seguridad de la información como un activo estratégico.

Referencias bibliográficas

Agencia de la Unión Europea para la Ciberseguridad (2021). Cybersecurity for SMEs: Challenges and Recommendations. https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

Agencia de Seguridad Cibernética de Singapur (2022). Cyber Essentials. https://www.csa.gov.sg/Programmes/cyber-essentials

Banco Mundial. (2021). Pequeñas y medianas empresas (PYMES) financieras. https://www.worldbank.org/es/topic/smefinance

Bolaño Rocha, E. F., & Amaya Corredor, Y. A. (2023). Arquitectura empresarial para PYMES: Caso SIGED [Tesis de maestría, Universidad Cooperativa de Colombia]. https://repository.ucc.edu.co/handle/20.500.12494/57780

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

Bueno, G. (2019). Ciberseguridad en Colombia: Avances y retos. (Disponible en Cuarta Compilación)

Díaz Chantre, R. A. (2023). Análisis de los estándares y buenas prácticas de ciberseguridad utilizados por la industria colombiana [Tesis de maestría, UNAD]. https://repository.unad.edu.co/handle/10596/60407

González & Ramírez. (2020). Herramientas de ciberseguridad para detectar vulnerabilidades en microempresas. (Disponible en Cuarta Compilación)

ISO/IEC. (2012). ISO/IEC 27032: Directrices para la Ciberseguridad. https://www.iso.org/standard/44375.html

ISO/IEC. (2013). ISO/IEC 27001: Sistemas de Gestión de Seguridad de la Información – Requisitos. https://www.iso.org/standard/54534.html

López-Anchala, K. A., & Ordóñez-Parra, Y. L. (2024). Auditoría y ciberseguridad en el sector comercial: Diagnóstico en PYMES de Ambato. Revista Multidisciplinaria Perspectivas Investigativas, 5(1), 42–55. https://doi.org/10.61384/27985903.498

Luján Rodas, L. R., et al. (2023). Transformación digital de las PYMES en Paraguay: Retos y oportunidades. Ciencia Latina Revista Científica Multidisciplinar, 7(5), 8294–8303. https://doi.org/10.37811/cl_rcm.v7i5.8411

Maggi Murillo, G., & Gómez Gómez, O. S. (2021). Estudio sobre conocimiento de ciberseguridad en usuarios de PYMES. Perspectivas, 3(2), 45–53. https://doi.org/10.47187/perspectivas.vol3iss2.pp45-53.2021

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

Martínez, J. A., & Blanco, L. X. (2020). Recomendaciones de buenas prácticas de ciberseguridad en PYMES. Universidad Autónoma de Bucaramanga. https://repository.unab.edu.co/handle/20.500.12749/13911

National Cyber Security Alliance. (2018). Cybersecurity Awareness Toolkit for SMBs. https://staysafeonline.org/wp-content/uploads/2018/09/SMB-Toolkit-FINAL.pdf

Navarro Uriol, C. (2020). Estrategias de ciberseguridad: el caso de la pequeña y mediana empresa [Trabajo de grado, Universidad de Zaragoza]. https://zaguan.unizar.es/record/101988/files/TAZ-TFG2020-1242.pdf

Orellana, F. D. (2020). Cybersecurity incident response capabilities in the Ecuadorian small business sector [Tesis doctoral, Northcentral University]. https://www.proquest.com/docview/2466034020

Organización de los Estados Americanos (OEA). (2020). Informe de Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe. https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

Palafox-Pascual, L. (2019). NUTRIA: Una metodología de ciberseguridad para PYMES en entornos industriales [Tesis de maestría, UNIR]. https://reunir.unir.net/handle/123456789/9422

Peralta Zuñiga, M. L., & Aguilar Valarezo, D. N. (2021). La ciberseguridad y su concepción en las PYMES de Cuenca, Ecuador. Contabilidad y Auditoría, 53, 99–126. https://ojs.econ.uba.ar/index.php/Contyaudit/article/view/2061

ISSN L: 2992-6629
Vol. 2, No. 2, julio – diciembre 2025
pp. 8 - 41
https://revistas.up.ac.pa/index.php/vanguardiajuridica

Pineño, G. (2019). Ciberseguridad para PYMES. Universidad de Sevilla. (Disponible en Cuarta Compilación)

UIT. (2008). UIT-T X.1205 Serie X: Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad. https://www.itu.int/rec/T-REC-X.1205-200804-I

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004