ISBN: 978-628-96613-3-0. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2026.1.1.1611

Applicability Evaluation of a Managed Cybersecurity Solution as a Service for Micro, Small and Medium-Sized Enterprises (MSMEs) in Honduras

Eleazar Guifarro Chávez[1]; Boniek Daniel Chavarría Romero[2]
[1] Universidad Nacional Autónoma de Honduras, UNAH-VS, Honduras, *eleazar_chavez@unitec.edu*
[2] Centro Universitario Tecnológico, Universidad Tecnológica Centroamericana (UNITEC), Honduras, *boniek_chavarria@unitec.edu*

***Abstract* — This research evaluates the applicability of a managed cybersecurity solution for MSMEs in Honduras in response to the growing incidence of cyberattacks affecting the digital economy. A mixed applied, exploratory, and descriptive approach was adopted, collecting data through 389 surveys administered to MSMEs and interviews with subject-matter experts. The analysis was grounded in change management theory, strategic planning principles, international cybersecurity frameworks (ISO 27001, NIST CSF, and CIS Controls), and the PMBOK good practices guide. The findings reveal a low level of digital maturity: 53.21% of MSMEs lack formal risk management policies, and 31.88% do not possess legally licensed basic software. Nevertheless, 83.54% expressed willingness to invest in cybersecurity solutions. As a result, this study proposes an original five-phase, tiered model designed to externalize technical complexity and ensure operational continuity, representing a viable and adapted proposal to strengthen business resilience against current cybersecurity risks.**

***Keywords*-- Cybersecurity, MSMEs, MSS, Incident, SOC.**

Evaluación de Aplicabilidad de una Solución de Ciberseguridad Gestionada como Servicio para MIPYMES en Honduras

Eleazar Guifarro Chávez[1]; Boniek Daniel Chavarría Romero[2]
[1] Universidad Nacional Autónoma de Honduras, UNAH-VS, Honduras, eleazar_chavez@unitec.edu
[2] Centro Universitario Tecnológico, Universidad Tecnológica Centroamericana (UNITEC), Honduras, boniek_chavarria@unitec.edu

Resumen*– Esta investigación evalúa la aplicabilidad de una solución de ciberseguridad gestionada para MIPYMES en Honduras ante la creciente incidencia de ataques que afectan la economía digital. Se adoptó un enfoque mixto de tipo aplicado, exploratorio y descriptivo, recolectando datos mediante 389 encuestas a MIPYMES y entrevistas a expertos. El análisis se sustentó en teorías de gestión del cambio, planeación estratégica, marcos internacionales de ciberseguridad (ISO 27001, NIST CSF y CIS Controls) y la guía de buenas prácticas del PMBOK. Se identificó una baja madurez digital: 53.21% de las MIPYMES carece de políticas formales de gestión de riesgos y 31.88% no posee licencias legales de software básico. No obstante, un 83.54% está dispuesta a invertir en ciberseguridad. Se propone un modelo original, escalonado en cinco fases, diseñado para externalizar la complejidad técnica y garantizar la continuidad operativa, representando una propuesta viable y adaptada para fortalecer la resiliencia empresarial frente al riesgo actual.

***Palabras clave*-- Ciberseguridad, MIPYMES, MSS, Incidente, SOC.**

I. INTRODUCCIÓN

Mientras la revolución tecnológica impulsa el desarrollo, la ciberdelincuencia ha dejado de ser un riesgo periférico para convertirse en una fuerza disruptiva a escala macroeconómica, con daños globales estimados en 10.29 billones de dólares durante el año 2025 y daños proyectados a 16 billones de dólares para el año 2029 [1]. En Honduras, las MIPYMES constituyen el 95% del tejido empresarial y generan el 70% de los empleos formales [2]. A nivel internacional, los marcos normativos y metodológicos recomiendan ampliamente fortalecer la seguridad de la información en organizaciones de cualquier tamaño, sin embargo, su adopción en las MIPYMES hondureñas es prematura, operando bajo una alta informalidad, escasez de personal calificado y recursos limitados.

Este escenario se agrava por la evolución del concepto de ciberseguridad, que ha transitado desde la simple seguridad informática perimetral (transmisión segura de datos) hacia un ecosistema complejo de gestión de riesgos que involucra personas-procesos-gobernanza, y que debe preservar la tríada CIA (confidencialidad, integridad y disponibilidad) de la información en el ciberespacio [3]. Honduras fue catalogada en 2020 con un nivel de preparación "incipiente" ante ciberataques [4]. Datos de 2025 indican que el país carece de mecanismos esenciales, cumpliendo parcialmente con solo 12 de 49 indicadores de protección evaluados internacionalmente [5]. Las empresas enfrentan amenazas como ransomware y phishing, donde los rescates exigidos oscilan entre 2,000 y 20,000 dólares, sin garantías de recuperación [6].

La problemática se profundiza al considerar que en Honduras operan aproximadamente 1,200,000 empresas, y menos del 30% son formales, lo que significa que más de 870,000 negocios en Honduras operan en la informalidad, generando el 44% del PIB (equivalente a unos 300,000 millones de lempiras), dificultando la inclusión de las MIPYMES en planes nacionales de protección digital [7]. Además, el país carece de una ley integral de ciberseguridad, limitándose a tipificar delitos en el Código Penal como el acceso no autorizado (Art. 398) y la suplantación de identidad (Art. 401) [8].

A pesar de los avances en protección de datos se identifica que existe un vacío de conocimiento y limitación académica sobre las soluciones de ciberseguridad gestionada; actualmente no hay estudios previos de la aplicabilidad de ningún modelo de solución ciber gestionada de dominio público en el país con este nivel de complejidad para la MIPYME, constituyendo el modelo que se propone en esta investigación como el primero de su clase en Honduras. Este escenario evidencia la urgente necesidad de investigaciones que orienten estrategias efectivas, informadas y sostenibles que guíen la toma decisiones, disminuyan la vulnerabilidad y contribuyan a la resiliencia económica y digital del país ante un entorno cibernético en evolución.

II. METODOLOGÍA

El objetivo final de la investigación es diseñar un modelo adaptado a las capacidades operativas y necesidades del sector, analizando su madurez en gestión de riesgos y su viabilidad técnica, económica y organizacional. Para ello, se estableció una ruta metodológica solida replicable para futuras investigaciones en este campo de conocimiento, con resultados sustanciales, y un marco aplicable construido en base a marcos internacionales, metodologías de gestión y guías de buenas prácticas, con carácter referente, ampliamente probados, aceptados y reconocidos.

A. Diseño metodológico

La investigación se enmarca en un estudio aplicado, exploratorio y descriptivo, orientada a evaluar la viabilidad de implementar una solución de ciberseguridad gestionada como

servicio (MSS) en MIPYMES hondureñas. Se adoptó un enfoque mixto, combinando técnicas cuantitativas (encuestas estructuradas) y cualitativas (entrevistas semiestructuradas y análisis documental de marcos normativos), con el objetivo de obtener una visión holística de las condiciones tecnológicas, organizacionales y financieras del sector. Este diseño metodológico asegura la coherencia entre los objetivos de la investigación y las variables de estudio, posibilitando identificar las brechas existentes en infraestructura, gobernanza y cultura digital, así como oportunidades de aplicar modelos graduales de madurez en ciberseguridad adaptados al modelo hondureño.

B. Fundamentación técnica

El sustento técnico de esta investigación es una integración de marcos y estándares internacionales utilizados como fundamento durante todo el proceso de construcción de la investigación y el modelo propuesto, con el objetivo de ofrecer una estructura real y apegada al avance global, puesto que la ciberseguridad no es un concepto aislado.

Al utilizar referencias sólidas y con reconocimiento internacional, este modelo de investigación es replicable en cualquier entorno que tenga condiciones similares a las de nuestras MIPYMES:

- NIST Cybersecurity Framework (CSF) 2.0: Organizando las actividades en cinco pilares: Identificar, Proteger, Detectar, Responder y Recuperar [9].
- CIS Controls V8: Prioriza 18 controles críticos; priorizando el nivel IG1 diseñado específicamente para ciberhigiene básica en entornos con recursos limitados [10].
- ISO/IEC 27001: Para definir los requisitos de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en riesgos [11].
- ISO 22301: Se centra en la continuidad del negocio, y se utilizó para establecer métricas de resiliencia operativa, definiendo un Tiempo Objetivo de Recuperación (RTO), un Umbral de Pérdida Aceptable (MTL) y un Periodo máximo tolerable de interrupción (MPO) [12].

C. Marco teórico de adopción

El marco teórico de la investigación se fundamenta en la congruencia entre el problema, los objetivos y las técnicas de recolección de datos, siguiendo la guía de buenas prácticas del PMBOK, lo que asegura coherencia metodológica y rigor en la aplicación de modelos de gestión. Para comprender la manera de adoptar el modelo de ciberseguridad gradual a las MIPYMES:

- Teoría de gestión del cambio: Modelo de tres fases de Kurt Lewin (descongelar, cambiar, recongelar) [13].
- Teoría de gestión del cambio: Modelo de ocho pasos de John Kotter, con su descripción de fases (urgencia, coalición, visión, comunicación, empoderamiento, victorias rápidas, consolidación, institucionalización) [14].
- Metodología de planeación estratégica: Se utilizaron herramientas de análisis estratégico como PESTEL, FODA y las 5 fuerzas de Porter [15]. Con el objetivo de evaluar la realidad actual y la interacción entre los actores clave, interesados y segmentos de la población estudiada.

Estas teorías permiten comprender cómo las MIPYMES pueden adoptar gradualmente un modelo de ciberseguridad gestionada sin generar resistencia organizacional.

D. Población y muestra

La población objetivo está compuesta por propietarios, gerentes, supervisores, administradores y responsables de TI de MIPYMES hondureñas de diversos sectores económicos (comercio, servicios, manufactura), seleccionando empresas que cumplieran con criterios de representatividad en cuanto a:

- Tamaño: La MIPYMES en Honduras, se pueden clasificar por su tamaño, definido principalmente por su cantidad de empleados en micro (de 1 a 9 colaboradores), pequeñas (10 a 49) y medianas empresas (50 o más).
- Ubicación: Zona centro y norte del país.
- Nivel de digitalización: Operan con al menos un grado básico de infraestructura tecnológica (uso de computadoras, acceso a internet, software administrativo).

Además de los criterios de representatividad, se establecieron tipos de muestreo diferenciados para los instrumentos de recolección de datos:

- Encuesta: El muestreo utilizado fue no probabilístico de tipo intencional - estratificado. El tamaño de la muestra se calculó mediante la fórmula para poblaciones infinitas (n=384.16), obteniendo 389 encuestas filtradas con una confiabilidad del 95% y un margen de error del 5%.
- Entrevista: Aplicada por medio de un muestreo no probabilístico por conveniencia, seleccionando y entrevistando un grupo reducido de 5 expertos, consultores y responsables de seguridad digital con más de 10 años de experiencia comprobable en materia de ciberseguridad para MIPYMES. No se definió un número de entrevistas con base a criterio estadístico, sino bajo el principio de saturación teórica.

E. Instrumentos de recolección de datos

- Encuesta: Se aplicó una encuesta estructurada de 30 preguntas para medir el nivel de madurez digital, percepción de riesgo, inversión en seguridad y conocimiento sobre MSS.
- Guia de entrevista: Se utilizó una guía de entrevista temática de 15 ítems sobre viabilidad técnica, cultural y económica de implementar MSS en MIPYMES.
- Ficha de análisis documental: utilizada para revisar informes nacionales e internacionales sobre ciberseguridad, legislación vigente y políticas públicas.

F. Operacionalización de variables

Por motivos de estudio, se definieron estratégicamente las variables a estudiar de manera sistemática:

- Condiciones tecnológicas (V1): infraestructura, conectividad, uso de software, presencia de firewalls y antivirus.

- Madurez y resiliencia en gestión de riesgos digitales (V2): existencia de políticas, frecuencia de evaluaciones, respuesta a incidentes.
- Costos asociados (V3): inversión actual en seguridad, percepción de impacto financiero ante ataques.
- Factores de gobernanza y organizacionales (V4): apoyo gerencial, actitud del personal, capacitación interna.
- Pertinencia del modelo MSS (V5): percepción sobre la utilidad, escalabilidad y adaptabilidad del modelo propuesto.

Cada variable fue operacionalizada con indicadores específicos y escalas de medición tipo Likert.

G. Procedimiento de análisis

El proceso metodológico se desarrolló en cinco etapas:

- Diseño y validación de instrumentos por expertos: Se contó con la participación de un especialista con más de treinta años de trayectoria comprobable en ciberseguridad para el sector, quien validó la suficiencia y relevancia de los ítems técnicos, un experto metodológico que verificó la consistencia lógica, la estructura y la adecuación de las escalas de medición y un experto en análisis estadístico de fiabilidad de instrumentos). Para asegurar la consistencia interna del instrumento de recolección de datos, se realizó un análisis de fiabilidad sobre una submuestra de n=50 casos. Los resultados ofrecieron indicadores robustos de consistencia interna con un Alpha de Cronbach's (α) de 0.85 y un Alpha de Cronbach's ordinal (αρ) de 0.91 (siendo este indicador el más adecuado para la naturaleza de la escala Likert empleada en la herramienta). Complementariamente, se obtuvo un Lambda 6 de Guttman (λ6) de 0.90 y un Omega de McDonald (ω) de 0.82 (ajustado por cargas factoriales), ratificando que el instrumento posee la estabilidad necesaria para diagnosticar con rigor las brechas de ciberseguridad en las MIPYMES de Honduras.
- Recolección de datos.
- Codificación y análisis estadístico (cualitativo y cuantitativo).
- Integración multivariada de resultados: utilizando software estadístico especializado (POWER BI AI). El análisis se apoyó en matrices de cruce entre variables criticas para determinar coeficientes de relación causal.
- Finalmente, los resultados se sintetizaron en una propuesta de modelo aplicable y adaptable, reconociendo que su eficiencia operativa debe ser contrastada en futuras implementaciones empíricas a gran escala.

III. RESULTADOS Y ANÁLISIS

El análisis de los datos obtenidos permite identificar las principales condiciones técnicas, organizacionales, económicas y culturales que determinan la viabilidad de implementar un modelo de ciberseguridad gestionada como servicio (MSS) en las MIPYMES hondureñas. Los hallazgos de la investigación reflejan tanto fortalezas como debilidades a nivel estructural, que condicionan la pertinencia del modelo propuesto.

En la Tabla I se demuestra que la MIPYME posee el "cuerpo" tecnológico (antivirus y conectividad), pero carece del "cerebro" administrativo (políticas y gobernanza). Esta desconexión genera un alto riesgo residual, invalidando la inversión técnica actual al no tener procesos que garanticen la tríada CIA (Confidencialidad, Integridad y Disponibilidad).

TABLA I
BRECHA DE INFRAESTRUCTURA VS. GOBERNANZA
LA PARADOJA ESTRUCTURAL: INFRAESTRUCTURA VS. GOBERNANZA

Dimensión de análisis	Indicador crítico	Estadística (%)	Implicación de ingeniería / Gestión
Infraestructura técnica (Fortaleza)	Disponibilidad de antivirus actualizados.	80.98%	Existe una base tecnológica adecuada y capacidad de protección perimetral básica.
Gobernanza y gestión (Debilidad)	Incumplimiento de factores de gobernanza estatal.	88.18%	La tecnología carece de un marco normativo que dirija su uso estratégico.
Infraestructura técnica (Fortaleza)	Presencia de Firewalls activos.	68.38%	Conectividad protegida a nivel de red para soportar servicios gestionados.
Gobernanza y gestión (Debilidad)	Ausencia de políticas formales de gestión de riesgos.	53.21%	La seguridad se maneja de forma reactiva y empírica, no sistemática.
Infraestructura técnica (Fortaleza)	Estabilidad de conexión a internet.	68.38%	Viabilidad técnica inmediata para la adopción de un modelo MSS remoto.
Gobernanza y gestión (Debilidad)	Falta de apoyo gerencial a iniciativas de seguridad.	40.10%	Barrera cultural que impide anclar la ciberseguridad como un valor del negocio.

Fuente: Elaboración propia.

Estos hallazgos revelan lo que denominamos paradoja estructural: una desconexión crítica entre la adopción de herramientas técnicas y la madurez administrativa. Esta disparidad sugiere que la ciberseguridad en el sector se percibe erróneamente como un producto adquirible (software) y no como un proceso de gestión sostenido, lo que anula la efectividad de la infraestructura existente al carecer de un marco de políticas que la dirija.

A continuación, se presentan los resultados organizados por dimensiones (V1 – V5), todas vinculadas a las variables de estudio.

A. Condiciones Tecnológicas (V1)

La viabilidad técnica es positiva desde la disponibilidad y diversidad de equipos tecnológicos. La mayoría de las MIPYMES operan con entre 1 y 6 computadoras (84.23%), lo que evidencia un nivel básico de infraestructura digital. Asimismo, un 78.16% de las MIPYMES digitaliza más del 25% de sus procesos y la estabilidad de conexión a internet es adecuada para un servicio gestionado. La estabilidad de conexión es adecuada para soportar un MSS, y se identifican prácticas técnicas favorables como la presencia de firewall activos (68.38%) y un 80.98% declara tener sus antivirus actualizados. Sin embargo, la mayor barrera técnica

identificada es que el 46.01% de las empresas carece de políticas de protección física y respaldo y un 31.88% de las MIPYMES utiliza sus softwares sin licencia legal vigente. Estas debilidades representan riesgos significativos, ya que limitan la capacidad operativa y reflejan la necesidad de acompañar la implementación con procesos de regularización tecnológica y capacitación en buenas prácticas.

B. Gestión de Riesgos Digitales (V2)

La madurez en gestión de riesgos en MIPYME hondureñas es baja y se caracteriza por la ausencia de procesos sistemáticos formales. Solo el 22.11% utiliza herramientas específicas para analizar riesgos. Un 53.21% de las MIPYMES no cuenta con documentación formal de políticas de gestión de riesgos digitales, el 48.33% no realiza de manera formal evaluaciones periódicas de riesgos y 49.10% no ejecuta acciones correctivas o mejoras derivadas de incidentes o evaluaciones de riesgos, estableciendo una clara interconexión entre la ausencia de herramientas de análisis y la falta de procesos documentados y acciones correctivas. En términos prácticos, esta situación refleja que las empresas en esta clasificación operan de manera reactiva, atendiendo incidentes a la medida que ocurren, sin mecanismos previstos ni registros formales que permitan adquirir retroalimentación de experiencias pasadas. Esta variable nos confirma la pertinencia del modelo MMS que incorpore procesos de gestión de riesgos estandarizados y accesibles para empresa de baja madurez digital.

C. Viabilidad Económica (V3)

El escenario económico es favorable para la adopción de una solución gestionada, principalmente por la alta percepción positiva de los representantes del sector (49.10% considera muy beneficiosa la inversión en servicios gestionados y un 32.13% considera que tiene beneficios moderados) y el 83.54% de las MIPYMES ya realiza algún tipo de inversión (desde básica hasta completa) en seguridad informática. Un hallazgo determinante para la pertinencia del modelo es la ceguera financiera ante el riesgo. A pesar de que el 74.55% de los empresarios asocia las fallas de sistema con pérdidas económicas, el 35.99% desconoce el monto exacto del impacto financiero que tendría un ciberataque real en su organización. Esta incapacidad de cuantificación impide el cálculo del Retorno de Inversión (ROI) y deja a la gerencia sin métricas para justificar presupuestos proactivos. Esta brecha de conocimiento valida la inclusión obligatoria de un componente educativo y de métricas de resiliencia (MTL y RTO) en la propuesta de solución gestionada, transformando la percepción de la ciberseguridad de un gasto operativo a una herramienta de protección de activos financieros.

D. Gobernanza y Cultura (V4)

La viabilidad organizacional presenta desafíos significativos en términos de gobernanza formal. El 88.18% de las MIPYMES no implementa factores de gobernanza dispuestos por el estado de Honduras, lo cual refleja una desconexión entre las políticas nacionales, las normas internacionales y la práctica empresarial. Asimismo, un 40.10% no apoya gerencialmente las iniciativas de seguridad informática, sin embargo, el 60% de los encuestados percibe el riesgo de no contar con medidas de seguridad como alto o muy alto, lo cual abre espacio para la sensibilización. Por otra parte, la actitud de los colaboradores hacia la adopción de nuevas tecnologías de seguridad es positiva (67.86%) con un 48.32% que ya realiza capacitaciones en ciberseguridad con alguna frecuencia, sentando bases para una cultura de seguridad. Estos hallazgos sugieren que, aunque la gobernanza formal es débil, existe una base cultural.

E. Pertinencia del modelo MSS (V5)

La pertinencia y la aceptación generalizada es alta (77.64%) para un modelo de ciberseguridad gestionada adaptado a las características de las MIPYMES hondureñas. Para su efectividad, se priorizaron los elementos más críticos (muy importantes) solicitados: soporte técnico 24/7 (85.86%), un plan de recuperación ante desastres (84.31%), la capacidad de integración a sus necesidades (84.07%) y la oferta de modelos flexibles (79.18%) y la actualización automática (62.47%). Con estos datos establecimos las bases técnicas para estructurar una guía de implementación enfocada en la sencillez operativa, adaptabilidad, escalabilidad y la continuidad del negocio.

E. Análisis multivariado e integración total

El análisis demuestra la pertinencia del modelo MSS (aceptación del 77.64%). El éxito de una solución gestionada en ciberseguridad no depende únicamente de la disponibilidad tecnológica, sino del equilibrio dinámico entre capacidades técnicas, disposición organizacional y conciencia del riesgo digital. La Fig. 1 presenta un esquema de relación causal multivariada que sustenta la pertinencia del modelo MSS, evidenciando cómo la interacción entre condiciones tecnológicas, madurez en gestión de riesgos, costos asociados y factores de gobernanza, determinan el nivel de preparación para la adopción de la ciberseguridad en el sector.

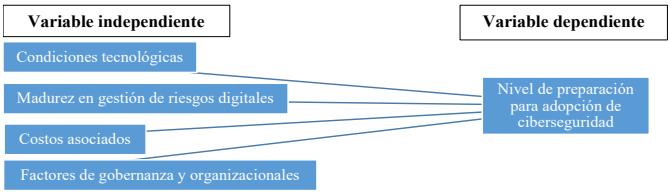

Fig.1. Esquema de relación causal multivariada.

surge precisamente de las debilidades identificadas. Al cruzar las variables, se determinó que:

- V1 x V4 (Riesgo estructural): La falta de apoyo gerencial (40.10%) es la principal barrera para superar la informalidad de gobernanza (88.18%).
- V2 x V3 (Balance de oportunidad): La vulnerabilidad por falta de licencias se mitiga mediante la Actualización

Automática, servicio priorizado como "muy importante" por el 62.47% de las MIPYMES analizadas (por su falta de personal calificado para el desarrollo de tareas relacionadas a la protección cibernética).

- V1 + V2 + V3 + V4 = V5: La solución gestionada actúa como un "entrenador personal", donde la MIPYME externaliza la complejidad técnica (Soporte 24/7, priorizado por el 85.86% de las MIPYMES) para garantizar su supervivencia económica.

IV. PROPUESTA DE MODELO

La propuesta de valor de esta investigación, titulada "Diseño aplicable de una propuesta de modelo de ciberseguridad gestionada para MIPYMES: Una solución práctica en el contexto hondureño", se propone como un modelo pionero de dominio público en el país diseñado y adaptado para MIPYMES hondureñas. Este modelo posee una alta relevancia estratégica al responder a una necesidad urgente del ecosistema empresarial hondureño, ya que no solo busca reducir vulnerabilidades digitales técnicas, sino transformar la ciberseguridad en una práctica organizacional sostenida que garantice la supervivencia económica del negocio, por medio del fortalecimiento de la confianza en el comercio electrónico, la promoción de la formalización tecnológica y la contribución a la competitividad regional, siendo técnicamente viable, financieramente accesible y culturalmente adaptable, considerando las limitaciones específicas del sector.

El modelo propuesto se diseñó atendiendo un análisis estratégico del entorno hondureño. Utilizando la herramienta PESTEL, se identificó que la gobernanza estatal débil y carencia de una ley nacional de ciberseguridad, generan un vacío técnico/legal, y en vista de esto, el modelo busca mitigar ese efecto a través de la formalización de políticas internas desde su fase esencial.

El análisis de las 5 Fuerzas de Porter reveló un alto poder de los proveedores de servicios especializados ante la inexistencia de un CSIRT, CERT o SOC nacional oficial, razón que justifica la externalización de la complejidad técnica a través de un esquema MSS como la vía más viable para asegurar la continuidad operativa sin colapsar los recursos limitados del sector.

La matriz FODA permitió balancear la debilidad de la ¨baja cultura digital¨ con una oportunidad estratégica detectada en la ¨actitud positiva de los colaboradores hacia la ciberseguridad¨ (67.86%), orientando la estructura de la fase 1 del modelo hacia la gestión del cambio y la sensibilización como pilares fundamentales para garantizar la adopción y sostenibilidad a largo plazo.

A continuación, se profundiza en los componentes críticos, fases y mecanismos de control que integran esta solución:

A. Fundamentación y filosofía del modelo

El modelo se fundamenta en un equilibrio dinámico entre capacidades técnicas y disposición organizacional, utilizando como base los pilares del NIST CSF 2.0, CIS Controls IG1, ISO 27001 e ISO 22301. Su implementación sigue la estrategia de la gestión del cambio positivo, para asegurar que la gerencia y los colaboradores adopten la seguridad como un valor propio.

Este modelo combina múltiples disciplinas con una integración que permite que el modelo sea replicable, escalable y compatible con estándares internacionales de gestión de riesgos, gestión de proyectos e ingeniería.

La arquitectura del modelo propuesto posee una alta validez externa al presentar una correspondencia estructural con estudios piloto exitosos realizados en América Latina. En experiencias similares documentadas en Colombia, la aplicación de un esquema escalonado basado en los pilares del NIST CSF permitió mejorar la madurez digital de las empresas del 28% al 74% en un periodo de solo seis meses [16]. Por su parte, los modelos implementados en Panamá confirman que la externalización de la complejidad técnica a través de diagnósticos personalizados y ciberhigiene gestionada reduce significativamente el riesgo operativo sin generar una sobrecarga financiera para el empresario [17]. Esta alineación regional garantiza que las fases de este modelo sean no solo replicables en Honduras, sino también compatibles con el avance global de la ciberseguridad para organizaciones con recursos limitados al combinar pertinencia local con escalabilidad internacional.

El modelo dimensiona a nivel organizacional, cultural y educativo el reconocimiento de que la ciberseguridad no es solo un tópico técnico, sino un proceso de cambios organizacionales que amplía el campo de estudio en factores humanos y sociales, lo cual es poco explorado en nuestra región actualmente por diversas razones.

C. Enfoque de segmentación y alcance

A diferencia de los servicios de ciberseguridad tradicionales que resultan costosos o complejos para el sector, el modelo propuesto evita un enfoque genérico al priorizar las necesidades de los segmentos mayoritarios identificados en el diagnóstico. La aplicabilidad se centra en las microempresas (1 a 9 empleados) y pequeñas empresas (10 a 49 empleados), que representan el 68.12% y el 27.25% de la muestra respectivamente, sectores que enfrentan las mayores barreras financieras y de personal especializado en el país.

Sectorialmente, la solución presenta una mayor sinergia con los rubros de: servicios profesionales (27.5%), comercio (18.51%) y hostelería (15.17%), los cuales muestran una alta exposición al comercio digital, pero mantienen una brecha crítica de gobernanza estatal (88.18% de incumplimiento). Por esta razón, el modelo impone de manera obligatoria un componente de diagnóstico inicial y reporte sistemático adaptado a la baja madurez técnica de estos rubros, permitiendo una transición fluida hacia la formalización tecnológica en las zonas centro y norte de Honduras.

B. Ciclo de vida y ruta de madurez digital (5 fases)

La implementación del modelo MSS se desglosa en un ciclo ágil de 9.5 meses, permitiendo una adopción gradual compatible con los recursos limitados de las MIPYMES y

facilitando su inserción al proceso desde cualquier nivel de madurez. Este flujo de trabajo dinámico, que integra los principios de 'descongelar, cambiar y recongelar' de Lewin, se ilustra en la Fig. 2, donde se observan las cinco fases críticas desde la planificación hasta la optimización de la resiliencia operativa.:

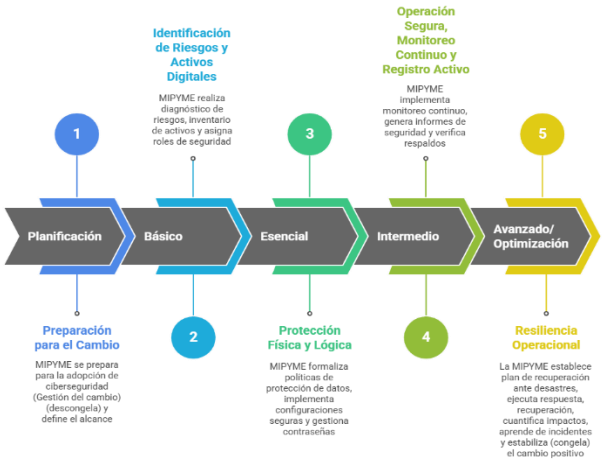

Fig.2. Fases de implementación del modelo propuesto de ciberseguridad para MIPYMES hondureñas.

Fase 1: Planificación (Meses 1-3). Se enfoca en el compromiso gerencial y la definición del alcance. Es vital para superar la brecha de apatía gerencial (40.10% de falta de apoyo) identificada en el diagnóstico. El entregable principal es el Acta de Constitución del Proyecto y el inicio del programa de capacitación básica.

Fase 2: Nivel básico (Meses 4-6). Su objetivo es la Identificación de Riesgos y Activos. Se desarrolla la Matriz de Inventario de Activos Digitales para documentar hardware y software, abordando la debilidad crítica detectada: el 31.88% de las empresas carece de licencias legales. También se formaliza la gobernanza mediante la Matriz RACI.

Fase 3: Nivel esencial (Meses 5-8). Implementación de la Ciberhigiene Crítica. Se formaliza el Documento de Políticas de Protección de Datos y Respaldos, atacando la brecha donde el 46.01% de las MIPYMES opera sin políticas de respaldo. Incluye configuraciones seguras (hardening) y actualización automática de software.

Fase 4: Nivel intermedio (Meses 6.5-9.5). Activación del Monitoreo Continuo y Soporte 24/7. Se generan registros de eventos (logs) y reportes mensuales de desempeño, servicio priorizado como "muy importante" por el 85.86% de las MIPYMES.

Fase 5: Nivel avanzado/optimización (Meses 6.5-9.5). Consolidación de la resiliencia operacional. Se establece el Plan de Recuperación ante Desastres (DRP) y se formaliza la cuantificación del riesgo financiero, permitiendo que la empresa gestione sus incidentes basándose en el aprendizaje continuo.

D. Parámetros de continuidad (Métricas ISO 22301)

Para garantizar que el modelo no sea solo reactivo, se integran indicadores de clase mundial adaptados a la realidad hondureña:

- RTO (Recovery Time Objective): El modelo exige un tiempo máximo de recuperación de 8 horas para servicios esenciales tras un incidente.
- MTL (Maximum Tolerable Loss): Define que el impacto de un ataque no debe exceder el 10% de los ingresos mensuales de la MIPYME.
- MPO (Maximum Tolerable Period of Disruption): Asegura que ninguna interrupción operativa exceda las 48 horas, evitando pérdidas irreversibles.

E. Gestión del factor humano y gobernanza

Según el más reciente Verizon Data Breach Investigations Report (DBIR) 2025, el 60% de las brechas analizadas a nivel global involucran directamente el elemento humano, reafirmando que este sigue siendo el vector crítico de vulnerabilidad en cualquier arquitectura de seguridad sea por errores, ingeniería social o mal uso [18], el desarrollo de una cultura de seguridad deja de ser opcional para convertirse en el eje del modelo. La forma adecuada de abordaje es por medio de planes estructurados que tengan tanto un fin como una ruta clara, con motivos y logros secuenciales que auto validen su ejecución, y que se auto justifiquen conectando directamente los costos con los beneficios de manera efectiva, para eliminar la percepción de que la ciberseguridad es un gasto.

El componente educativo presentado aprovecha la actitud positiva detectada en los colaboradores hacia la adopción de nuevas tecnologías. La propuesta formaliza la gobernanza mediante la asignación de roles técnicos claros (Matriz RACI), transformando la seguridad de una tarea aislada a una responsabilidad compartida y jerarquizada según el nivel de ejecución, tal como se detalla en la ruta de madurez digital presentada en la Fig. 3.

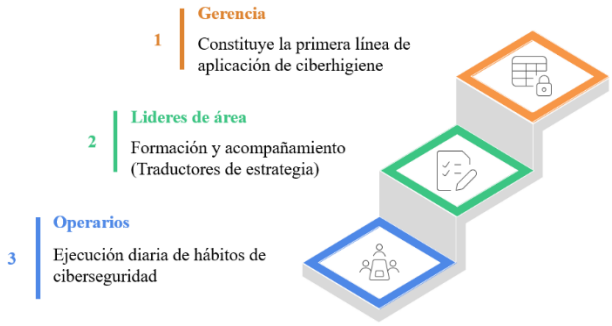

Fig.3. Ruta de madurez digital.

F. Esquema económico y sostenibilidad financiera

La solución está diseñada para ser financieramente accesible, con una inversión total estimada de L. 60,000 (L. 12,000 por fase) que cubre el ciclo completo de implementación, incluyendo capacitación, herramientas básicas, monitoreo y asesoría. Este monto fue validado mediante análisis comparativo con soluciones regionales en

Panamá y Colombia, y se considera accesible para MIPYMES con ingresos mensuales superiores a L. 100,000.

Como modelos de pago, se proponen esquemas de suscripción mensual flexibles (entre US100yUS 1,500) según el tamaño y madurez de la empresa.

Finalmente, el modelo utiliza la Ficha de Cuantificación de Impacto para demostrar el ahorro financiero al reducir el tiempo de inactividad, ayudando al 35.99% de los empresarios que actualmente no saben medir sus pérdidas potenciales ante ataques.

G. Mecanismos de control y mejora continua

El modelo incluye un repositorio de formatos estandarizados alineados a la Guía del PMBOK (Sexta Edición):

- Diagnóstico de Ciberhigiene Inicial: Basado en CIS Controls IG1 para identificar brechas desde el día uno.
- Checklist de Hardening: Para verificar la seguridad física y lógica de los equipos.
- Registro Post-Incidente: Herramienta para analizar causas raíz y estabilizar el "cambio positivo" mediante lecciones aprendidas.

Este diseño integral permite a las MIPYMES externalizar la complejidad técnica (Soporte 24/7 y SOC) mientras mantienen el control de su negocio, convirtiendo la ciberseguridad en un habilitador de confianza para el comercio digital futuro en Honduras.

V. CONCLUSIONES Y RECOMENDACIONES

La investigación revela una contradicción crítica en el ecosistema hondureño: mientras que una cantidad considerable de MIPYMES ha digitalizado más de una cuarta parte de sus procesos y cuenta con conectividad estable, esta base tecnológica carece de un "cerebro" administrativo. Al operar sin políticas documentadas, la infraestructura actual no es un activo de competitividad, sino una superficie de ataque desprotegida que genera un riesgo residual inmanejable para el dueño del negocio.

El alto nivel de aceptación del modelo propuesto no debe interpretarse únicamente como una preferencia comercial, sino como una respuesta a la incapacidad operativa interna.

Se concluye que, en este punto del tiempo, la externalización mediante un MSS es la vía más eficiente para fortalecer la resiliencia operativa y la confianza en el ecosistema digital hondureño.

El análisis cualitativo y cuantitativo confirma que la ciberseguridad en Honduras no es un problema de "software", sino un desafío de gestión del cambio organizacional que requiere "descongelar" la cultura apática actual.

Ante la ausencia de un marco legal integral y la falta de un equipo oficial de respuesta a incidentes en Honduras, se recomienda la creación de un CERT nacional que dicte políticas de cumplimiento para el sector privado y eventualmente un SOC. Mientras esto ocurre, las MIPYMES deben adoptar una Matriz RACI para formalizar roles internos, asegurando que la seguridad no sea una tarea aislada, sino una responsabilidad compartida con el proveedor de servicios gestionados.

En nuestro país, además de no existir un plan de ciberseguridad formalmente socializado y de acceso general, tampoco se ha definido un ente académico que evalúe y norme la calidad de los conocimientos de ciberseguridad, por lo que es necesario que se realice un estudio amplio de los componentes que deben conformar dicha información, para formar un esquema de capacitación formal, incremental, y con los términos pedagógicos adecuados para el aprendizaje del público en general y las MIPYMES hondureñas.

Es imperativo que las empresas dejen de medir la seguridad en términos de "ataques evitados" y comiencen a medirla en "capacidad de recuperación". Se recomienda la implementación sistemática del Plan de Recuperación ante Desastres (DRP) detallado en esta propuesta, utilizando la Ficha de Cuantificación de Impacto para que la gerencia pueda visualizar el ahorro financiero obtenido al reducir el tiempo de inactividad operativa.

Se recomienda establecer alianzas entre el estado, cámaras de comercio y entes como INFOP o CNBS para desarrollar un programa de certificación en ciberhigiene para usuarios no técnicos. Dado que más del 50% de las empresas nunca ha capacitado a su personal, la capacitación debe dejar de ser eventual para convertirse en un requisito de ingreso y permanencia, apalancando la actitud positiva de los empleados identificada en el estudio.

Para las empresas que presentan alta sensibilidad al costo, se recomienda iniciar con la Fase 1 (Planificación) y Fase 2 (Básico) del modelo propuesto, lo que permite estabilizar la gobernanza y el inventario de activos con una inversión mínima por etapa. Esto garantiza victorias rápidas que motiven el apoyo gerencial necesario para escalar hacia el monitoreo 24/7 y la optimización de la resiliencia operativa.

Finalmente, se debe considerar que, al ser el primer modelo de su clase en Honduras, su eficacia plena requiere de validación empírica mediante estudios longitudinales a largo plazo para medir el impacto real en la resiliencia empresarial.

AGRADECIMIENTO/RECONOCIMIENTO

A la Facultad de Postgrado de UNITEC por el apoyo académico. A los asesores Mario Lagos y Oscar Sady Orellana por su guía incondicional. A CSIRT Honduras por facilitar su experiencia de la realidad nacional.

REFERENCIAS

[1] A. Petrosyan, «Cybercrime worldwide - statistics & facts», Statista. Accedido: 20 de agosto de 2025. [En línea]. Disponible en: https://www.statista.com/topics/13546/cybercrime-worldwide/

[2] E. M. Rodezno, L. E. Santos, y J. E. Delcid, «Informe de la MIPYME en Honduras 2024: Talento, innovación y rendimiento», ResearchGate. Accedido: 20 de agosto de 2025. [En línea]. Disponible en: https://www.researchgate.net/publication/393185061_Talento_innovacion_y_rendimiento

[3] International Telecommunication Union, *ITU-T X.1205*. 2008.
[4] Banco Interamericano de Desarrollo y Organización de los Estados Americanos, «2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean», *IDB Publ.*, jul. 2020, doi: 10.18235/0002513.
[5] e-Governance Academy Foundation, «NCSI :: Honduras», National Ciber Security Index. Accedido: 20 de agosto de 2025. [En línea]. Disponible en: https://ncsi.ega.ee/country/hn/
[6] J. Molina, «Crecen amenazas de ciberataque a empresas hondureñas», La Prensa. Accedido: 28 de septiembre de 2025. [En línea]. Disponible en: https://www.laprensa.hn/economia/honduras-hackers-ataques-crecen-amenazas-empresas-hondurenas-BL26960634
[7] K. Baquedano, «Más de 870,000 empresas están en la informalidad en Honduras», Laprensa. Accedido: 20 de agosto de 2025. [En línea]. Disponible en: https://www.laprensa.hn/honduras/crece-negocios-informales-procesos-engorrosos-falta-incentivos-mipymes-ilegalidad-AC20661724
[8] Congreso Nacional de Honduras, «Código Penal (2019)», Tribunal Superior de Cuentas - Biblioteca Virtual. Accedido: 23 de agosto de 2025. [En línea]. Disponible en: https://www.tsc.gob.hn/biblioteca/index.php/codigos/830-codigo-penal-2019
[9] National Institute of Standards and Technology, «The NIST Cybersecurity Framework (CSF) 2.0», National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 29, feb. 2024. doi: 10.6028/NIST.CSWP.29.
[10] «CIS Controls Version 8», CIS. Accedido: 26 de abril de 2026. [En línea]. Disponible en: https://www.cisecurity.org/controls/v8/
[11] ISO, «ISO/IEC 27001:2022», ISO. Accedido: 24 de agosto de 2025. [En línea]. Disponible en: https://www.iso.org/standard/27001
[12] V. Avinash, «ISO 22301: Clause 3 - Terms and Definitions», ISO Templates and Documents Download. Accedido: 21 de noviembre de 2025. [En línea]. Disponible en: https://iso-docs.com/blogs/iso-22301-standard/iso-22301-clause-3-terms-and-definitions
[13] B. Burnes, «Kurt Lewin and the Planned Approach to Change: A Re-appraisal», *J. Manag. Stud.*, vol. 41, n.º 6, pp. 977-1002, ago. 2004, doi: 10.1111/j.1467-6486.2004.00463.x.
[14] J. P. Kotter, «Leading Change: Why Transformation Efforts Fail», *Harvard Business Review*, 1 de mayo de 1995. Accedido: 27 de abril de 2026. [En línea]. Disponible en: https://hbr.org/1995/05/leading-change-why-transformation-efforts-fail-2
[15] M. E. Porter, *Competitive Strategy: Techniques for Analyzing Industries and Competitors*. New York: Free Press, 1980.
[16] H. A. Robles, «Desarrollo de un modelo de ciberseguridad basado en SCRUM para MiPyMEs del Huila, asegurando su viabilidad y escalabilidad.», dic. 2025, Accedido: 25 de diciembre de 2025. [En línea]. Disponible en: http://repository.unad.edu.co/handle/10596/77829
[17] NUMU GROUP, «Ciberseguridad: Fortalecimiento de la ciberseguridad en PYMES – Análisis de Vulnerabilidad – NUMU Group». Accedido: 25 de diciembre de 2025. [En línea]. Disponible en: https://numu.group/portfolio/ciberseguridad-fortalecimiento-de-la-ciberseguridad-en-pymes-analisis-de-vulnerabilidad/
[18] «2026 Data Breach Investigations Report (DBIR)», Verizon Business. Accedido: 27 de abril de 2026. [En línea]. Disponible en: https://www.verizon.com/business/resources/reports/dbir/