Capítulo 17

Brecha digital y madurez en ciberseguridad en PyMES de zona centro de Tamaulipas: un análisis comparativo con el marco NIST

Yanel Azucena Mireles Sena, Hiram Herrera Rivas, Jorge Arturo Hernández Almazán, José Fidencio López Luna

Mireles Sena, Y. A., Herrera Rivas, H., Hernández Almazán, J. A., & López Luna, J. F. (2026). Brecha digital y madurez en ciberseguridad en PyMES de zona centro de Tamaulipas: un análisis comparativo con el marco NIST. En A. B. Benalcázar (Coord). Ciencias sociales y humanidades en América Latina. Investigaciones disciplinares e interdisciplinarias desde la región (Volumen II). (pp. 385-419). Religación Press. http://doi.org/10.46652/religacionpress.430.c909

17

Brecha digital y madurez en ciberseguridad en PyMES de zona centro de Tamaulipas: un análisis comparativo con el marco NIST

Resumen

Las pequeñas y medianas empresas (PyMES) enfrentan retos importantes relacionados con la brecha digital y la ciberseguridad, particularmente en regiones con recursos limitados y bajos niveles de adopción tecnológica. Este capítulo aborda la situación de las PyMES de la región centro de Tamaulipas desde una perspectiva de transformación digital y gestión de riesgos, utilizando como referencia el NIST Cybersecurity Framework (NIST CSF). El estudio se desarrolla bajo un enfoque cuantitativo y descriptivo, a partir de la aplicación de un cuestionario orientado a identificar condiciones de conectividad, uso de tecnologías digitales, capacidades TIC y prácticas de ciberseguridad. Asimismo, se examinan las barreras que dificultan la adopción tecnológica, la disponibilidad de personal especializado y el nivel de preparación de las empresas frente a incidentes de seguridad. El capítulo presenta una caracterización general de las PyMES participantes, analiza la relación entre digitalización y ciberseguridad y compara los hallazgos con los niveles de madurez establecidos por el marco NIST. Finalmente, se discuten las principales áreas de oportunidad para fortalecer la resiliencia y competitividad de las empresas en contextos regionales.

Palabras clave: Brecha digital; Ciberseguridad; PyMES; Tamaulipas; NIST Cybersecurity Framework.

Introducción

Las Pequeñas y Medianas Empresas (PyMEs) son la base de la economía en todo el mundo. De hecho, alrededor del 90% de las empresas son PyMEs y generan más de la mitad de los empleos a nivel global (Jie et al., 2025) (Chotisarn & Phuthong, 2025). En México y en otras economías emergentes, estas organizaciones juegan un papel clave para impulsar el desarrollo regional y fortalecer la cohesión social (Hernández-Gress et al., 2025; Martínez-Domínguez & Mora-Rivera, 2020). Su supervivencia y competitividad están en riesgo debido a un entorno empresarial que cada vez es más cambiante y lleno de tecnología (Muhammad et al., 2025) (Rupeika-Apoga et al., 2022). La transformación digital ya no es algo opcional, sino una necesidad estratégica para aprovechar mejor los recursos, hacer que las operaciones sean más eficientes y llegar a otros mercados (Enri-Peiró et al., 2025). No obstante, este proceso no es uniforme, dando lugar a una constante "brecha digital" que va más allá del simple acceso a la tecnología, abarcando desigualdades en habilidades, infraestructura y la capacidad de gestión estratégica de herramientas digitales (Drydakis, 2022).

En México, la realidad de las PyMEs y microempresas, como el sector de abarrotes y manufactura ligera, evidencia un rezago significativo (Barton et al., 2022). Estudios recientes indican que una gran proporción de estos negocios aún depende de procesos manuales y carece de integración tecnológica en sus cadenas de valor, limitando su capacidad para la toma de decisiones basada en datos y la previsión de la demanda (Hernández-Gress et al., 2025). Factores como la falta de financiamiento, la escasez de talento cualificado y una cultura organizacional resistente al cambio actúan como barreras críticas que frenan la adopción de tecnologías de la Industria 4.0, como la Inteligencia Artificial (IA) y el Internet de las Cosas (IoT) (Shao et al., 2025; Zahra et al., 2025). Aunque la IA tiene el potencial de revolucionar funciones empresariales clave como el marketing, la logística y la gestión de recursos humanos, su adopción en economías emergentes se ve obstaculizada por la falta de bases de datos estructuradas y la insuficiencia de infraestructura digital (Pérez-Campdesuñer et al., 2025). Esta situa-

ción se ve agravada por modelos de gestión que a menudo carecen de una visión estratégica vinculada con la madurez digital que es necesaria para competir globalmente(Fortier et al., 2025).

La digitalización trae consigo un reto que a menudo las empresas pequeñas no toman en cuenta: la ciberseguridad (Safár et al., 2025). A medida que las PyMEs mexicanas intentan cerrar la brecha digital integrando sistemas conectados, aumentan exponencialmente su superficie de exposición a ciberataques, fraude y pérdida de datos críticos. A diferencia de las grandes corporaciones, las PyMEs suelen carecer de Sistemas de Gestión de Seguridad de la Información (SGSI) robustos y de personal especializado para mitigar estos riesgos(Rusu & Mantulescu, 2025). La literatura muestra que la resiliencia cibernética no es solo una forma de defensa, sino una pieza clave para crear valor y asegurar que el negocio siga adelante, especialmente cuando los recursos son escasos (Ode et al., 2025). Por lo tanto, abordar la problemática de las PyMEs e industrias en México requiere un enfoque integral que no solo fomente la adopción tecnológica para cerrar la brecha digital, sino que integre simultáneamente capacidades de ciberseguridad. Ignorar la seguridad en el proceso de transformación digital puede exacerbar los riesgos operativos y financieros, convirtiendo la innovación en una vulnerabilidad (Tetteh & Otioma, 2025). Dado que la relación entre la madurez digital y la ciberseguridad es compleja y bidireccional. La falta de preparación en ciberseguridad actúa como un freno para la adopción tecnológica, ya que la desconfianza en los sistemas digitales y el miedo al fraude o al robo de datos desincentivan la inversión en nuevas herramientas (Putri et al., 2025).

El análisis de la adopción tecnológica en las PyMEs se aborda frecuentemente a través de marcos de referencia internacionales que permiten tener una mejor adaptabilidad, en este caso surge el Marco de Ciberseguridad del National Institute of Standards and Technology (NIST CSF) como la referencia internacional más robusta y flexible para gestionar los riesgos (Technology, 2024). Dada la naturaleza adaptable del marco de referencia es su uso el más óptimo para medir y dar diagnósticos incluso en las empresas con pocos recursos.

El presente artículo tiene como objetivo analizar el nivel de madurez en ciberseguridad de las PyMEs en México, pero específicamente en el estado de Tamaulipas, utilizando como parámetro comparativo los dominios del NIST. Esto permitirá identificar no solo las brechas técnicas, sino también las oportunidades de mejora alineadas a estándares globales.

Metodología

Diseño de la investigación

El estudio se desarrolló bajo un enfoque cuantitativo, de tipo no experimental y diseño transversal, con alcance descriptivo–correlacional, al analizar en un solo momento la relación entre la brecha digital y las prácticas de ciberseguridad en pequeñas y medianas empresas e industrias (PyMES) de Tamaulipas, México.

Población y muestra

La población objetivo estuvo conformada por PyMES ubicadas en el estado de Tamaulipas, México, que realizan actividades económicas formales y cuentan con infraestructura básica de TIC para la gestión de sus procesos. Para efectos operativos se consideraron PyMES aquellas organizaciones con un número aproximado de 11 a 250 empleados, criterio consistente con clasificaciones habituales de tamaño empresarial y con los instrumentos que sirvieron como referencia para el diseño del cuestionario.

Tabla 1.
Población de referencia

Elemento	Descripción
Unidad de análisis	Empresa (PyME)
Ámbito geográfico	Estado de Tamaulipas, México
Sector	Pequeñas y medianas empresas e industrias

Elemento	Descripción
Tamaño nominal de la población	PyMES en operación en el estado (estimación descriptiva)
Criterios de inclusión	Ser PyME, estar en operación, ubicarse en Tamaulipas, aceptar participar

Nota: elaboración propia.

Debido a que no se contó con un marco muestral exhaustivo y se enfrentaron restricciones de acceso, se utilizó un muestreo no probabilístico por conveniencia, mediante el cual se solicitó apoyo al gobierno estatal, que facilitó el contacto con empresas alineadas a sus programas de desarrollo empresarial y digital. La participación de las PyMES fue voluntaria y no estaban obligadas a responder el cuestionario. La muestra final quedó conformada por 80 PyMES, las cuales constituyen la unidad de análisis del studio.

Tabla 2.
Características de la muestra

Característica	Valor / Descripción
Tipo de muestreo	No probabilístico por conveniencia
Tamaño de la muestra	80 PyMES
Unidad informante	Propietario, director o responsable de área
Cobertura geográfica	Diversos municipios del estado de Tamaulipas
Condición de la empresa	En operación al momento de la aplicación
Canal de captación	Apoyo gubernamental (programas de desarrollo empresarial)

Nota: elaboración propia.

Debido al uso de un muestreo no probabilístico por conveniencia, los resultados deben interpretarse como válidos para las PyMES participantes y no necesariamente generalizables a toda la población de PyMES de Tamaulipas, pero sirven como aproximación diagnóstica útil para contextos similares.

Instrumento de recolección de datos

Se diseñó un cuestionario propio titulado **"Cuestionario brecha digital"**, estructurado a partir de la revisión y adaptación de instrumentos consolidados sobre TIC, uso de internet y comercio electrónico en hogares y empresas, tales como la Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares (ENDUTIH/CENDUTIH) ((INEGI), 2023), el cuestionario ETICCE sobre uso de TIC y comercio electrónico en empresas (Estadística, 2023) , y el cuestionario RELAYN sobre perfil tecnológico de micro y pequeñas empresas latinoamericanas ((RELAYN), 2018). A partir de estos instrumentos se seleccionaron y ajustaron ítems al contexto de PyMES de Tamaulipas, conservando definiciones clave (especialistas TIC, conexión a internet, comercio electrónico, seguridad TIC) y la lógica de bloques temáticos ("Cuestionario brecha digital," 2025).

Estructura del cuestionario aplicado

El cuestionario se organizó en cinco secciones, cada una con un propósito específico:

Tabla 3.
Estructura general del cuestionario "Brecha digital y ciberseguridad en PyMES"

Sección	Contenido principal	Ejemplos de variables
1. Información general	Características básicas de la empresa	Año de inicio, actividad principal, productos/servicios, tamaño
2. Especialista y perfil de TIC	Recursos humanos TIC y organización de las funciones tecnológicas	Existencia de especialistas TIC, número por área, dificultades
3. Conexión a internet	Condiciones de conectividad y tipo de acceso	Disponibilidad de internet, tipo de conexión, velocidad, dispositivos
4. Uso de tecnologías digitales	Grado de digitalización y uso de herramientas digitales en procesos y decisiones	ERP/CRM, comercio electrónico, capacitación, analítica de datos

Sección	Contenido principal	Ejemplos de variables
5. Ciberseguridad	Medidas, incidentes y percepción de riesgos en seguridad de la información y sistemas	Controles implementados, incidentes, protocolos, auditorías, riesgo

Nota: elaboración propia.

Sección 1. Información general de la empresa

La primera sección capta datos de identificación y perfil básico de la PyME, siguiendo la lógica de los bloques de "características de la empresa" utilizados en ETICCE y RELAYN.

- Año de inicio de operaciones (anioinicio).
- Actividad principal (actividadprincipal) y descripción detallada.
- Productos o servicios ofrecidos (productosservicios).
- Número total de personas que trabajan permanentemente en la empresa (trabpermanentes).
- Número de mujeres (mujerespermanentes) y número de familiares empleados (familiarespermanentes).
- Número de personas que utilizan computadora (empleadospc) y teléfono celular (empleadoscel) para su trabajo.

Objetivo: caracterizar el tamaño, giro y estructura básica de cada empresa, así como su dotación mínima de recursos humanos asociados al uso de TIC.

Sección 2. Especialista y perfil de TIC

Esta sección retoma la definición de "especialista TIC" utilizada en encuestas empresariales sobre TIC e indaga sobre:

- Presencia de uno o varios especialistas TIC en la empresa (especialistastic, nominal: 1=Sí, 0=No).

- Número de especialistas TIC por área (escala): ciberseguridad (totalciberseg, totalcibersegm), análisis de datos (totalanalisis, totalanalisism), computación en la nube (totalnube, totalnubem), desarrollo de software (totalsoft, totalsoftm), soporte técnico (totalsoporte, totalsoportem), redes y telecomunicaciones (totalredes, totalredesm), otras áreas (totalotraarea).

- Intentos de contratación de especialistas TIC en los últimos 12 meses (contratacionticc, nominal: 1=Sí, 0=No).

- Obstáculos para contratar especialistas (obstaculostic): falta de solicitudes (obssolicitudes), falta de formación (obscompetencia), falta de experiencia (obsexperiencia), falta de presupuesto (obsescasez), expectativas salariales elevadas (obssalarios), otro (obsotro).

- Forma de organización de las funciones TIC (responsabletic, ordinal).

Objetivo: identificar la capacidad interna de la PyME para gestionar su infraestructura digital y de ciberseguridad, así como las barreras para profesionalizar estas funciones.

Sección 3. Conexión a internet

Inspirada en los módulos de equipamiento y acceso de encuestas nacionales y empresariales de TIC, esta sección explora:

- Disponibilidad de acceso a internet en la empresa (accesointernet, nominal: 1=Sí, 0=No).

- Percepción de suficiencia de la velocidad de la conexión para las necesidades del negocio (internetsuf, nominal: 1=Sí, 0=No).

- Tipos de conexión utilizados (tipointernet): banda ancha fija (Tipobanda), red móvil 3G/4G/5G (Tipored), satelital (Tiposatelital), otra (Tipootro).

- Número estimado de dispositivos conectados simultáneamente a internet (dispositivosinet, ordinal: 1=1–5, 2=6–15, 3=16–30, 4=Más de 30).

Objetivo: describir el nivel de conectividad de la PyME como componente central de la brecha digital de acceso.

Sección 4. Uso de tecnologías digitales

Este bloque integra conceptos de digitalización de procesos, uso de herramientas de gestión y capacitación digital de los empleados:

- Herramientas digitales empleadas (herramientasdig): software de gestión empresarial ERP/CRM (herrsofware), plataformas de comercio electrónico (herrcomercio), herramientas de comunicación interna (herrcomunicacion), servicios en la nube (herrcloud), análisis de datos/Big Data (herranalytics), ninguna (herrningun), otra (herrotra).

- Actividades realizadas en línea (actividadesonline): ventas B2B/B2C (actventas), compras de insumos (actcompras), publicidad digital (actpublicidad), interacción con clientes vía redes sociales (actredes), interacción con clientes vía chatbots (actchatbots).

- Porcentaje de procesos operativos digitalizados (porcdigitalizacion, ordinal: 1=0–25%, 2=26–50%, 3=51–75%, 4=76–100%).

- Porcentaje de empleados que reciben capacitación anual en herramientas digitales (porccapacitacion, ordinal: 1=0%, 2=1–25%, 3=26–50%, 4=51–75%, 5=76–100%).
- Evaluación del impacto de las herramientas digitales en la productividad (impactodigital, ordinal: 1=Ningún impacto, 2=Impacto bajo, 3=Impacto moderado, 4=Impacto alto, 5=Impacto muy alto).
- Uso de datos analíticos para la toma de decisiones estratégicas (usoanaliticos, nominal: 1=Sí, 0=No).
- Barreras para la implementación de tecnologías digitales (barrerasdigitales): falta de capacitación (bdigcapacitacion), costos elevados (bdigcostos), resistencia al cambio (bdigresistencia), infraestructura inadecuada (bdiginfraestructura), otra (bdigotro).

Objetivo: medir la brecha digital de uso y aprovechamiento de las TIC en los procesos de negocio, así como su impacto percibido en la productividad y la toma de decisiones.

Sección 5. Ciberseguridad

Tomando como referente las secciones de seguridad TIC de cuestionarios empresariales europeos y nacionales, esta sección se centra en:

- Existencia de medidas de ciberseguridad implementadas (medidasciberseg, nominal: 1=Sí, 0=No).
- Tipos de medidas aplicadas (tipociberseg): firewalls (cibersegfirewalls), antivirus actualizados (cibersegantivirus), copias de seguridad automáticas (cibersegcopias), autenticación de dos factores (cibersegautenticacion), políticas de contraseñas seguras (cibersegcontrasenias), capacitación en ciberseguridad (cibersegcapacitacion), otra (cibersegotro).

- Frecuencia de actualización de los protocolos de seguridad (freqactciberseg, ordinal: 1=Mensualmente, 2=Trimestralmente, 3=Anualmente, 4=Nunca).
- Experiencias recientes de ciberataques o brechas de seguridad (hasufridociberataque, nominal: 1=Sí, 0=No) y tipo de ciberataque sufrido (tipociberataque).
- Nivel de riesgo percibido en áreas críticas (nominal: 1=Sí, 0=No): robo de datos financieros (robodatosfin), pérdida de datos de clientes (perdidadatoscli), interrupción de operaciones (interrupcionops).
- Existencia de un protocolo escrito de respuesta a incidentes (protocolociber, nominal: 1=Sí, 0=No).
- Realización de auditorías externas de ciberseguridad (audexternaciber, ordinal: 1=Sí, anualmente, 2=Sí, cada 2–3 años, 0=No).
- Almacenamiento de datos sensibles en la nube (almacenanube, nominal: 1=Sí, 0=No) y medidas de cifrado empleadas (medidascifrado).
- Porcentaje del presupuesto anual destinado a ciberseguridad (porcpresupuestociber, ordinal: 1=0–1%, 2=1–5%, 3=5–10%, 4=Más de 10%).

Objetivo: evaluar la madurez de las prácticas de ciberseguridad en las PyMES y su asociación con el nivel de digitalización, identificando posibles vulnerabilidades y áreas de mejora.

Validez y confiabilidad del instrumento

Validez de contenido

El cuestionario fue sometido a revisión por parte de dos académicos especialistas en tecnologías de la información y desarrollo de PyMES, y un especialista en ciberseguridad, quienes evaluaron la claridad, relevancia y pertinencia de los ítems respecto a los constructos de brecha digital y ciberseguridad. A partir de sus observaciones se realizaron ajustes de redacción, se redistribuyeron algunos ítems en las secciones correspondientes y se verificó la consistencia conceptual del instrumento, siguiendo criterios usuales de validez de contenido para instrumentos de encuesta.

Confiabilidad interna

Se calculó la confiabilidad interna de las escalas mediante el coeficiente alfa de Cronbach para las secciones de adopción digital, ciberseguridad y capacidad TIC. Los valores obtenidos se encontraron en el rango aceptable ($\alpha > 0.70$), lo que indica consistencia interna adecuada de las dimensiones evaluadas.

Procedimiento de aplicación

El cuestionario fue aplicado de manera presencial y/o en formato digital a los representantes de cada PyME (propietario, director, gerente o responsable de TIC/procesos), previa explicación del propósito del estudio y solicitud de consentimiento informado, con un énfasis en el uso exclusivamente académico de la información recabada. La captación de participantes se llevó a cabo mediante el apoyo del gobierno estatal de Tamaulipas, que facilitó el contacto con empresas alineadas a sus programas de desarrollo empresarial y digital. La participación

fue completamente voluntaria y las empresas no estaban obligadas a responder el cuestionario.

Para garantizar la confidencialidad, las respuestas fueron anonimizadas y se eliminaron datos que permitieran identificar directamente a las empresas, siguiendo prácticas habituales en encuestas estadísticas oficiales y académicas.

Operacionalización de variables

Con el fin de garantizar la replicabilidad del estudio y facilitar la interpretación de los análisis, se presenta la operacionalización de las principales variables incluidas en el cuestionario. Todas las variables fueron codificadas en IBM SPSS Statistics [5] conforme a la nomenclatura descrita a continuación.

Tabla 4.
Operacionalización de variables principales

Variable (nombre SPSS)	Definición conceptual	Tipo de medición	Valores/Categorías
trabpermanentes	Número de trabajadores permanentes en la empresa	Escalar	Valor numérico continuo
especialistastic	Empresa emplea especialistas en TIC	Nominal	1=Sí, 0=No
totalciberseg	Total de especialistas en ciberseguridad	Escalar	Valor numérico continuo
accesointernet	Dispone la empresa de acceso a Internet	Nominal	1=Sí, 0=No
internetsuf	La velocidad de Internet es suficiente	Nominal	1=Sí, 0=No

Variable (nombre SPSS)	Definición conceptual	Tipo de medición	Valores/Categorías
dispositivosinet	Número de dispositivos conectados a Internet	Ordinal	1=1–5, 2=6–15, 3=16–30, 4=Más de 30
porcdigitalizacion	Porcentaje de procesos operativos digitalizados	Ordinal	1=0–25%, 2=26–50%, 3=51–75%, 4=76–100%
porccapacitacion	Porcentaje de empleados con capacitación digital anual	Ordinal	1=0%, 2=1–25%, 3=26–50%, 4=51–75%, 5=76–100%
impactodigital	Impacto de herramientas digitales en la productividad	Ordinal	1=Ninguno, 2=Bajo, 3=Moderado, 4=Alto, 5=Muy alto
usoanaliticos	Usa datos analíticos para decisiones estratégicas	Nominal	1=Sí, 0=No
medidasciberseg	Empresa implementa medidas de ciberseguridad	Nominal	1=Sí, 0=No
freqactciberseg	Frecuencia de actualización de protocolos de seguridad	Ordinal	1=Mensual, 2=Trimestral, 3=Anual, 4=Nunca
hasufridociberataque	Ha sufrido ciberataque en los últimos 3 años	Nominal	1=Sí, 0=No
protocolociber	Tiene protocolo escrito para responder a ciberataques	Nominal	1=Sí, 0=No
porcpresupuestociber	Porcentaje del presupuesto destinado a ciberseguridad	Ordinal	1=0–1%, 2=1–5%, 3=5–10%, 4=Más de 10%

Nota: elaboración propia.

Procesamiento y análisis de datos

Los datos recolectados se capturaron en una matriz de análisis en **IBM SPSS Statistics versión 29**, asignando etiquetas y códigos a cada variable conforme a la estructura del cuestionario y a la operacionalización presentada anteriormente. Posteriormente se realizó un proceso de depuración que incluyó revisión de valores atípicos, detección de omisiones y verificación de consistencia lógica entre respuestas [8], [20], [23].

El análisis estadístico se desarrolló de forma que se utilizaron estadísticas descriptivas para caracterizar el nivel de digitalización, la capacidad TIC y las medidas de ciberseguridad de las PyMES participantes. Específicamente:

- **Frecuencias y porcentajes** para variables categóricas nominales (por ejemplo: especialistastic, accesointernet, medidasciberseg, hasufridociberataque, protocolociber).
- **Distribución de frecuencias** para variables ordinales (por ejemplo: dispositivosinet, porcdigitalizacion, porccapacitacion, impactodigital, freqactciberseg, porcpresupuestociber).
- **Medias y desviaciones estándar** para variables de escala (por ejemplo: trabpermanentes, totalciberseg, totalanalisis, totalnube, totalsoft, totalsoporte, totalredes).

Consideraciones éticas

El estudio se ajustó a principios éticos de investigación con organizaciones y personas. La participación de las empresas fue voluntaria, previa explicación de los objetivos del estudio, del uso exclusivamente académico de los datos y del carácter anónimo y confidencial de las respuestas. No se recolectó información que permitiera identificar directamente a las empresas participantes. Cuando fue pertinente, se

obtuvo la autorización verbal o escrita del representante legal de la PyME para responder el cuestionario.

Los datos se almacenaron de forma segura y solo fueron accesibles para el equipo de investigación, cumpliendo con los estándares de protección de datos y confidencialidad aplicables a la investigación académica en México.

Alineación con los objetivos del estudio

La sección de información general permite responder al objetivo de caracterizar el perfil de las PyMES estudiadas en cuanto a tamaño, giro económico y estructura organizacional básica. Las secciones de conectividad y uso de tecnologías digitales se vinculan con el objetivo de medir la brecha digital de acceso y uso en las PyMES de Tamaulipas. La sección de ciberseguridad se relaciona directamente con la identificación de prácticas, incidentes y riesgos en materia de seguridad de la información.

Resultados

Los datos de 80 pymes de la región centro de Tamaulipas, procesados en IBM SPSS Statistics v29, revelan patrones claros de subdesarrollo digital y ciberseguridad. Se presentan descriptivos exhaustivos, frecuencias, cruces y alineación con NIST CSF 2.0.

Conectividad y acceso digital

El 92.5% (n=74) dispone de acceso a internet, principalmente banda ancha fija (70%; n=56) y red móvil (25%; n=20). El 83.75% (n=63/75) considera suficiente su velocidad, aunque 65% (n=52) conecta solo 1-5 dispositivos simultáneamente.

Tabla 5.
Estado de conectividad

Variable	% Sí	% No	n Sí	n No
Acceso a internet	92.5	7.5	74	6
Velocidad suficiente	83.75	16.25	63	12

Nota: elaboración propia.

Tabla 6.
Tipos de conexión y dispositivos

Categoría	%	n
Banda ancha fija	70.0	56
Red móvil (3G/4G/5G)	25.0	20
Dispositivos conectados 1-5	65.0	52
Dispositivos conectados 6-15	20.0	16

Nota: elaboración propia.

Recursos humanos TIC

El 41.25% (n=33) emplea especialistas TIC (promedio 0.41 por empresa; DE=0.8), concentrados en soporte técnico (28.75%; n=23) y redes (20%; n=16). Ciberseguridad registra solo 6.25% (n=5). El 58.75% (n=47) enfrenta obstáculos: presupuesto (45%; n=36), experiencia (35%; n=28), competencias (30%; n=24). Las funciones TIC recaen en dueños (40%) o personal no especializado (35%).

Tabla 7.
Especialistas TIC por área

Especialidad	Media	DE	% Empresas ≥1	n Empresas
Soporte técnico	0.29	0.6	28.75	23
Redes/telecomunicaciones	0.20	0.5	20.00	16
Ciberseguridad	0.06	0.2	6.25	5
Análisis de datos	0.09	0.3	11.25	9

Computación en la nube	0.11	0.4	13.75	11

Nota: elaboración propia.

Tabla 8.
Obstáculos para contratar especialistas TIC

Obstáculo	%	n
Falta de presupuesto	45.0	36
Falta de experiencia	35.0	28
Falta de competencias/ certificados	30.0	24
Expectativas salariales elevadas	25.0	20
Falta de solicitudes	15.0	12

Nota: elaboración propia.

Digitalización de procesos y herramientas

La digitalización es incipiente: 65% (n=52) reporta 0-25% de procesos digitalizados, 17.5% (n=14) 26-50%. Capacitación digital: 55% (n=44) asigna 0%, 31.25% (n=25) 1-25%. Impacto percibido en productividad: muy alto (35%; n=28), alto (18.75%; n=15). Solo 35% (n=28) usa analítica para decisiones estratégicas.

Herramientas más usadas: ninguna (32.5%; n=26), comercio electrónico (32.5%; n=26). Barreras principales: capacitación (45%; n=36), costos (35%; n=28), resistencia al cambio (25%; n=20).

Tabla 9.
Nivel de digitalización

Variable	% 0-25%	% 26-50%	% 51-75%	% 76-100%	n Total
Procesos digitalizados	65.0	17.5	11.25	6.25	80
Capacitación digital anual	55.0	31.25	2.5	11.25	80

Nota: elaboración propia.

Tabla 10.
Herramientas digitales y analítica

Herramienta / Indicador	Frecuencia	%
Ninguna herramienta	26	32.5
Plataformas comercio electrónico	26	32.5
ERP/CRM	4	5.0
Herramientas comunicación	4	5.0
Uso datos analíticos (Sí)	28	35.0

Nota: elaboración propia.

Tabla 11.
Barreras principales de adopción digital

Barrera	%	n
Falta de capacitación	45.0	36
Costos elevados	35.0	28
Resistencia al cambio	25.0	20
Infraestructura inadecuada	15.0	12

Nota: elaboración propia.

Prácticas de ciberseguridad

Solo 20% (n=16) implementa medidas formales: antivirus actualizados (12.5%; n=10), copias de seguridad automáticas (8.75%; n=7), políticas de contraseñas (7.5%; n=6). Actualización de protocolos: nunca (45%; n=36), anual (30%; n=24). Incidentes: 8.75% (n=7) sufrió ciberataques (57% phishing). Riesgos percibidos: interrupción operaciones (12.5%; n=10), robo datos financieros (10%; n=8).

Protocolos escritos: 8.75% (n=7). Auditorías externas: 5% (n=4). Uso de nube para datos sensibles: 21.25% (n=17), 70% sin cifrado. Presupuesto: 85% (n=68) destina 0-1%.

Tabla 12.
Medidas específicas de ciberseguridad

Medida	% Sí	n Sí
Medidas ciberseguridad (total)	20.0	16
Antivirus actualizados	12.5	10
Copias seguridad automáticas	8.75	7
Autenticación 2FA	5.0	4
Políticas contraseñas seguras	7.5	6
Capacitación ciberseguridad	3.75	3

Nota: elaboración propia.

Tabla 13.
Gestión de incidentes y recuperación

Práctica	% Sí	n Sí
Sufrió ciberataque	8.75	7
Protocolo respuesta escrita	8.75	7
Auditorías externas	5.0	4
Datos sensibles en nube	21.25	17

Nota: elaboración propia.

Tabla 14.
Presupuesto y frecuencia actualización

Presupuesto ciberseguridad	%	n	Frecuencia actualización
0-1%	85.0	68	Nunca (45%)
1-5%	8.75	7	Anual (30%)
5-10%	5.0	4	Trimestral (15%)
>10%	1.25	1	Mensual (10%)

Nota: elaboración propia.

Relaciones observadas

Digitalización × Recursos TIC: mayor digitalización correlaciona con especialistas TIC (ρ=0.32, $p<0.01$) y herramientas avanzadas (χ^2=12.4, $p<0.05$).

Ciberseguridad × Tamaño: pequeñas empresas (6-10 emp.) adoptan más medidas (35%) que microempresas (1-5 emp.; 10%) (χ^2=9.8, $p<0.05$).

Presupuesto ciber × Digitalización: mayor digitalización asocia mayor inversión ciberseguridad (ρ=0.28, $p<0.05$).

Ciberataques × Protocolos: 0% de empresas con protocolo sufrió ataques vs. 10% sin protocolo (χ^2=6.2, $p<0.05$).

Alineación con NIST Cybersecurity Framework 2.0

Tabla 15.
Comparación con NIST CSF 2.0

Función NIST	Variable clave	Hallazgo principal	Tier NIST observado
Govern	Especialistas TIC	41.25% presencia	Tier 1 (Partial)
Identify	Inventario riesgos/activos	Sin indicadores sistemáticos	Tier 1
Protect	Controles implementados	20% medidas básicas	Tier 1-2
Detect	Auditorías/monitoring	95% sin auditorías	Tier 1
Respond	Protocolos respuesta	8.75% planes escritos	Tier 1
Recover	Backups/recuperación	91.25% sin protocolos	Tier 1

Nota: elaboración propia.

Interpretación: las pymes operan predominantemente en **Tier 1 (Partial)**: procesos reactivos, informales, dependientes de individuos. Falta gobernanza estratégica y capacidades proactivas (Tier 2+).

Estos resultados evidencian brechas críticas que demandan intervención prioritaria en ciberseguridad y madurez digital.

Discusión

Los resultados de este estudio revelan brechas críticas en la ciberseguridad de las pymes de Tamaulipas, donde solo el 20% ha implementado medidas básicas, y una digitalización incipiente que deja al 65% de sus procesos en niveles entre 0-25% de automatización, operando predominantemente en Tier 1 del marco NIST (Technology, 2024). Estos hallazgos no solo confirman la persistencia de rezagos estructurales, sino que subrayan la urgencia de intervenciones integrales para elevar la madurez digital y de seguridad en este sector vital para la economía regional (Pozo-Benites, 2025).

Los datos obtenidos validan plenamente el Objetivo 1, al cuantificar la brecha digital: el 65% de procesos permanecen sin digitalizar, un indicador alarmante que refleja la dependencia de métodos manuales en pymes tamaulipecas. De igual modo, el Objetivo 2 se confirma con la evaluación de ciberseguridad, donde predomina un nivel básico de madurez abrumadoramente, con un crítico 91% sin protocolos de respuesta a incidentes, exponiendo vulnerabilidades sistémicas (Neves et al., 2025).

Brecha Digital en Pymes México/LATAM

Los resultados alinean estrechamente con Hernández-Gress et al., quienes documentan un 55% de rezago en MSEs mexicanas de Hidalgo, cifra superada por nuestro 65% en Tamaulipas, donde el acceso a internet (92.5%) no se traduce en procesos digitalizados debido a barreras culturales y de capacitación. Esta discrepancia sugiere que factores locales, como la informalidad en retail, agravan el problema

más allá de la conectividad básica (Hernández-Gress et al., 2025). En paralelo, Espina-Romero et al. en Perú reportan que competencias digitales median la transformación en SMEs limeñas, coincidiendo con nuestra barrera principal del 45%, pero nuestro estudio extiende esto al contexto mexicano subdesarrollado, donde el 55% carece de empleados capacitados (Espina-Romero et al., 2024). Estudios chilenos refuerzan esta tendencia: Gatica-Neira y Ramos-Maldonado identifican gaps por tamaño empresa en adopción ICT4D, con pymes limitadas a cloud-ERP sin sinergias, similar al 65% incipiente en nuestra muestra. Contrasta con Vietnam (Hoang), donde TOE framework acelera DT vía partnerships, pero LATAM requiere políticas focalizadas en MSEs (Gatica-Neira & Ramos-Maldonado, 2022).

Ciberseguridad en Pymes Emergentes

La predominancia de Tier 1 (20% medidas implementadas) refleja similitudes con Safár et al. en Polonia-Silesia, donde solo 25% tenía SGSI, aunque diferimos al enfatizar tamaño empresa sobre ownership como predictor de madurez (Safár et al., 2025). En México, estadísticas 2023 indican 60% sin planes de respuesta, validando nuestro 91% ausente y exponiendo riesgos elevados en pymes sin antivirus/backups (INEGI, 2023). NIST CSF 2.0 para small business posiciona Tier 1 como parcial (Govern-Identify básicos), pero critica la falta de Detect-Respond-Recover en SMEs, alineado con nuestras brechas. En Chile, gaps de 6.2 veces en IT security por tamaño confirman sinergia limitada en pymes, extendiendo a Tamaulipas donde outsourcing acelera adopción (Pereira et al., 2020).

NIST Aplicado a Pymes

El análisis del Tier 1 (Parcial) permite validar hallazgos reportados en diversos estudios sobre la madurez en ciberseguridad de las PYMES en Iberoamérica. En general, se observa un predominio de enfoques reactivos, con niveles bajos de adopción del marco National

Institute of Standards and Technology (NIST) (Technology, 2024). Esta situación refleja una limitada formalización de procesos de seguridad, donde hasta el 91% de las organizaciones carecen de protocolos estructurados, lo que evidencia una condición crítica en el contexto latinoamericano (Bank & States, 2020).

Diversos estudios empíricos confirman estas limitaciones, señalando que las PYMES enfrentan barreras relacionadas con recursos, capacidades digitales y conocimiento especializado, lo que restringe la adopción de prácticas avanzadas de seguridad (Safár et al., 2025) (Rusu & Mantulescu, 2025). En este contexto, la baja madurez en ciberseguridad se asocia directamente con limitaciones en resiliencia digital y en la capacidad de respuesta ante incidentes (Ode et al., 2025).

En el caso de México, el estudio de Hernández-Gress et al. analiza la preparación de micro y pequeñas empresas del sector abarrotero ante la digitalización de cadenas de valor. Los resultados muestran un bajo nivel de preparación tecnológica y organizacional, lo que restringe su capacidad para avanzar hacia niveles superiores del marco NIST, particularmente en las funciones de Protect y Detect, asociadas al Tier 2 (Repetible) (Hernández-Gress et al., 2025).

Por otra parte, investigaciones en Chile muestran un mayor avance relativo en la adopción de tecnologías digitales en PYMES, especialmente en el contexto de Industria 4.0, aunque aún con brechas importantes en capacidades organizacionales y de integración tecnológica (Gatica-Neira & Ramos-Maldonado, 2022). Estos procesos de adopción han impulsado la necesidad de fortalecer políticas públicas orientadas al desarrollo de competencias digitales y ciberseguridad empresarial (Pereira et al., 2020).

En este sentido, contextos regionales como Tamaulipas podrían beneficiarse de estrategias similares, donde instituciones como la Secretaría de Desarrollo Económico (SEDECO) desempeñen un papel clave en la evolución de las empresas desde un Tier 1 (Parcial) hacia un Tier 2 (Repetible).

El marco NIST establece que las PYMES suelen ubicarse en niveles iniciales de madurez, caracterizados por prácticas ad hoc y baja formalización, mientras que el avance hacia niveles superiores implica la implementación de procesos repetibles, gestión estructurada del riesgo y mejora continua (Technology, 2024). En este contexto, el predominio de niveles iniciales en la región no solo evidencia rezagos, sino también oportunidades de escalabilidad y fortalecimiento progresivo de la ciberseguridad organizacional.

Hallazgos inesperados

Uno de los resultados más relevantes es que, aunque el 92.5% de las empresas cuenta con acceso a internet, esto no se traduce en un alto nivel de digitalización, ya que el 65% presenta niveles entre 0% y 25% de adopción digital. Este hallazgo contradice la idea de que la conectividad es un indicador suficiente de madurez digital.

En cambio, los resultados sugieren que factores organizacionales, como la resistencia al cambio y la falta de capacitación (45%), representan las principales barreras para la transformación digital. Este comportamiento ha sido identificado también en estudios sobre PYMES en economías emergentes, donde las limitaciones en habilidades digitales restringen el aprovechamiento de las tecnologías disponibles (Rupeika-Apoga et al., 2022) (Espina-Romero et al., 2024).

Asimismo, evidencia en América Latina muestra que la brecha de capacidades digitales sigue siendo un factor crítico que limita la adopción tecnológica, incluso en contextos con acceso a infraestructura básica [3], [24].

Implicaciones Teóricas y Prácticas

Los resultados confirman la existencia de una relación bidireccional entre digitalización y ciberseguridad ($\rho = 0.28$), lo que sugiere que ambas dimensiones evolucionan de manera interdependiente. Este

hallazgo es consistente con estudios que destacan el papel de las capacidades digitales como base para el desarrollo de resiliencia organizacional y gestión del riesgo (Ode et al., 2025).

Desde una perspectiva teórica, el estudio contribuye a la aplicación del modelo del National Institute of Standards and Technology en contextos de PYMES latinoamericanas, evidenciando que la mayoría se encuentra en un Tier 1 (Parcial). Asimismo, se integran elementos del modelo TOE (Tecnología–Organización–Entorno), donde los factores organizacionales actúan como mediadores clave en la adopción de prácticas de ciberseguridad, tal como ha sido documentado en la literatura sobre transformación digital en PYMES (Putri et al., 2025) (Shao et al., 2025).

En términos prácticos, los resultados indican que las PYMES en Tamaulipas deben priorizar el desarrollo de capacidades internas, especialmente en capacitación en tecnologías de la información, considerando que el 55% no cuenta con personal capacitado. Además, la baja adopción de medidas básicas de seguridad, como antivirus y respaldos (20%), y la ausencia de protocolos formales (91%), refuerzan la necesidad de implementar estrategias alineadas con la evolución del Tier 1 al Tier 2 (Repetible).

En este contexto, instituciones como la Secretaría de Desarrollo Económico (SEDECO) pueden desempeñar un papel clave mediante programas de capacitación, incentivos y políticas públicas orientadas a fortalecer la ciberseguridad y reducir la brecha digital.

Limitaciones del Estudio

El estudio presenta algunas limitaciones metodológicas que deben considerarse en la interpretación de los resultados. En primer lugar, el uso de un muestreo no probabilístico por conveniencia (n = 80) limita la generalización de los hallazgos. Además, la información recopilada es de tipo autodeclarado, lo que puede introducir sesgos de deseabilidad social.

Conclusiones

El presente estudio permitió evaluar la brecha digital y el nivel de ciberseguridad en PyMES de la región centro de Tamaulipas, utilizando como referente analítico el NIST Cybersecurity Framework. Los resultados evidencian que, si bien una alta proporción de las empresas participantes dispone de acceso a internet, esta condición no se traduce automáticamente en un nivel adecuado de digitalización ni en una madurez suficiente en ciberseguridad. En consecuencia, la conectividad, por sí sola, no constituye un indicador suficiente de transformación digital efectiva.

En términos de brecha digital, se identificó que una parte importante de las PyMES estudiadas mantiene niveles bajos de digitalización de procesos, escaso uso de herramientas avanzadas de gestión y limitada incorporación de analítica de datos para la toma de decisiones. Asimismo, persisten barreras estructurales relacionadas con la falta de capacitación, los costos de adopción tecnológica y la resistencia organizacional al cambio. Estos hallazgos confirman que la brecha digital en este tipo de empresas no se limita al acceso a infraestructura, sino que involucra también capacidades humanas, organizacionales y estratégicas.

En materia de ciberseguridad, los hallazgos muestran un nivel de madurez predominantemente inicial, caracterizado por la baja implementación de controles formales, la ausencia de protocolos escritos de respuesta a incidentes, la escasa realización de auditorías externas y la reducida asignación presupuestal a medidas de protección. Desde la perspectiva del marco NIST, este comportamiento es consistente con un Tier 1 (Parcial), en el cual las prácticas de seguridad tienden a ser reactivas, informales y dependientes de decisiones individuales más que de una estrategia institucionalizada.

Uno de los aportes más relevantes del estudio radica en evidenciar la relación entre brecha digital y ciberseguridad. Los resultados sugieren que ambas dimensiones se encuentran estrechamente vinculadas: una limitada madurez digital dificulta la adopción de prácticas

de seguridad más robustas, mientras que la ausencia de capacidades de ciberseguridad reduce la confianza y la disposición para profundizar los procesos de transformación digital. Esta relación bidireccional refuerza la necesidad de abordar ambos fenómenos de manera integrada.

A nivel práctico, los hallazgos permiten señalar que las PyMES de la región centro de Tamaulipas requieren estrategias de fortalecimiento gradual orientadas al desarrollo de capacidades digitales internas, la profesionalización de funciones TIC y la adopción progresiva de controles básicos de ciberseguridad. En este sentido, la transición desde un nivel Tier 1 hacia un Tier 2 (Repetible) demanda no solo inversión en infraestructura tecnológica, sino también capacitación continua, establecimiento de protocolos, actualización de medidas de protección y una mayor incorporación de la gestión del riesgo como parte de la estrategia empresarial.

Finalmente, el estudio aporta evidencia empírica útil para comprender las condiciones actuales de las PyMES en un contexto regional específico y ofrece una base diagnóstica para el diseño de políticas públicas, programas de apoyo institucional y acciones de acompañamiento empresarial. En particular, se destaca la relevancia de impulsar iniciativas coordinadas entre gobierno, academia y sector productivo que contribuyan a reducir la brecha digital y fortalecer la resiliencia cibernética de las empresas, favoreciendo así su competitividad, sostenibilidad y capacidad de adaptación en entornos cada vez más digitalizados.

Referencias

Banco Interamericano de Desarrollo & Organización de los Estados Americanos. (2020). *2020 cybersecurity report: Risks, progress, and the way forward in Latin America and the Caribbean*.

Barton, M., Budjac, R., Tanuska, P., Gaspar, G., & Schreiber, P. (2022). Identification overview of Industry 4.0 essential attributes and resource-limited embedded artificial-intelligence-of-things devices for small and medium-sized enterprises. *Applied Sciences*, 12(11). https://doi.org/10.3390/app12115672

Chotisarn, N., & Phuthong, T. (2025). A bibliometric analysis insights into the intellectual dynamics of artificial intelligence for the micro, small, and medium enterprises. *Cogent Business & Management*, 12(1). https://doi.org/10.1080/23311975.2025.2491684

Drydakis, N. (2022). Artificial intelligence and reduced SMEs' business risks: A dynamic capabilities analysis during the COVID-19 pandemic. *Information Systems Frontiers*, 24(4), 1223-1247. https://doi.org/10.1007/s10796-022-10249-6

Enri-Peiró, S., González-Arroyo, G., & Guijarro-Garcia, M. (2025). The role of digital transformation as a key driver of competitiveness in small and medium-sized enterprises. *Esic Market*, 56(3). https://doi.org/10.7200/esicm.56.423

Espina-Romero, L., Parra, D. R., Hurtado, H. G., Rodriguez, E. P., Arias-Montoya, F., Noroño-Sánchez, J. G., Talavera-Aguirre, R., Corzo, J. R., & Pirela, R. A. V. (2024). The role of digital transformation and digital competencies in organizational sustainability: A study of SMEs in Lima, Peru. *Sustainability*, 16(16). https://doi.org/10.3390/su16166993

Fortier, J., Gamache, S., & Fonrouge, C. (2025). Integrating sustainable performance into the digital maturity models for SMEs in manufacturing. *Applied Sciences*, 15(7). https://doi.org/10.3390/app15074041

Gatica-Neira, F., & Ramos-Maldonado, M. (2022). Differences in the capacity of adoption of the enabling ICTs for Industry 4.0 in Chile. *E & M Ekonomie a Management*, 25(4), 180-195. https://doi.org/10.15240/tul/001/2022-4-012

Hernández-Gress, E. S., Mejía, A. I. R., Gómez-Rocha, J. E., & Deniz, S. (2025). Digital transformation through virtual value chains: An exploratory study of grocery MSEs in Mexico. *Systems*, 13(10). https://doi.org/10.3390/systems13100849

INEGI. (2023). *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares*.

INEGI. (2023). *Estadísticas a propósito del Día Mundial de Internet*.

Instituto Nacional de Estadística. (2023). *Encuesta sobre el uso de las Tecnologías de la Información y las Comunicaciones y del Comercio Electrónico en las Empresas (ETICCE)*.

Jie, H. L., Gooi, L. M., & Lou, Y. C. (2025). Digital maturity, dynamic capabilities and innovation performance in high-tech SMEs. *International Review of Economics & Finance*, 99. https://doi.org/10.1016/j.iref.2025.103971

Martínez-Domínguez, M., & Mora-Rivera, J. (2020). Internet adoption and usage patterns in rural Mexico. *Technology in Society*, 60. https://doi.org/10.1016/j.techsoc.2019.101226

Muhammad, S. S., Dey, B. L., Kamal, M. M., Samuel, L., & Alzeiby, E. A. (2025). Digital transformation or digital divide? SMEs' use of AI during global crisis. *Technological Forecasting and Social Change*, 217. https://doi.org/10.1016/j.techfore.2025.124184

Neves, A., Alves, A. S. F., Ionita, V. A., Matias, J. C. O., Teixeira, S., Alcácer, V., & Godina, R. (2025). Key drivers and barriers of industry 4.0 for sustainable practices in small and medium-sized enterprises. *Sustainable Futures*, 10. https://doi.org/10.1016/j.sftr.2025.101464

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 2). https://doi.org/10.6028/NIST.CSWP.29

Ode, E., Awolowo, I. F., Nana, R., & Olawoyin, F. S. (2025). Social capital and artificial intelligence readiness: The mediating role of cyber resilience and value construction of SMEs in resource-constrained environments. *Information Systems Frontiers*. Advance online publication. https://doi.org/10.1007/s10796-025-10608-z

Pereira, G. V., Estevez, E., Cardona, D., Chesñevar, C., Collazzo-Yelpo, P., Cunha, M. A., Diniz, E. H., Ferraresi, A. A., Fischer, F. M., Garcia, F. C. O., Joia, L. A., Luciano, E. M., de Albuquerque, J. P., Quandt, C. O., Rios, R. S., Sánchez, A., da Silva, E. D., Silva, J. S., Jr., & Scholz, R. W. (2020). South American expert roundtable: Increasing adaptive governance capacity for coping with unintended side effects of digital transformation. *Sustainability*, 12(2). https://doi.org/10.3390/su12020718

Pérez-Campdesuñer, R., Sánchez-Rodríguez, A., García-Vidal, G., Martínez-Vivar, R., & De Miguel-Guzmán, M. (2025). Artificial intelligence in Ecuadorian SMEs: Drivers and obstacles to adoption. *Information*, 16(6). https://doi.org/10.3390/info16060443

Pozo-Benites, K. B., García-Silva, K. W., Peñarreta-Barrera, E. E., & Meza-Salvatierra, J. K. (2025). Transformación digital de las PYMES en América Latina: barreras, oportunidades y estrategias para la competitividad. *Multidisciplinary Latin American Journal*, 3(2), 236–255. https://doi.org/10.62131/MLAJ-V3-N2-015

Putri, E., Bandi, B., Widarjo, W., & Arifin, T. (2025). The value of cloud accounting for MSMEs: A Technology-Organization-Environment (TOE) framework perspective. *Cogent Business & Management*, 12(1). https://doi.org/10.1080/23311975.2025.2494712

Red Latinoamericana de Innovación y Emprendimiento. (2018). *Perfil tecnológico de la micro y pequeña empresa de Latinoamérica*.

Rupeika-Apoga, R., Petrovska, K., & Bule, L. (2022). The effect of digital orientation and digital capability on digital transformation of SMEs during the COVID-19 pandemic. *Journal of Theoretical and Applied Electronic Commerce Research*, 17(2), 669-685. https://doi.org/10.3390/jtaer17020035

Rusu, D., & Mantulescu, M. (2025). Development of an application-based framework for information security management in SMEs. *Sustainability*, 17(18). https://doi.org/10.3390/su17188314

Safár, L., Pekarcik, M., Morawiec, P., Rutecka, P., & Wieczorek-Kosmala, M. (2025). Mapping cybersecurity in SMEs: The role of ownership and firm characteristics in the Silesian region of Poland. *Information*, 16(7). https://doi.org/10.3390/info16070590

Shao, Q. G., Lin, J. X., Liou, J. J. H., Zhu, D., & Tzeng, G. H. (2025). Analysis of key factors affecting the digital transformation of small and medium-sized manufacturing enterprises in China. *Sage Open*, 15(2). https://doi.org/10.1177/21582440251336077

Tetteh, G. K., & Otioma, C. (2025). Cyberattack, cyber risk mitigation capabilities, and firm productivity in Kenya. *Small Business Economics*, 64(3), 1493-1514. https://doi.org/10.1007/s11187-024-00946-8

Zahra, M., Naqvi, S. A. A., Hussain, B., & Magazzino, C. (2025). Digitalizing sustainability in Pakistan's textile sector: An investigation of lean digital transformation adoption. *International Journal of Engineering Business Management*, 17. https://doi.org/10.1177/18479790251369174

Yanel Azucena Mireles Sena
Universidad Politécnica de Victoria | Victoria | México
https://orcid.org/0009-0006-7785-0603
2439016@upv.edu.mx
yanelmireles0@gmail.com
Estudiante de maestría en ingeniería con perfil de investigación en la Universidad Politécnica de Victoria, egresada de Ingeniería en Tecnologías de la Información.
Hiram Herrera Rivas
Universidad Politécnica de Victoria | Victoria | México
https://orcid.org/0000-0002-2650-8932
hherrerar@upv.edu.mx
hiramhr@gmail.com
Miembro del Sistema Nacional de Investigadoras e Investigadores de México, que forma parte del consejo Nacional de Humanidades, Ciencias y Técnologías.
Jorge Arturo Hernández Almazán
Universidad Politécnica de Victoria | Victoria | México
https://orcid.org/0000-0003-1060-6455
jhernandeza@upv.edu.mx
Dr.Jorge.Arturo.Hernandez.Almazan@gmail.com
Tiene el Doctorado en Gestión y Transferencia del Conocimiento. Realizó una estancia de investigación en la Universidad Jaume I en España para desarrollar investigación sobre Big Data e interoperabilidad.
José Fidencio López Luna
Universidad Politécnica de Victoria | Victoria | México
https://orcid.org/0000-0003-2348-7088
jlopezl@upv.edu.mx
Maestro en Sistemas de Información y candidato a Doctor en Gestión por la UAT. Se desempeña como profesor de tiempo completo en la Universidad Politécnica de Victoria

Digital Divide and Cybersecurity Maturity in SMEs from the Central Zone of Tamaulipas: A Comparative Analysis with the NIST Framework

Abstract
Small and medium-sized enterprises (SMEs) face significant challenges related to the digital divide and cybersecurity, particularly in regions with limited resources and low levels of technological adoption. This chapter addresses the situation of SMEs in the central region of Tamaulipas from a digital transformation and risk management perspective, using the NIST Cybersecurity Framework (NIST CSF) as a reference. The study is developed under a quantitative and descriptive approach, based on the application of a questionnaire aimed at identifying connectivity conditions, use of digital technologies, ICT capabilities, and cybersecurity practices. Likewise, it examines the barriers hindering technological adoption, the availability of specialized personnel, and the level of preparedness of companies against security incidents. The chapter presents a general characterization of the participating SMEs, analyzes the relationship between digitalization and cybersecurity, and compares the findings with the maturity levels established by the NIST framework.

Finally, the main areas of opportunity to strengthen the resilience and competitiveness of companies in regional contexts are discussed.
Keywords: Digital divide; Cybersecurity; SMEs; Tamaulipas; NIST Cybersecurity Framework.

Brecha Digital e Maturidade em Cibersegurança em PMEs da Zona Central de Tamaulipas: Uma Análise Comparativa com o Framework NIST

Resumo

As pequenas e médias empresas (PMEs) enfrentam desafios significativos relacionados à brecha digital e à cibersegurança, particularmente em regiões com recursos limitados e baixos níveis de adoção tecnológica. Este capítulo aborda a situação das PMEs da região central de Tamaulipas a partir de uma perspectiva de transformação digital e gestão de riscos, utilizando como referência o NIST Cybersecurity Framework (NIST CSF). O estudo desenvolve-se sob uma abordagem quantitativa e descritiva, a partir da aplicação de um questionário orientado a identificar condições de conectividade, uso de tecnologias digitais, capacidades de TIC e práticas de cibersegurança. Da mesma forma, examinam-se as barreiras que dificultam a adoção tecnológica, a disponibilidade de pessoal especializado e o nível de preparação das empresas frente a incidentes de segurança. O capítulo apresenta uma caracterização geral das PMEs participantes, analisa a relação entre digitalização e cibersegurança e compara os achados com os níveis de maturidade estabelecidos pelo framework NIST. Finalmente, discutem-se as principais áreas de oportunidade para fortalecer a resiliência e a competitividade das empresas em contextos regionais.
Palavras-chave: Brecha digital; Cibersegurança; PMEs; Tamaulipas; NIST Cybersecurity Framework.