Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), julio-agosto 2026,
Volumen 10, Número 4.

https://doi.org/10.37811/cl_rcm.v10i4

FACTORES DETERMINANTES DEL CUMPLIMIENTO DE NORMAS DE CIBERSEGURIDAD EN PEQUEÑAS Y MEDIANAS EMPRESAS: UN ANÁLISIS INTEGRAL DESDE LA GESTIÓN TECNOLOGÍCA Y ORGANIZACIONAL

DETERMINING FACTORS OF CYBERSECURITY COMPLIANCE IN SMALL AND MEDIUM ENTERPRISES: A COMPREHENSIVE ANALYSIS FROM TECHNOLOGICAL AND ORGANIZATIONAL MANAGEMENT

Franz Enrique Vinicio López García
Universidad Mariano Gálvez, Guatemala

DOI: https://doi.org/10.37811/cl_rcm.v10i4.25601

Factores Determinantes del Cumplimiento de Normas de Ciberseguridad en Pequeñas y Medianas Empresas: Un Análisis Integral desde la Gestión Tecnologíca y Organizacional

Franz Enrique Vinicio López García[1]
fralop16@gmail.com
https://orcid.org/0009-0005-8898-1505
Universidad Mariano Gálvez
Guatemala

RESUMEN

La creciente digitalización de los procesos empresariales ha incrementado significativamente la exposición de las pequeñas y medianas empresas a amanezas cibernéticas que afectan la continuidad operativa, la integridad de la información y la sostenibilidad organizacional. Aunque múltiples estándares internacionales han establecido lineamientos para fortalecer la seguridad de la información, persisten brechas importantes relacionadas con el cumplimiento efectivo de las normas de ciberseguridad por parte de los empleados dentro del entorno empresarial. En este contexto el presente estudio tuvo como objetivo determinar los factores que influyen en el cumplimiento de normas de ciberseguridad por parte de los empleados en las PYMES mediante un análisis integral desde las dimensiones tecnológicas y organizacional. La investigación se desarrollo bajo un enfoque cualitativo de carácter documental, sustentado exclusivamente en fuentes secundarias provenientes de artículos científicos, tesis, informes técnicos y publicaciones académicas recientes. Se realizó un búsqueda sistemática en base en base de datos científicas y repositorios abiertos utilizando palabras claves relacionadas con el cumplimiento normativo de ciberseguridad. Los resultados sugieren que las estrategias empresariales deben de trascender la implementación tecnológica y priorizar mecanismos sostenibles de gestión del comportamiento humano para incrementar los niveles de cumplimiento y resiliencia organizacional.

Palabras clave: ciberseguridad; cumplimiento normativo; pymes; gestión tecnológica, cultura organizacional.

[1] Autor principal.
Correspondencia: fralop16@gmail.com

Determining Factors of Cybersecurity Compliance in small and Medium Enterprises: A Comprehensive Analysis From Technological and Organizational Management

ABSTRACT

The growing digitalization of business processes has significantly increased the exposure of small and medium-sized enterprises to cyber threats that affect operational continuity, information integrity, and organizational sustainability. Although multiple international standards have established guidelines to strengthen information security, significant gaps persist regarding the effective compliance with cybersecurity rules by employees within the business environment. In this context, this study aimed to determine the factors that influence employees' compliance with cybersecurity rules in SMEs through a comprehensive analysis from technological and organizational dimensions. The research was conducted using a qualitative documental approach, based exclusively on secondary sources from scientific articles, theses, Recent technical reports and academic publications. A systematic search was carried out based on scientific databases and open repositories using keywords related to cybersecurity regulatory compliance. The results suggest that business strategies should go beyond technological implementation and prioritize sustainable mechanisms for managing human behavior to increase compliance levels and organizational resilience.

***Keywords*:** cybersecurity; regulatory compliance; smes; technology management; organizational culture

Artículo recibido 20 junio 2026
Aceptado para publicación: 20 julio 2026

INTRODUCCIÓN

La transformación digital ha redefinido los modelos operativos empresariales y generado oportunidades significativas para el crecimiento económico, la innovación y la eficiencia organizacional. Este proceso también ha aumentado la exposición frente a amenazas cibernéticas cada vez mas sofisticadas, afectando especialmente a las pequeñas y medianas empresas (PYMES), organizaciones que presentan limitaciones presupuestarias, escasez de capacidades técnicas y menor madurez en gestión de riesgos tecnológicos.

Las PYMES constituyen uno de los segmentos más vulnerables frente a incidentes de ciberseguridad debido a la limitada adopción de controles técnicos y políticas institucionales. En escenarios de creciente dependencia digital, el cumplimiento de normas de ciberseguridad deja de ser exclusivamente un desafío tecnológico y se convierte en una cuestión estratégica vinculada con la gobernanza organizacional y el comportamiento humano.

Los marcos de normativa internacional como ISO/IEC 27001, el marco de ciberseguridad del NIST y las recomendaciones sobre seguridad digital impulsadas por organismos multilaterales han promovido modelos orientados al fortalecimiento institucional mediante procesos continuos de identificación, protección, detección , respuesta y recuperación ante incidentes. Sin embargo existen estudios que han evidenciado que la adopción formal de estándares no garantiza comportamientos seguros por parte de los empleados.

El incumplimiento de normas internas continúa siendo una de las principales causas de incidentes de seguridad. El comportamiento organizacional sostienen que factores como percepción del riesgo, compromiso directivo, cultura institucional y formación continua poseen una influencia significativa sobre la adhesión a políticas de seguridad.

El conocimiento técnico individual resulta insuficiente cuando no existe una estructura organizacional capaz de sostener prácticas seguras de manera permanente. En consecuencia, ha surgido un interés creciente por integrar enfoques multidimensionales que combinen variables tecnológicas, humanas y administrativas.

En las PYMES esta problemática adquiere una relevancia particular debido a que dichas organizaciones suelen implementar controles de manera reactiva, priorizando inversiones operativas inmediatas por

encima de estrategias preventivas. Como resultado de los anterior persisten debilidades relacionadas con capacitación limitada, ausencia de monitoreo continuo y escaso involucramiento de los niveles directivos. Aunque existe una amplia producción científica sobre gestión de ciberseguridad, se observa una fragmentación conceptual respecto a los factores que implican el cumplimiento de normas por parte de los empleados. Gran parte de la evidencia se concentra en estudios cualitativos o en modelos desarrollados para grandes corporaciones, dejando un espacio limitado para investigaciones integradoras centradas en las particularidades de las PYMES.

Ante esta necesidad, el presente estudio propone una revisión cualitativa y comparativa de modelos documentados internacionalmente para identificar factores determinantes del cumplimiento normativo y construir una propuesta conceptual orientada a fortalecer la gestión tecnológica y organizacional.

El cumplimiento de normas de ciberseguridad en las PYMES no depende únicamente de la implementación tecnológica, sino de la interacción entre factores organizacionales, culturales y de gestión de conocimiento.

METODOLOGÍA

El estudio se desarrollo con un enfoque cualitativo con alcance descriptivo-análitico basado exclusivamente en fuentes secundarias. Este diseño permitió examinar de manera sistemática evidencia científica reciente relacionada con factores que influyen en el cumplimiento de normas de ciberseguridad de entornos empresariales.

La elección de la metodología respondió al interés de construir conocimiento integrador a partir de estudios existentes, evitando la generación de datos primarios mediante encuestas, entrevistas o experimentos.

El proceso metodológico consistió en identificar y depurar diversos modelos integrados de cumplimiento de normas de ciberseguridad para PYMES que fueron analizados para reconocer los enfoques y determinar los elementos mas útiles para la propuesta del modelo propio. La recopilación de información se desarrolló mediante una búsqueda sistemática estructurada en cuatro fases, utilizando palabras claves definidas en el estudio y realizando un análisis mediante codificación temática y comparación cruzada entre modelos.

Se aplicaron criterios de inclusión que exigieron textos completos disponibles, estudios relacionados con normas internacionales, investigaciones sobre comportamiento organizacional y publicaciones igual o posterior a 2022, lo que permitió integrar información reciente y coherente con la tendencias actuales.

RESULTADOS Y DISCUSIÓN

Síntesis general del análisis documental

El proceso de revisión documental permitió identificar patrones recurrentes asociados al cumplimiento de normas de ciberseguridad por parte de los empleados en las PYMES. Al comparar modelos y estudios recientes se observó que el cumplimiento no depende exclusivamente de controles tecnológicos, sino de la interacción entre condiciones organizacionales, capacidades humanas y mecanismos institucionales de gobernanza.

Del análisis surgieron seis factores principales:

1. Cultura organizacional orientada a la seguridad
2. Capacitación y concientización
3. Disponibilidad de infraestructura tecnológica
4. Apoyo de la dirección
5. Percepción del riesgo
6. Nivel de conocimiento en ciberseguridad

Estos factores fueron integrados posteriormente en una propuesta conceptual adaptada al contexto operativo de las PYMES.

Caracterización de los factores identificados

Tabla 1: Factores determinantes del cumplimiento de normas de ciberseguridad

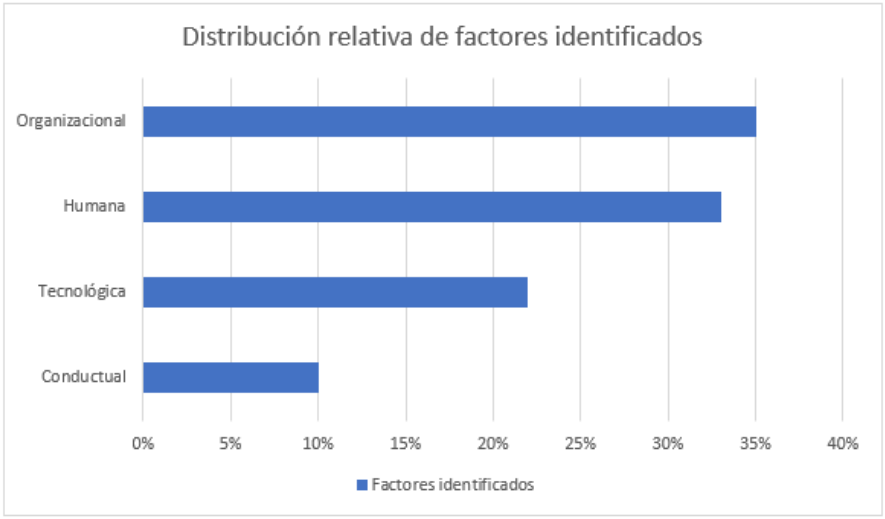
Factor	Dimensión	Descripción analítica	Nivel de influencia estimada
Cultura organizacional	Organizacional	Integración de prácticas seguras en procesos cotidianos	Muy alta
Capactiación y contización	Humana	Formación continua y desarrollo de hábitos de seguridad	Muy alta

Infraestructura tecnológica	Tecnológica	Disponibilidad de herramientas y controles	Alta
Apoyo de la dirección	Organizacional	Liderazgo y asignación de recursos	Muy Alta
Percepción del riesgo	Conductual	Reconocimiento del impacto potencial de incidentes	Alta
Nivel de conocimiento	Humana	Comprensión operativa de normas y amenazas	Alta

Los resultados muestran predominio en variables humanas y organizacionales sobre variables exclusivamente tecnológicas. La evidencia comparada indica que la tecnología actúa como habilitador del cumplimiento, pero no constituye el elemento central de sostenibilidad del comportamiento seguro.

Distribución conceptual de factores por dimensión

Figura 1. Distribución relativa de factores identificados



La distribución evidencia que aproximadamente dos terceras partes de los factores identificados corresponden a dimensiones organizacionales y humanas, reforzando la necesidad de modelos integrados de gestión.

Resultados por dimensión organizacional

La dimensión organizacional concentró la mayor cantidad de relaciones explicativas asociadas al cumplimiento. Particularmente, la cultura institucional y el compromiso de la dirección aparecieron como elementos transversales presentes en la mayoría de modelos analizados.

Tabla 2. Hallazgos asociados a la dimensión organizacional

Elemento observado	Evidencia recurrente	Impacto esperado
Cultura de seguridad	Incrementa adhesión a políticas	Alto
Liderazgo directivo	Facilita asignación de recursos	Alto
Comunicación institucional	Reduce incumplimiento	Medio-alto
Formalización de procesos	Favorece continuidad opertiva	Alto

Se identificó que organizaciones con políticas visibles y liderazgo activo presentan mayor estabilidad en prácticas seguras y menores desviaciones operativas.

Resultados por dimensión humana

El comportamiento del empleado fue identificado como uno de los componentes más sensibles dentro del cumplimiento normativo.

Tabla 3. Factores humanos vinculados al cumplimiento

Variable	**Manifestación observada**	**Resultado Esperado**
Capacitación continua	Mayor adherencia a normas	Incremento del cumplomiento
Concientización	Disminución de errores humanos	Reducción del riesgo
Conocimiento técnico	Mayor Capactidad de respuesta	Mayor resilencia
Percepción del riesgo	Conductas preventivas	Menor exposición

Figura 2. Relación concepctual entre formación y cumplimiento

La evidencia indica que la capacitación aislada genera mejoras limitadas, cuando se combina con mecanismos de concientización y seguimiento institucional, el efecto sobre el cumplimiento aumenta de manera consistente.

Resultados por dimensión tecnológica

La infraestructura tecnológica apareció como un factor facilitador del cumplimiento más que como un determinante independiente.

Tabla 4. Componentes tecnológicos identificados

Componente	Función principal	Relación con cumplimiento
Gestión de accesos	Control de exposición	Alta
Monitoreo continuo	Detección temprana	Alta
Automatización	Reducción del error humano	Media
Herramientas de protección	Mitigación de amenazas	Alta

Se observó que la eficiencia tecnológica aumenta cuando existe acompañamiento organizacional y formación de usuarios.

Integración de factores determinantes

Con base en la síntesis documental se desarrolló una estructura conceptual que explica el cumplimiento normativo como resultado de interacciones multidimensionales.

Figura 3. Modelo integrado de cumplimiento de normas de ciberseguridad para Pymes

Descripción del modelo: El modelo propuesto establece que el apoyo directivo constituye el factor habilitador inicial. Este componente fortalece simultáneamente la cultura organizacional y la disponibilidad tecnológica. Ambas dimensiones favorecen procesos permanentes de capacitación y generación de conocimiento, incrementando la percepción del riesgo y produciendo una mayor nivel de cumplimiento.

Matriz de consolidación de resultados

Tabla 5. Matriz integradora de factores identificados

Factor	Evidencia documnetal	Relación observada	Inclusión en modelo
Cultura organizacional	Alta	Directa	Si
Capacitación	Alta	Directa	Si
Infraestructura tecnológica	Media-alta	Indirecta	Si
Liderazgo directivo	Alta	Directa	Si
Percepción del riesgo	Alta	Mediadora	Si
Conocimiento	Alta	Directa	Si

Resultado principal del estudio

El análisis documental concluye que el cumplimiento de normas de ciberseguridad en las PYMES responde a un fenómeno organizacional multidimensional donde las capacidades tecnológicas son necesarias, pero insuficientes por sí solas. El cumplimiento sostenible surge cuando existe alineación entre liderazgo, cultura institucional, formación continua y apropiación del conocimiento por parte de los empleados de las PYMES.

DISCUSION

Interpretación general de los hallazgos

El presente estudio tuvo como objetivo determinar los factores que influyen en el cumplimiento de normas de ciberseguridad por parte de los empleados en las pequeñas y medianas empresas mediante un análisis documental de la literatura científica reciente y de los principales marcos internacionales de ciberseguridad. Los resultados obtenidos permitieron identificar seis factores determinantes: cultura organizacional orientada a la seguridad, capacitación y concientización, disponibilidad de infraestructura tecnológica, apoyo de la dirección, percepción del riesgo y nivel de conocimiento en ciberseguridad.

Estos factores fueron integrados en un modelo conceptual que explica el cumplimiento normativo como un proceso sistemático en el que convergen elementos organizacionales, tecnológicos y conductuales.

Los hallazgos confirman una tendencia observada en la literatura publicada durante los últimos años: la ciberseguridad en las PYMES ha dejado de ser exclusivamente como un problema tecnológico para entenderse como una capacidad organizacional que requiere liderazgo, aprendizaje continuo y una cultura institucional orientada a la gestión del riesgo. En este sentido, (Ye, 2026) desarrolló un modelo integrado en los enfoques Technology-Organization-Environment (TOE) y Resource-Based View (RBV), demostrando que la concientización en ciberseguridad constituye el predictor mas importante de la efectividad de la gestión de la ciberseguridad en las micro, pequeñas y medianas empresas, seguido por la preparación tecnológica y el cumplimiento regulatorio. Adicional, el estudio evidenció que la efectivad de la gestión actúa como variable mediadora entre los recursos organizacionales y el desempeño empresarial, lo que coincide con el modelo conceptual propuesto en la presente investigación.

Esta convergencia teórica resulta importante porque sugiere que el cumplimiento de normas no depende únicamente de la existencia de políticas de seguridad o de controles tecnológicos, sino de la capacidad de la organización para trasformar y procesar dichos recursos en comportamientos seguros por parte de los empleados. Desde esta perspectiva, la presente investigación aporta una visión complementaria al demostrar que la interacción entre liderazgo, cultura organizacional, capacitación y conocimiento constituye el mecanismo mediante el cual las organizaciones fortalecen la resiliencia frente a amenazas cibernéticas.

Otro aspecto significativo identificado durante el análisis documental fue la estrecha relación entre la percepción institucional de la ciberseguridad y la madurez organizacional. Investigaciones recientes han mostrado que muchas PYMES sobreestiman su nivel de preparación frente a amenazas digitales cuando la evaluación se basa exclusivamente en autopercepción. (Chidukwani, Zander y Koutsakis, 2026), mediante un estudio de casos múltiples publicado en Computers & Security, compararon autoevaluaciones empresariales con evaluaciones técnicas independientes y encontraron discrepancias sistemáticas entre la percepción de cumplimiento y la implementación real de controles de seguridad.

Los autores concluyen que las organizaciones suelen confundir la existencia de soporte informático con capacidades efectivas de ciberseguridad, especialmente en funciones críticas como identificación de activos, gestión de vulnerabilidades, monitoreo continuo y respuesta ante incidentes.

Este resultado guarda una estrecha relación con el modelo propuesto en la presente investigación, en el cual la infraestructura tecnológica aparece como un elemento habilitador del cumplimiento, pero no como factor suficiente para garantizar comportamientos seguros. En consecuencia, la evidencia reciente respalda la necesidad de complementar las inversiones tecnológicas con mecanismos de gobernanza, capacitación permanente y fortalecimiento de cultura organizacional.

Los resultados obtenidos son consistentes con la evolución reciente de los marcos internacionales de ciberseguridad. Tanto la actualización de ISO/IEX 27001:2022 como la NIST Cybersecurity Framework 2.0 enfatizan que la gestión de la ciberseguridad debe de integrarse en la estrategia organizacional, promoviendo una gobernanza que involucre activamente a la alta dirección, los responsables tecnológicos y los usuarios finales. Esta orientación coincide con el modelo conceptual desarrollado en esta investigación, en el cual el apoyo directivo constituye el elemento articulador que conecta las dimensiones organizacionales y tecnológicas para favorecer el cumplimiento sostenible de las normas.

En conjunto los resultados permiten sostener que el cumplimiento de normas de ciberseguridad debe entenderse como un proceso organizacional continuo, sustentado en capacidades dinámicas de aprendizaje, adaptación y mejora continua, más que como un requisito regulatorio o una consecuencia automática de la implementación tecnológica.

Cultura organizacional y cumpliminto de normas de ciberseguridad

Entre los factores identificados en esta investigación, la cultura organizacional orientada a la seguridad emergió como el componente con mayor capacidad integradora dentro del modelo propuesto. La evidencia documental analizada mostró que las organizaciones que incorporan la ciberseguridad como parte de sus valores institucionales presentan mayores niveles de cumplimiento normativo, mayo participación de los empleados en actividades preventivas y una mayor capacidad para responder ante incidentes.

Esta observación coincide con la revisión de evidencia publicada por (Sharma y aparacio, 2022) en Computers & Security, quienes analizaron la influencia de la cultura organizacional y la cultura de equipo sobre la motivación de protección de los empleados. Los autores demostraron que una cultura organizacional caracterizada por el liderazgo participativo, comunicación efectiva y apoyo institucional incrementa la percepción de amenaza y la percepción de eficiencia de los controles de seguridad, fortaleciendo así la intención de cumplir las políticas organizacionales. Asimismo, evidenciaron que las subculturas presentes en los equipos de trabajo pueden reforzar o debilitar la efectividad de las políticas institucionales, destacando la importancia de la coherencia entre los distintos niveles organizacionales.

La importancia de la cultura organizacional también ha sido confirmada por la revisión de evidencia realizada por investigadores de Computers & Security en el año de 2025, quienes sintetizaron 59 estudios sobre cultura de ciberseguridad con el propósito de construir un marco conceptual para su medición. Los resultados muestran que una cultura solida de ciberseguridad no puede reducirse a campañas de capacitación o al cumplimiento formal de políticas, sino que requiere liderazgo visible, participación activa de la alta dirección, comunicación permanente, mecanismos de retroalimentación y alineación entre los objetivos estratégicos y los comportamientos esperados de los empleados. El estudio concluye que la cultura de ciberseguridad constituye un problema de gestión organizacional antes que un problema exclusivamente tecnológico, recomendando integrar indicadores culturales dentro de los sistemas de gestión de seguridad de información.

Los resultados obtenidos en la presente investigación respaldan plenamente este perspectiva. Durante el análisis documental se observó que la cultura organizacional no actúa como un factor independiente, sino como un elemento transversal que condiciona la efectividad de la capacitación, la apropiación del conocimiento, la percepción del riesgo y la utilización adecuada de la infraestructura tecnológica. En consecuencia, la cultura organizacional opera como un mecanismo de integración que facilita la consolidación de comportamientos seguros en todos los niveles de la empresa.

En el contexto específico de las PYMES este aspecto adquiere especial relevancia debido a sus limitaciones estructurales en recursos financieros y humanos. En este sentido, (Awolowo,2026), en el Canadian Journal of Administrative Sciences, propone un marco conceptual de aseguramiento de la ciberseguridad para PYMES que integra cultura organizacional, gestión del riesgo de fraude y

contabilidad forense. El autor sostiene que las pequeñas empresas obtienen mayores beneficios cuando la ciberseguridad se incorpora como un activo estratégico de la organización y no como un requisito exclusivamente técnico o regulatorio. Además, plantea que una cultura organizacional orientada a la seguridad incrementa la confianza de los clientes, fortalece la continuidad operativa y mejora la competitividad empresarial.

En consecuencia, la evidencia reciente coincide en señalar que el fortalecimiento de la cultura organizacional constituye una de las estrategias más efectivas para incrementar el cumplimiento de normas de ciberseguridad en las PYMES. El modelo conceptual desarrollado en esta investigación amplía dicha perspectiva al proponer que la cultura organizacional interactúa dinámicamente con el liderazgo, la capacitación, el conocimiento, la percepción del riesgo y la infraestructura tecnológica, configurando un sistema integral de cumplimiento normativo. Este enfoque sistémico representa una contribución teórica relevante, ya que permite comprender el cumplimiento de normas como un proceso organizacional continuo y no como el resultado aislado de intervenciones tecnológicas o regulatorias.

El propósito del presente estudio fue determinar los factores que influyen en el cumplimiento de normas de ciberseguridad por parte de los empleados en pequeñas y medianas empresas mediante un análisis integral desde la gestión tecnológica y organizacional. A partir de la revisión documental sistemática y del análisis comparativo de modelos recientes, los resultados evidenciaron que el cumplimiento normativo constituye un fenómeno multidimensional cuya explicación excede la implementación de controles tecnológicos aislados.

Los hallazgos muestran que la cultura organizacional orientada a la seguridad, el apoyo de la dirección, la capacitación continua, el conocimiento en ciberseguridad, la percepción del riesgo y la disponibilidad tecnológica conforman un sistema interdependiente que condiciona el comportamiento del cumplimiento dentro de las organizaciones.

Estos resultados respaldan enfoques contemporáneos de gobernanza de ciberseguridad que reconocen el factor humano como un componente central en la efectividad de las estrategias de protección digital.

Modelo conceptual propuesto

El principal aporte de esta investigación consiste en el desarrollo de un modelo conceptual integrador para explicar el cumplimiento de normas de ciberseguridad en las PYMES desde una perspectiva

tecnológica y organizacional. A diferencia de modelos que analizan de manera aislada variables relacionas con la infraestructura tecnológica, la capacitación o la cultura organizacional, la propuesta desarrollada integra estos factores dentro de un sistema dinámico de relaciones que permite comprender el cumplimiento como un proceso continuo de gestión organizacional.

El modelo plantea que el apoyo de la alta dirección constituye el punto de partida para el fortalecimiento de la cultura organizacional y la asignación de recursos tecnológicos. Estas dos dimensiones crean las condiciones necesarias para implementar programas permanentes de capacitación y generación de conocimiento, los cuales incrementan la percepción del riesgo y favorecen el cumplimiento de las normas institucionales. Finalmente, el cumplimiento sostenido fortalece la resiliencia organizacional y mejora la capacidad de respuesta frente a incidentes de ciberseguridad.

Desde una perspectiva teórica, esta propuesta presenta importantes puntos de convergencia con el modelo TOE. Mientras que el enfoque del modelo TOE explica la adopción de innovaciones tecnológicas a partir de factores tecnológicos, organizacionales y ambientales, el modelo propuesto incorpora explícitamente variables relacionadas con el comportamiento humano y la cultura organizacional, ampliando su capacidad explicativa para el contexto específico del cumplimiento normativo en ciberseguridad.

De igual forma, el modelo guarda correspondencia con la Resource-Based View (RBV) al considerar que el conocimiento, la cultura organizacional y el liderazgo constituyen recursos capaces de generar ventajas competitivas sostenibles. Sin embargo, la presente investigación propone que dichos recursos adquieren valor únicamente cuando interactúan mediante procesos organizacionales que favorecen el aprendizaje, la coordinación institucional y la apropiación de las normas de seguridad.

Otra contribución relevante consiste en la alineación del modelo con la estructura del NIST Cibersecurity Framework 2.0, particularmente con la función Govern, incorporada en la actualización de 2024. Mientras este marco internacional establece la necesidad de fortalecer la gobernanza de la ciberseguridad, el modelo desarrollado identifica los mecanismos organizacionales mediante los cuales dicha gobernanza puede traducirse en comportamientos afectivos de cumplimiento dentro de las PYMES.

La propuesta resulta consistente con los principios establecidos en la ISO/IEC 27001:2022, especialmente en lo referente al liderazgo, la competencia, la concientización, la comunicación y la mejora continua. No obstante, el modelo amplía esta perspectiva al representar gráficamente las relaciones funcionales entre los factores identificados durante el análisis documental, proporcionando una herramienta conceptual que puede orientar futuras investigaciones empíricas y procesos de implementación organizacional.

En consecuencia, el modelo propuesto constituye una contribución teórica que integra evidencia reciente sobre gestión de ciberseguridad, comportamiento organizacional y gobernanza tecnológica, ofreciendo una visión sistémica del cumplimiento de normas adaptada a las características operativas de las PYMES.

CONCLUSIONES

El Presente estudió facilitó la identificación de los factores clave que afectan el cumplimiento de las normas de ciberseguridad por parte de los empleados de las PYMES, a través de un análisis documental que consideró enfoques tanto tecnológicos como organizacionales.

Los hallazgos indican que el cumplimiento no solo es el resultado de la tecnología disponible, sino un fenomeno complicado que se ve afectado por elementos culturales, organizacionales y de comportamiento. Entre los factores mas relevantes se identificaron la cultura organizacional orientada a la seguridad, el apoyo de la dirección, la capacitación continua, la percepción del riesgo, el nivel de conocimiento y la disponibilidad de infraestructura tecnológica.

El análisis mostró que el liderazgo dentro de la institución actúa como un conector que trasnforma habilidades tecnológicas en prácticas sostenibles de cumplimiento.

Como contribución principal, se elaboró un modelo conceptual integrador para pequeñas y medianas empresas que sugiere relaciones entre factores humanos, organizacionales y tecnológicos, ofreciendo un fundamento teórico para futuras pruebas empíricas.

Las estrategias empresariales enfocadas en mejorar la ciberseguridad deben avanzar de enfoques que se centran solo en herramientas hacia modelos holísticos que den prioridad a la gestión del comportamiento organizacional y al aprendizaje continuo.

REFERENCIAS BIBLIOGRAFICAS

Agencia de la Unión Europea para la Ciberseguridad (ENISA). (2023). Directrices sobre la cultura de ciberseguridad: Enfoques conductuales y organizacionales de la ciberseguridad. ENISA. Obtenido de: Agencia de la Unión Europea para la Ciberseguridad | Unión Europea

Alshaikh, M. (2020). Desarrollando una cultura de ciberseguridad para influir en el comportamiento de los empleados. Computers & Security, 98, 102003. Obtenido de: https://www.sciencedirect.com/science/article/abs/pii/S0167404820302765

Awolowo, I. F. (2026). Marco de aseguramiento de la ciberseguridad para pequeñas y medianas empresas: Integrando la contabilidad forense y la resiliencia organizacional. Canadian Journal of Administrative Sciences. https://doi.org/10.1002/cjas.70051. Obtenido de: https://onlinelibrary.wiley.com/doi/full/10.1002/cjas.70051?msockid=334914ce2f896c232a82062a2e376d1c

Chidukwani, A., Zander, S., & Koutsakis, P. (2026). Evaluación de la postura de ciberseguridad en pequeñas y medianas empresas: Un marco para validar la madurez de la ciberseguridad organizacional. *Computers & Security*, 143, Artículo 104119. Obtenido de: https://www.sciencedirect.com/science/article/pii/S0167404826000155

Chikwendu, Stephen. (2026). Conciencia y cumplimiento en ciberseguridad entre las pequeñas y medianas empresas (pymes) en el estado de anambra. Obtenido de: https://www.nigerianjournalsonline.org/index.php/NJAH/article/view/506

Instituto Nacional de Estándares y Tecnología. (2024). El Marco de Ciberseguridad NIST (CSF 2.0). Departamento de Comercio de EE. UU. Obtenido de: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf

ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de seguridad de la información — Requisitos. Obtenido de: https://www.iso.org/es/norma/27001?tid=331662889277

ISO/IEC 27002:2022. Controles de seguridad de la información.

NIST. (2024). Marco de Ciberseguridad (CSF 2.0).

Michalek, J, O'Shaughnessy, p, Wahlstrom K, (2026), Prevención y respuesta a incidentes cibernéticos para pequeñas y medianas empresas: una revisión del alcance. https://doi.org/10.1016/j.cose.2026.104972 . Obtenido de: https://www.sciencedirect.com/science/article/pii/S0167404826001483

OCDE. (2022). Marco de Gestión de Riesgos de Seguridad Digital.

Organización Internacional de Normalización. (2022). ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de datos personales—Sistemas de gestión de la seguridad de la información—Requisitos. ISO. Obtenido de: https://www.iso.org/es/norma/27001?tid=331662889277

Rand, M., Bada, M., Furnell, S., Nurse, J. R. C., & Khan, N. (2026). Comprender las prácticas de ciberseguridad en pymes: una investigación de métodos mixtos. *Revista de Seguridad de la Información: Una perspectiva global,* 1-39. https://doi.org/10.1080/19393555.2026.2648174

Sarker, I. H., et al. (2020). Ciencia de datos en ciberseguridad. Journal of Big Data, 7(1). Obtenido de: https://www.scirp.org/reference/referencespapers?referenceid=3286801

Sharma, R., y Aparicio, M. (2022). Cultura organizacional, cultura del equipo y cumplimiento de ciberseguridad por parte de los empleados: Un análisis empírico basado en la teoría de la motivación de protección. Computers & Security, 121, 102840. Obtenido de: https://www.mendeley.com/catalogue/6ea8c2b8-a791-33f1-8731-9dcac9b87aa6/

Ye, Y. (2026). Determinants of cybersecurity management effectiveness in SMEs: An integrated TOE and Resource-Based View approach. SAGE Open, 16(1). https://doi.org/10.1177/21582440251414951

Zyoud, A., y Lutfi, A. (2024). Cultura de seguridad de la información y adopción de Zero Trust: El papel moderador del liderazgo organizacional. IEEE Access, 12, 1–18. Obtenido de: https://ui.adsabs.harvard.edu/abs/2024IEEEA..1272420Z/abstract