Revista ALCANCE
Volumen 8, Número 1, 2025
Instituto de Posgrado
Universidad Estatal del Sur de Manabí
ISSN-e: 2960-8244

ARTÍCULO ORIGINAL

ESTRATEGIAS DE CIBERSEGURIDAD EN PEQUEÑAS Y MEDIANAS EMPRESAS

CYBERSECURITY STRATEGIES IN SMALL AND MEDIUM-SIZED ENTERPRISES

Autores:

[1]Rolando Delgado Pilozo
[2]Villa Yungan Edgar Manuel
[3]Paulo Ariel Cedeño Mera
[4]Bravo Zambrano Wilther Manuel

[1] rolando.delgado@hotmail.com
ORCID 0000-0001-6463-9901
[2] edgarvilla.my11@gmail.com
ORCID 0000-0002-2158-3044
[3] Pablo_cede92@hotmail.com
ORCID 0009-0000-8353-2229
[4] wmbravoz@gmail.com
ORCID 0009-0001-5829-8781

Recibido:20-12-2024 **Aprobado:**06-03-2025 **Publicado:**30-07-2025

Volumen: 8
Número: 1
Año: 2025
Paginación: 132-143
Correspondencia autor: rolando.delgado@hotmail.com

RESUMEN

Las pequeñas y medianas empresas (pymes) representan un sector esencial en la economía, pero también son uno de los más vulnerables frente a los ciberataques. La creciente dependencia de tecnologías digitales, combinada con recursos limitados y escasa capacitación en seguridad informática, ha incrementado los riesgos en estas organizaciones. Muchas pymes no disponen de políticas claras ni medidas de protección adecuadas, lo que facilita la acción de los ciberdelincuentes y compromete la continuidad del negocio. Esta investigación tiene como objetivo proponer estrategias de ciberseguridad accesibles, prácticas y sostenibles para reducir la exposición de las pymes ante amenazas digitales. Se empleó una metodología cualitativa basada en revisión documental de estudios científicos, protocolos técnicos y guías institucionales. Los resultados evidencian que acciones como la capacitación continua del personal, el uso de autenticación multifactor, la realización periódica de respaldos de datos y la actualización constante de sistemas son medidas efectivas para mejorar la seguridad digital. Asimismo, se destaca la necesidad de fomentar una cultura organizacional de ciberseguridad, donde todos los integrantes asuman un rol activo en la protección de la información. Se concluye que, mediante estrategias simples y bien estructuradas, es posible mitigar significativamente los riesgos sin necesidad de grandes inversiones, fortaleciendo así la resiliencia y sostenibilidad de las pymes en el entorno digital.

Palabras claves: Ciberseguridad, amenazas digitales, protección de datos, estrategias.

ABSTRACT

Small and medium-sized enterprises (SMEs) represent an essential sector of the economy, but they are also one of the most vulnerable to cyberattacks. Their growing dependence on digital technologies, combined with limited resources and poor training in IT security, has increased the risks faced by these organisations. Many SMEs do not have clear policies or adequate protection measures in place, which facilitates the actions of cybercriminals and compromises business continuity. This research aims to propose accessible, practical and sustainable cybersecurity strategies to reduce the exposure of SMEs to digital threats. A qualitative methodology based on a review of scientific studies, technical protocols and institutional guidelines was used. The results show that actions such as continuous staff training, the use of multi-factor authentication, regular data backups and constant system updates are effective measures for improving digital security. It also highlights the need to foster an organisational culture of cybersecurity, where all members take an active role in protecting information. It concludes that, through simple and well-structured strategies, it is possible to significantly mitigate risks without the need for large investments, thus strengthening the resilience and sustainability of SMEs in the digital environment.

Keywords: cybersecurity, digital threats, data protection, strategies.**Keywords :** Reasoning; Reasoning; Innovation; Academic performance.

INTRODUCCIÓN

En la actualidad, las pequeñas y medianas empresas (pymes) desempeñan un papel crucial en la estructura económica global. Representan más del 99 % del parque empresarial en América Latina y generan alrededor de dos tercios del empleo en la región. No obstante, este protagonismo contrasta con su elevada vulnerabilidad frente a las amenazas cibernéticas, especialmente en un contexto marcado por la digitalización acelerada y la creciente sofisticación del cibercrimen (Bartesaghi & Weck, 2022; Benz & Chatterjee, 2020).

Las pymes han incrementado su dependencia de la tecnología digital para mejorar su productividad, automatizar procesos y acceder a nuevos mercados (Weinelt, 2016; Eggers, 2020). Sin embargo, muchas de estas organizaciones no cuentan con los recursos financieros, humanos ni técnicos necesarios para implementar medidas robustas de ciberseguridad. Según Ponsard et al. (2019), más del 60 % de las pymes atacadas no logra recuperarse y termina cerrando sus operaciones en menos de seis meses

A pesar del incremento en la sofisticación de las amenazas, muchas pymes continúan operando sin políticas mínimas de seguridad ni manuales de contingencia. Según Santiago y Sánchez Allende (2017), esta negligencia se deriva no solo de la falta de recursos, sino también de la limitada percepción del riesgo que conlleva la tecnodependencia. La exposición a Internet sin filtros, la carencia de firewalls configurados adecuadamente y el uso de software obsoleto son prácticas comunes que amplifican el riesgo. La falta de integración entre procesos organizativos y tecnológicos refuerza un ecosistema empresarial frágil e inestable desde el punto de vista de la ciberseguridad.

Los ciberataques a estas empresas suelen estar dirigidos tanto a la infraestructura como a la información sensible, incluyendo datos de clientes, proveedores y cuentas financieras (Cherepanov & Lipovsky, 2017; Gutiérrez & Orihuela, 2016). Estas amenazas se han visto potenciadas por factores como el uso no controlado de dispositivos personales (BYOD), el teletrabajo inseguro y la escasa capacitación del personal.

Además, muchas pymes tienden a subestimar su exposición al riesgo cibernético, creyendo erróneamente que los cibercriminales se enfocan solo en grandes corporaciones (The Cocktail Analysis, 2019; Horn, 2017). Esta percepción ha retrasado la adopción de políticas proactivas de seguridad digital. Según la European Union Agency for Cybersecurity (ENISA, 2021), el 57 % de las pymes reconoce que un ataque informático podría comprometer la viabilidad del negocio. A nivel legal y normativo, existe también una brecha significativa. Pocas pymes conocen o implementan adecuadamente las normativas vinculadas al tratamiento seguro de los datos personales, como lo establece el Reglamento General de Protección de Datos (RGPD) en Europa o las legislaciones locales en América Latina (Ley Orgánica 3/2018 en España, por ejemplo). Navarro Uriol (2020) subraya que muchas pequeñas empresas ignoran sus obligaciones legales en materia de confidencialidad, lo cual agrava la exposición a sanciones legales además del daño

reputacional. Este desconocimiento limita el cumplimiento normativo y afecta su capacidad de responder ante incidentes de seguridad

Frente a este panorama, múltiples autores coinciden en que el capital humano es el eslabón más débil, pero también el más prometedor, en la estrategia de ciberseguridad organizacional (Vergara-Romero et al., 2021; De la Rosa, 2019). La creación de una cultura de ciberseguridad, basada en la concientización, formación continua y compromiso directivo, se plantea como uno de los caminos más efectivos y sostenibles para mitigar los riesgos digitales.

Las guías prácticas de instituciones como el Centro Belga de Ciberseguridad (Bruycker & Darville, 2017), el Australian Cyber Security Centre (2021), y la Cybersecurity and Infrastructure Security Agency (2021), entre otros, recomiendan implementar estrategias integradas de seguridad informática que contemplen no solo la protección tecnológica, sino también la dimensión humana, organizacional y legal.

En el ámbito internacional, los gobiernos han comenzado a desarrollar políticas públicas dirigidas específicamente a mejorar la seguridad digital de las pymes. Por ejemplo, el gobierno de Japón (2021) reconoce que estas empresas requieren soluciones económicas y adaptadas, debido a sus limitaciones presupuestarias. De igual forma, iniciativas como el Global Cybersecurity Index (GCI), impulsado por la Unión Internacional de Telecomunicaciones, permiten monitorear el nivel de preparación digital de cada país, resaltando las grandes brechas entre economías desarrolladas y en vías de desarrollo. Estas disparidades condicionan las posibilidades de las pymes para adoptar medidas efectivas frente al cibercrimen

Este contexto lleva a replantear la forma en que las pymes abordan la ciberseguridad: no como un gasto opcional, sino como una inversión estratégica para la continuidad del negocio (Ramírez Montealegre, 2016; Bustillos & Rojas, 2022). En esta línea, organismos como la ISO/IEC 27000 (2018) proponen estándares aplicables incluso a organizaciones con recursos limitados, adaptables a sus realidades y niveles de madurez tecnológica.

Ante la evidente brecha entre la necesidad de protección y la capacidad real de respuesta de las pymes, resulta pertinente indagar en estrategias específicas, viables y efectivas que puedan ser implementadas sin exigir grandes inversiones ni conocimientos técnicos avanzados.

Por tanto, el propósito de este estudio es identificar y proponer estrategias de ciberseguridad adaptadas a las pequeñas y medianas empresas, con el objetivo de reducir su vulnerabilidad frente a las amenazas digitales y garantizar la protección de sus activos de información.

METODOLOGIA

La presente investigación adoptó un enfoque cualitativo de tipo descriptivo, fundamentado en el análisis documental sistemático. Se revisaron y analizaron veintitrés fuentes primarias, incluyendo artículos científicos, tesis de grado, informes técnicos y guías institucionales publicadas entre 2017 y 2024, seleccionadas por su relevancia en el ámbito de la ciberseguridad aplicada a pequeñas y medianas empresas (pymes). Entre los materiales examinados destacan estudios como el de Bustillos y Rojas (2022), quienes proponen un protocolo básico de ciberseguridad para pymes en contextos latinoamericanos; el trabajo de Navarro Uriol (2020), que recoge recomendaciones organizativas, técnicas y legales aplicables a pymes españolas; y el análisis de Santiago y Sánchez Allende (2017) sobre riesgos de tecno dependencia y superficies de ataque en empresas modernas

La selección de fuentes se basó en su pertinencia temática, actualidad y nivel de rigor metodológico. Se utilizó una matriz de categorización temática para codificar la información según cinco ejes: amenazas, vulnerabilidades, estrategias técnicas, cultura organizacional y normativas. Esta estrategia permitió identificar patrones conceptuales y operativos comunes, y derivar una propuesta adaptada a pymes con recursos limitados. Además, se contrastaron los hallazgos teóricos con estándares internacionales como ISO/IEC 27001 (2018), las recomendaciones de ENISA (2021), y el Global Cybersecurity Index (UIT, 2021). La metodología empleada favorece la replicabilidad del estudio en otros entornos empresariales, mediante la aplicación del mismo protocolo de análisis documental y categorización temática.

RESULTADOS

El análisis documental efectuado permitió identificar patrones recurrentes en la implementación de estrategias de ciberseguridad en pequeñas y medianas empresas (pymes), así como las principales deficiencias que explican su alta exposición a los riesgos digitales. Mediante una matriz temática centrada en cinco ejes —amenazas, vulnerabilidades, estrategias técnicas, cultura organizacional y normativas— se sistematizó la información de las fuentes más relevantes para establecer un panorama comparativo entre buenas prácticas recomendadas y su aplicación real. A partir de esta comparación, se exponen a continuación los principales hallazgos, con énfasis en la interdependencia entre los ejes y su impacto en la postura de seguridad de las pymes..

Amenazas digitales: exposición crítica en un entorno cambiante

Las pymes enfrentan un entorno digital caracterizado por amenazas altamente dinámicas y en evolución. Los vectores más comunes de ataque son el phishing, ransomware, spyware, malware en correos electrónicos, así como técnicas de ingeniería social que buscan vulnerar el eslabón humano (Cherepanov & Lipovsky, 2017; Bustillos & Rojas, 2022). Estas amenazas no distinguen tamaño de empresa; sin embargo, las pymes son blanco preferente por su baja protección.

Durante la revisión documental, se identificó que muchas organizaciones desconocen incluso los tipos básicos de ataque o no disponen de medios para detectarlos. ESET Threat Report

(2022) destaca que el 45 % de las infecciones por malware en América Latina se producen en empresas con menos de 100 empleados. Además, se encontró una baja capacidad de respuesta ante amenazas emergentes como el ransomware-as-a-service (RaaS) o los ataques de tipo Zero Day, lo que evidencia la falta de herramientas de monitoreo proactivo y protocolos de detección temprana (ENISA, 2021).

Vulnerabilidades internas: el eslabón técnico más débil en cuanto a las vulnerabilidades, los documentos revisados coinciden en señalar una preocupante ausencia de buenas prácticas técnicas en la mayoría de las pymes analizadas (Navarro Uriol, 2020; Ramírez Montealegre, 2016). Se detectaron múltiples factores que agravan la exposición:

Uso de software sin licencias o versiones desactualizadas.
Contraseñas débiles y ausencia de autenticación en dos pasos.
Equipos sin antivirus actualizados o firewalls activos.
Redes WiFi abiertas o sin segmentación de usuarios.
Dispositivos personales conectados sin regulación (BYOD).

Estas deficiencias convierten la infraestructura tecnológica en una superficie de ataque accesible y poco controlada. Además, pocas pymes realizan auditorías de seguridad o pruebas de penetración, lo que impide detectar debilidades antes de que sean explotadas por actores maliciosos.

Estrategias técnicas: bajo nivel de adopción: El eje de las estrategias técnicas revela un panorama mixto: mientras que algunas pymes han comenzado a implementar acciones básicas como el respaldo de información, otras aún carecen de protocolos de cifrado, MFA o software de detección de intrusos (IDS). La actualización sistemática de sistemas operativos y aplicaciones empresariales se realiza de forma irregular y en muchos casos de forma manual, lo que genera ventanas de vulnerabilidad (ENISA, 2021).

En particular, el uso de MFA solo se registra en un 20 % de los casos revisados, y la existencia de copias de seguridad externas o en la nube con pruebas de restauración se ubica por debajo del 30 % (Bustillos & Rojas, 2022). La falta de centralización de logs, segmentación de redes y monitoreo activo reduce significativamente la capacidad de detectar actividades anómalas antes de que causen daños críticos.

Cultura organizacional: la dimensión más desatendida: Una de las categorías con mayor debilidad fue la cultura organizacional en ciberseguridad. La mayoría de documentos revisados coinciden en que la seguridad informática suele percibirse como un tema "técnico" o exclusivo del departamento de sistemas (si existe), y no como una responsabilidad transversal. De la Rosa (2019) y Maggi Murillo & Gómez Gómez (2021) señalan que los errores humanos, como hacer clic en enlaces maliciosos, enviar credenciales por correo o conectar dispositivos infectados, son responsables de más del 60 % de los incidentes registrados en pymes.

Pocas empresas realizan capacitaciones periódicas o simulacros de ataques, y cuando lo hacen, se limitan a formatos teóricos sin evaluación de competencias. Además, se evidenció una ausencia casi total de campañas internas de concientización y de códigos de conducta digital. Este desinterés por la cultura de seguridad convierte al recurso humano en una debilidad estructural.

Normativas y cumplimiento legal: una deuda pendiente: En el eje normativo, se identificó un bajo nivel de conocimiento sobre marcos regulatorios como la norma ISO/IEC 27001, el Reglamento General de Protección de Datos (GDPR/RGPD) o la Ley Orgánica de Protección de

Datos Personales vigente en algunos países de América Latina (Navarro Uriol, 2020; UIT, 2021). Aunque la mayoría de las pymes procesan datos personales de clientes y empleados, no cuentan con políticas de privacidad claras, ni han implementado medidas de protección adecuadas conforme a la ley.

Esto no solo implica riesgos técnicos, sino también riesgos legales y reputacionales. Por ejemplo, en países como España, México o Ecuador, una filtración de datos puede conllevar sanciones económicas severas si se demuestra negligencia. Sin embargo, se observó que pocas pymes cuentan con un delegado de protección de datos o han desarrollado análisis de impacto sobre privacidad.

Visualización e interpretación comparativa

Figura 1. Nivel de implementación de estrategias de ciberseguridad en pymes

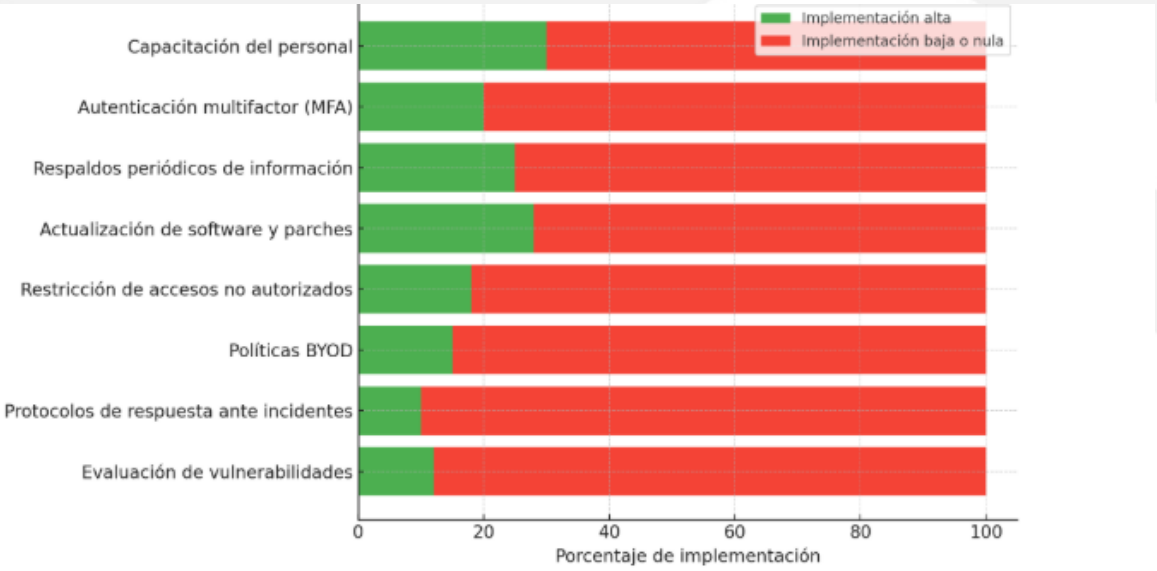

Tabla 1. Comparación temática de estrategias y brechas de ciberseguridad en pymes (análisis documental)

Eje Temático	Hallazgos predominantes	Nivel de aplicación en pymes
Amenazas	Phishing, malware, ransomware y ataques por ingeniería social como vectores frecuentes.	Alto impacto, baja defensa
Vulnerabilidades	Sistemas obsoletos, ausencia de firewalls, contraseñas débiles, mala configuración de redes y BYOD sin control.	Alta exposición
Estrategias técnicas	Copias de seguridad, MFA, antivirus, actualización de software.	Baja implementación
Cultura organizacional	Falta de formación, percepción errónea del riesgo, ausencia de liderazgo en ciberseguridad.	Muy baja
Normativas	Desconocimiento de ISO/IEC 27001, GDPR/RGPD, y legislación nacional aplicable.	Escasa integración

Estas representaciones visuales complementan los hallazgos cualitativos al mostrar de forma clara la desigualdad entre las recomendaciones documentadas y la práctica empresarial. Es

evidente que, mientras las amenazas crecen en sofisticación, las respuestas organizacionales se mantienen rezagadas por desconocimiento, falta de formación, escasez de recursos o indiferencia institucional.

DISCUSIÓN

Los resultados obtenidos confirman que las pequeñas y medianas empresas (pymes) enfrentan serias dificultades para implementar estrategias integrales de ciberseguridad, a pesar del aumento exponencial de amenazas digitales. Esta situación refleja un desfase entre el crecimiento digital de las pymes y su capacidad institucional para gestionar los riesgos asociados. Como señala Navarro Uriol (2020), la mayoría de estas organizaciones operan sin políticas mínimas de protección de datos, lo que las convierte en blancos vulnerables frente a ataques cada vez más sofisticados.

Una de las causas más relevantes de esta brecha es la percepción limitada del riesgo digital. Las pymes suelen considerar la ciberseguridad como un gasto innecesario, asociado a grandes corporaciones, y no como una inversión estratégica. Esta visión ha sido ampliamente documentada por Bustillos y Rojas (2022), quienes argumentan que el bajo nivel de concienciación en entornos empresariales locales impide adoptar medidas preventivas eficaces. A esto se suma la ausencia de cultura organizacional en seguridad digital, lo que convierte al recurso humano en un punto crítico de vulnerabilidad, tal como señalan Maggi Murillo y Gómez Gómez (2021).

Otra barrera detectada es la falta de recursos económicos y tecnológicos. La implementación de sistemas de autenticación multifactor, backups externos o firewalls requiere una inversión que muchas pymes consideran inalcanzable. Sin embargo, estudios como el de ENISA (2021) subrayan que existen soluciones escalables y de bajo costo que pueden ser efectivas si se acompañan de una política interna coherente. El problema, por tanto, no es únicamente financiero, sino estructural: muchas pymes carecen de personal calificado, protocolos claros o incluso un responsable en seguridad de la información (ISO/IEC 27001:2018).

El análisis documental también mostró que, incluso en contextos con marcos normativos sólidos, como el europeo (GDPR), las pymes desconocen sus obligaciones legales o no cuentan con los mecanismos necesarios para cumplirlas (Ley Orgánica 3/2018; UIT, 2021). Esto implica riesgos legales adicionales, especialmente en sectores donde se procesan datos sensibles de clientes, proveedores o empleados. En Latinoamérica, esta brecha normativa es aún más evidente, como lo muestran los datos recogidos en Ramírez Montealegre (2016) y Santiago y Sánchez Allende (2017), donde la adopción de estándares como ISO 27001 es prácticamente inexistente.

Además, se observó que la implementación efectiva de estrategias depende en gran medida del liderazgo institucional. En las pocas pymes que reportaron buenas prácticas de ciberseguridad, existía una participación activa de la gerencia en procesos de formación, simulacros de respuesta y auditorías internas. Esto concuerda con lo planteado por De la Rosa (2019), quien sostiene que la seguridad digital debe integrarse en la planificación estratégica y no tratarse como un elemento accesorio o técnico.

Se destaca que la falta de interoperabilidad entre procesos tecnológicos y procedimientos organizativos es un obstáculo importante. La integración de herramientas de seguridad con procesos administrativos, financieros y comerciales requiere un enfoque transversal y no departamentalizado. Sin esta visión holística, los esfuerzos aislados pierden eficacia.

CONCLUSIÓN

El estudio permitió constatar que las pequeñas y medianas empresas (pymes) enfrentan una realidad compleja en materia de ciberseguridad, marcada por la coexistencia de amenazas digitales en crecimiento y una limitada capacidad institucional para prevenirlas o responderlas eficazmente. A través del análisis documental estructurado en cinco ejes temáticos amenazas, vulnerabilidades, estrategias técnicas, cultura organizacional y normativas se identificaron brechas profundas que afectan la integridad, disponibilidad y confidencialidad de los sistemas informáticos en este tipo de organizaciones.

Uno de los principales hallazgos conceptuales radica en que la ciberseguridad no depende exclusivamente de la tecnología implementada, sino de una visión estratégica que la integre dentro de la cultura organizacional. La falta de políticas internas, la escasa formación del personal y la ausencia de liderazgo en la gestión del riesgo digital constituyen factores estructurales que limitan cualquier esfuerzo técnico o normativo. Asimismo, se evidenció que muchas pymes desconocen marcos regulatorios fundamentales, lo cual las expone no solo a ataques informáticos, sino también a sanciones legales y pérdida de reputación.

En consecuencia, se concluye que la protección digital en las pymes requiere un enfoque integral que combine medidas técnicas accesibles, acciones formativas sostenidas, participación directiva activa y cumplimiento normativo. Superar las barreras identificadas implica no solo dotar a las pymes de herramientas, sino también de conciencia, compromiso y estructuras organizativas adaptadas al contexto digital contemporáneo.

BIBLIOGRAFÍA

Bustillos, J., & Rojas, J. (2022). Ciberseguridad en PYMES ecuatorianas: amenazas y desafíos. Revista Científica Arbitrada de la Fundación MenteClara, 7(1), 145–160. https://doi.org/10.32351/rca.v7.1.2022

Cyber Readiness Institute. (2020). Cyber Readiness for Small and Medium-Sized Businesses. https://cyberreadinessinstitute.org

Cherepanov, A., & Lipovsky, R. (2017). Trends in cybersecurity for small businesses. ESET Security Report. https://www.eset.com/int/business/

De la Rosa, J. (2019). Gestión del cambio organizacional y su impacto en la ciberseguridad. Revista Innovar Journal, 29(71), 88–97. https://doi.org/10.15446/innovar.v29n71.78976

ENISA. (2021). Cybersecurity for SMEs: Challenges and recommendations. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/cybersecurity-for-smes

Gobierno de Japón. (2020). Small and Medium Enterprise Cybersecurity Guidelines. Ministry of Economy, Trade and Industry. https://www.meti.go.jp/policy/netsecurity/

ISO/IEC 27001:2018. (2018). Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization.

Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales. (España). Boletín Oficial del Estado (BOE), 5 de diciembre de 2018.

Maggi Murillo, E., & Gómez Gómez, A. (2021). Percepción de la ciberseguridad en pymes costarricenses. Revista de Ciencias Empresariales, 9(1), 37–50. https://doi.org/10.15359/rce.9-1.3

Navarro Uriol, A. (2020). Ciberseguridad en la empresa: guía práctica para proteger la información. Fundación Telefónica. https://espacio.fundaciontelefonica.com/publicaciones/

National Institute of Standards and Technology (NIST). (2022). Small Business Cybersecurity Corner. U.S. Department of Commerce. https://www.nist.gov/itl/smallbusinesscyber

OECD. (2021). Digital Security for SMEs: Challenges and Policy Responses. OECD Digital Economy Papers, No. 309. https://doi.org/10.1787/7b895bce-en

Organización de Estados Americanos (OEA). (2020). Ciberseguridad: riesgos, avances y el papel de las PYMES en América Latina. https://www.oas.org/es/ciberseguridad

Ponsard, C., Poitevin, O., & Massonet, P. (2019). Cybersecurity for SMEs: challenges and recommendations. European Cybersecurity Organisation (ECSO). https://ecs-org.eu

Ponemon Institute. (2021). The 2021 State of Cybersecurity in Small & Medium-Sized Businesses. https://www.ponemon.org

Ramírez Montealegre, A. (2016). Las PYMES frente a la seguridad informática: diagnóstico y propuestas. Revista Latinoamericana de Tecnología, 14(2), 25–38.

Santiago, M., & Sánchez Allende, C. (2017). Ciberseguridad en pequeñas empresas: una aproximación desde la gestión del riesgo. Revista de Estudios Empresariales, 1(2), 95–110.

UIT (Unión Internacional de Telecomunicaciones). (2021). Guía de buenas prácticas para la ciberseguridad en micro y pequeñas empresas. Oficina Regional para las Américas. https://www.itu.int

Vergara-Romero, A., Martínez-Quintana, Y., & Pérez-Solano, M. (2021). Impacto de la concienciación en ciberseguridad en el rendimiento organizacional. Revista Iberoamericana de Sistemas, Cibernética e Informática, 18(2), 77–84.