

Estrategias ante ciberdelincuencia en las MiPyME de México: Caso de estudio en San Andrés Cholula, Puebla

Dra. Laura Leticia Vélez Hernández, Mtra. Martha Patricia Tello Cano, Dra. Esther Tlaczani Conde, M.Sc.A Carlos Roberto Ibáñez Juárez, C. José Luis Cruz Palacios

Resumen - El presente trabajo se enfoca en la identificación de amenazas cibernéticas a las que se pueden enfrentar las MiPyME, considerando la evolución constante del uso de tecnología incluyendo el uso de la inteligencia artificial, se analizan los factores específicos de una MiPyME del ramo inmobiliario, ubicada en San Andrés Cholula analizando sus características y perspectiva. Se considera una investigación de corte mixto al realizar entrevistas en profundidad a los directivos de la empresa, así como la aplicación de cuestionarios al personal para conocer el grado de sensibilización ante los ciberdelitos, se analizarán las estrategias adoptadas preventivas y de atención ante un posible impacto operativo, con la intención de ofrecer un análisis y propuestas de protección que contribuyan al desarrollo de buenas prácticas aplicables a otras MiPyMEs. El presente trabajo pretende no solo ofrece información que contribuya a asegura la continuidad del negocio, sino que también promueve un entorno empresarial más seguro y confiable.

Índice de Términos – Ciberdelitos, Ciberseguridad, Continuidad del negocio, Inteligencia Artificial, MiPyME.

I. PROBLEMÁTICA

En el contexto actual, las micro, pequeñas y medianas empresas (MiPyME) desempeñan un papel esencial en el desarrollo económico, representando una proporción significativa del empleo y la productividad global. Sin embargo, este sector enfrenta desafíos crecientes relacionados con la seguridad digital. Durante los últimos años, el incremento en la sofisticación, frecuencia y alcance de los ciberataques ha expuesto la vulnerabilidad de estas organizaciones, que a menudo carecen de los recursos técnicos y financieros necesarios para implementar sistemas de ciberseguridad robustos.

Estudios recientes indican que las MiPyME son blanco atractivo para los ciberdelincuentes debido a la percepción de ser entidades con menor capacidad de respuesta ante incidentes. Esto se traduce en pérdidas económicas, daño a la reputación y, en ocasiones, el cese de operaciones. Según datos de organismos internacionales, más del 60% de las Mipymes

afectadas por un ciberataque no logran recuperar su estabilidad y cesan actividades en un lapso de seis meses [1].

Entre los principales factores que incrementan la exposición de las MiPyME a ciberataques se encuentra la limitada cultura de ciberseguridad, la falta de estrategias de prevención, y el desconocimiento de medidas básicas como el uso de contraseñas robustas, actualizaciones periódicas de software y sistemas de respaldo de información. Además, el auge del teletrabajo y la acelerada transformación digital han incrementado el uso de herramientas tecnológicas no seguras, amplificando las oportunidades de ataque.

Este problema no solo afecta a las empresas individualmente, sino que también tiene un impacto significativo en la estabilidad económica y social de las comunidades donde operan. Por ello, es necesario desarrollar estrategias efectivas y sostenibles que fortalezcan la ciberseguridad en las MiPyMEs, adaptadas a sus características y recursos limitados. Esto incluye campañas de concientización, programas de formación en seguridad digital y el diseño y uso de herramientas asequibles que permitan identificar y mitigar riesgos.

II. OBJETIVOS

A. General

Identificar las problemáticas de ciberdelincuencia a las que se enfrentan las MiPyME en México y conocer la situación específica de una empresa Inmobiliaria en San Andrés Cholula en el estado de Puebla para proponer estrategias de protección a la empresa y sirva como referente para otras similares.

B. Específicos

1. Revisión de literatura para identificar las problemáticas de ciberdelincuencia a las que se enfrentan las MiPyME en

¹Documento recibido el 8 de septiembre de 2026

México.

2. Conocer la situación de la empresa Inmobiliaria en San Andrés Cholula con relación al nivel de conocimiento que tienen sus directivos y empleados en ciberseguridad.
3. Identificar mecanismos de protección actuales y eficientes para MiPyME
4. Proponer estrategias de protección en ciberseguridad para MiPyME

III. PREGUNTA

¿Cómo afecta el desconocimiento de las amenazas específicas de ciberdelincuencia, junto con la subestimación de su probabilidad e impacto a la capacidad de las MiPyME, para implementar medidas de ciberseguridad que protejan sus operaciones?.

IV. CONTEXTO TEÓRICO

El crecimiento exponencial del uso de las tecnologías digitales ha obligado a las empresas a adaptarse rápidamente a nuevas formas de operar, con un enfoque cada vez mayor en el comercio electrónico, el trabajo remoto y la gestión de datos en la nube. Este desarrollo ha sido acompañado por una explosión de amenazas cibernéticas, lo que ha requerido una evolución constante de las estrategias de ciberseguridad. A continuación, se explora los conceptos, teorías y enfoques clave que sustentan la protección de los activos digitales en un entorno cada vez más interconectado.

El Instituto Nacional de Ciberseguridad (INCIBE), refiere a la ciberseguridad como el conjunto de procesos, políticas y tecnologías implementadas para proteger los sistemas informáticos, redes, datos y dispositivos digitales contra ataques maliciosos, accesos no autorizados, interrupciones y daños. Adicionalmente hay que mencionar que la ciberseguridad no solo busca garantizar la confidencialidad, integridad y disponibilidad de la información, sino también la protección de la privacidad personal de los usuarios en un entorno digital cada vez más complejo [2].

La evolución de la ciberseguridad ha seguido el ritmo de la innovación tecnológica, con un cambio de enfoque desde simples medidas reactivas hacia estrategias proactivas. Mientras que las primeras herramientas de ciberseguridad se centraban en cortafuegos y antivirus para proteger las redes internas, el panorama moderno incluye una gama más amplia de enfoques, desde la detección avanzada de amenazas hasta la inteligencia artificial aplicada a la seguridad.

Durante las primeras fases del desarrollo de la ciberseguridad, los sistemas estaban mayormente basados en enfoques perimetrales, donde se implementaban medidas como los antivirus y cortafuegos para evitar accesos no autorizados desde el exterior. Este modelo resultó eficaz durante las primeras

etapas de la digitalización, ya que las empresas gestionaban sus datos de manera local, con una infraestructura digital centralizada. Las empresas dependían de estas herramientas reactivas hasta que el aumento de las amenazas más sofisticadas, como el ransomware y el phishing, superaron su capacidad [3].

A continuación, se especifican los ciberataques más comunes dirigidos a las empresas u organizaciones, aunque también pueden estar dirigidos a cualquier tipo de persona.

Ataques Phishing, es un tipo de ataque que utiliza técnicas denominadas de ingeniería social para engañar a las víctimas y obtener información confidencial, como contraseñas, datos bancarios o credenciales de acceso. Los atacantes suelen hacerse pasar por entidades de confianza a través de correos electrónicos, mensajes de texto, o llamadas telefónicas, con el objetivo de redirigir a las víctimas hacia sitios web falsos o descargar malware. Este ataque puede manifestarse en varias formas, como el smishing (por SMS) y el vishing (por voz). El spear phishing, una variante dirigida, se enfoca en objetivos específicos mediante la investigación previa de sus perfiles públicos en línea [4].

Robo de Información, la cual puede ocurrir cuando datos críticos o confidenciales son eliminados, o se dañan quedando inaccesibles debido a ataques cibernéticos. Con el objetivo de que las organizaciones tengan una interrupción operativa, e incluso daños reputacionales y sanciones regulatorias.

Fuga de Información Sensible, se refiere a la exposición no autorizada de datos confidenciales, como información personal, financiera o de propiedad intelectual.

Ransomware, es un tipo de software malicioso que cifra los datos de la víctima, bloqueando su acceso hasta que se pague un rescate. Este ataque puede propagarse a través de correos electrónicos con archivos adjuntos maliciosos, sitios web comprometidos o vulnerabilidades de software [5], [6].

Suplantación de Identidad, implica hacerse pasar por otra persona u organización para engañar a las víctimas y obtener acceso a información confidencial o recursos financieros. Esto puede realizarse a través de correos electrónicos falsificados, llamadas telefónicas o redes sociales.

Denegación de Servicio, un ataque de denegación de servicio (DoS) tiene como objetivo interrumpir la disponibilidad de servicios en línea sobrecargando un sistema con solicitudes falsas, impidiendo que los usuarios legítimos accedan al recurso. En su variante distribuida (DDoS), los atacantes utilizan múltiples sistemas comprometidos para amplificar el impacto del ataque [5].

V. METODOLOGÍA

Se utilizó método de investigación mixta, en primer lugar, cualitativa, siguiendo un procedimiento lógico entendido la situación actual y respondiendo a las preguntas ¿por qué?, ¿cómo? y ¿en qué forma? También se utilizó el método cuantitativo al estudiar la relación entre las variables planteadas y entender con qué frecuencia e impacto y después de analizar los datos permitiera un planteamiento de estrategias de atención, para lo cual se aplicó un cuestionario a todos los integrantes de la empresa y se realizaron entrevistas al personal que representaba con un mayor rango de autoridad a cada una de las áreas: Administradores, Asesores inmobiliario, Ventas y Auxiliares.

Para entender cómo afecta el desconocimiento de las amenazas

específicas de ciberdelincuencia junto con la estimación de su probabilidad e impacto, y la capacidad de las MiPyME para implementar medidas de ciberseguridad que protejan sus operaciones, para tal efecto se establecen variables de análisis, mismas que se utilizan para la obtención de información mediante entrevistas y aplicación de cuestionarios.

En la Tabla 1, se describe la consideración de variables, así como su definición conceptual y operacional para identificar la relación de las diversas amenazas más frecuentes, con las probabilidades e impacto posible ante los mediadores de seguridad implementadas, su operacionalización se detalla a continuación

Tabla 1. Operacionalización de variables

Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Escala
Desconocimiento de las amenazas específicas de ciberdelincuencia	Nivel de desconocimiento de los responsables de las MiPyME acerca de los tipos de ciberataques que pueden afectarlas.	A través de cuestionario que evalúe el nivel de conocimiento de amenazas	- Tipos de amenazas - Consecuencias potenciales	- % de amenazas identificadas - Identificación de consecuencias	Ordinal, grupo de preguntas con Escala Likert con 3 niveles de conocimiento; bajo medio y alto
Estimación de la probabilidad e impacto de ciberataques	Probabilidad de ocurrencia de un ciberincidente, así como sus consecuencias	Mediante ítems de percepción de probabilidad y severidad de impacto	- Probabilidad percibida - Impacto percibido	- Diferencia entre percepción y estadísticas sectoriales. - Nivel de riesgo asignado por la empresa	
Capacidad para implementar medidas de ciberseguridad	Nivel en que la MiPyME implementa, y sostiene prácticas de protección tecnológica y organizacional.	Aplicación de checklist de medidas implementadas y su frecuencia de revisión.	- Medidas técnicas (software y hardware) - Medidas organizacionales - Capacitación	- No. de medidas implementadas. - Existencia de políticas escritas - Frecuencia de capacitaciones por año	Nominal (sí/no) y de frecuencia

Fuente. Elaboración propia.

VI. RESULTADOS

Se identifica como uno de los desafíos primordiales en temas de ciberseguridad para la empresa Inmobiliaria en San Andrés Cholula, la limitación de contar con personal técnico especializado, aunado a la disponibilidad de recursos financieros que les permita la implementación de mecanismos o contratación de empresas que los apoyen en el mismo sentido. A continuación, se muestran los hallazgos de acuerdo con los cuestionarios aplicados al personal.

Con respecto al Desconocimiento de las amenazas específicas de ciberdelincuencia encontramos que el 12.5 por ciento reconoce como amenaza a los correos fraudulentos (phishing), como un elemento de amenaza media, el 20% identifica como amenazas la recepción de mensajes vía mensajería instantánea principalmente WhatsApp como una posible extorsión en nivel alto, el 13,5 % mencionó que considera malware como una amenaza media el extraer información y contraseñas, mientras que el 54% mencionó que desconoce que otro tipo de ciberataque podrían ser objetos, así como el nivel de riesgo. Con respecto a la identificación de consecuencias, entre las mencionadas se encuentran la extorsión y la suplantación de

identidad con consecuencias de robo de información y extorsión mediante la solicitud de depósitos falsos.

Tabla 2. Distribución de amenazas y percepción de nivel de riesgo

Tipo de amenaza	Porcentaje	Nivel de riesgo / descripción
Phishing	12.50%	Amenaza media
Mensajes de extorsión	20.00%	Amenaza alta
Malware	13.50%	Amenaza media
Desconocido	54.00%	No identifican amenazas cibernéticas

Fuente. Elaboración propia.

Estimación de la probabilidad e impacto de ciberataques

Entre la probabilidad de ser extorsionados, el 45 % mencionó que considera como una posibilidad real ser víctimas de ciberataques, teniendo claridad en que eso puede generar interrupción de operaciones, pérdida de información crítica y afectaciones económicas por fraude o rescates y, en consecuencia, daño reputacional y pérdida de confianza de clientes y proveedores. En términos de probabilidad, puede estimarse un nivel medio el 45 % referido. Ver. Tabla 3. Estimación de la probabilidad e impacto. Estas cifras reflejan que la principal superficie de ataque en las MiPyMES mexicanas continúa siendo el factor humano al poder ser víctimas de engaños.

Tabla 3. Estimación de la probabilidad e impacto

Probabilidad	Media
Impacto	Alto

Fuente. Elaboración propia.

Respecto a la capacidad para implementar medidas de ciberseguridad, detectamos que no cuentan con un control de número de medidas implementadas, pero si refieren algunas. Entre ellas se encontró que como se aprecia en la Tabla 4, el 62.5 % de los trabajadores realizar respaldo de información, pero lo realizan sin una periodicidad específica y El 75% del personal refiere como prácticas el uso de software antivirus y antimalware, actualización de sistemas operativos principalmente en sus dispositivos móviles, y el empleo de contraseñas que consideran robustas, pero sin renovación obligatoria; el 37.5% no sabe si alguien más toma medidas respecto a su información ya que de manera personal no lo realiza. Refieren acceso a navegación web sin mayor conocimiento sobre seguridad por ejemplo de verificación de sitios seguros, así mismo refieren falta de personal especializado y capacitación, el 25% restante del personal, no toma medidas de seguridad refiriendo que no tienen una

capacitación u obligatoriedad en la empresa al respecto, tampoco cuentan con algún seguro en caso de ciberataque, ni con políticas escritas de ciberseguridad.

En cuanto a frecuencia de capacitaciones por año, están contemplando realizar capacitaciones, pero no tienen nada como compromisos, metas u objetivos específicos planteados.

Tabla 4. Capacidad para implementar medidas de seguridad

No. de medida implementada	Porcentaje de empleados que la implementa	Medidas de ciberseguridad implementada	Frecuencia
1	62.5%	Respaldo de información	Sin periodicidad específica
2	75.0%	Uso de software antivirus y antimalware	Sin periodicidad específica de actualización
3		Actualización de sistemas operativos	Sin periodicidad específica de actualización
4		Uso de contraseñas seguras	Sin renovación obligatoria

Fuente. Elaboración propia.

VII. CONCLUSIÓN

La empresa analizada requiere de programas de formación continua que permita la generación de un ambiente de seguridad ante los ciberdelitos siendo conscientes de llevar controles básicos como políticas de contraseñas seguras, realización periódica de respaldos de información y actualizaciones periódicas tanto en sus sistemas operativos como el uso de antivirus en sus equipos con acceso a internet para mantener segura la operatividad diaria, pues son elementos que no se aplican de manera consistente [7]. Adicionalmente apelar al pensamiento crítico ante la recepción de mensajes de personas desconocidas, con información acompañada de links o la invitación a tomar acciones inmediatas sin la reflexión y análisis.

Otra estrategia de protección en ciberseguridad es contemplar la posibilidad de adaptación como medidas de prevención y mitigación, la adopción de controles preventivos, detectivos y correctivos, alineados con marcos de referencia como ISO/IEC 27001 y el NIST Cybersecurity Framework (CSF) 2.0, que contribuye significativamente a disminuir la probabilidad y el impacto del ciberataque al verse comprometidas las empresas a implementar medidas y realizar auditorías.

Para mitigación el uso de aplicación de normas como lo es el caso de ISO 27032 Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad también podría

contribuir a que las MiPyMES a reducir sus niveles de riesgo e impacto de ser objetivo de ciberataques, principalmente mediante phishing, robo de credenciales, malware y ransomware, debido a la creciente dependencia de las tecnologías digitales y a las limitaciones de recursos destinados a la ciberseguridad. Aunque muchas organizaciones implementan medidas básicas como antivirus, firewalls, copias de seguridad y capacitación del personal, estas suelen ser insuficientes cuando no forman parte de una estrategia integral de gestión de riesgos. Por ello, resulta indispensable fortalecer la cultura de ciberseguridad, adoptar controles preventivos y de respuesta alineada a buenas prácticas nacionales e internacionales, y promover la actualización continua de los sistemas y del personal. Estas acciones no solo disminuyen la probabilidad e impacto de los incidentes, sino que también contribuyen a garantizar la continuidad operativa, la protección de la información y la confianza de clientes y socios comerciales.

REFERENCIAS

- [1] Kaspersky Lab. (2017). El 60 % de las pymes que sufren un ciberataque desaparece seis meses después, según Kaspersky Lab. *El Economista*. <https://www.eleconomista.es/tecnologia/noticias/8647058/10/17/El-60-de-las-pymes-que-sufren-un-ciberataque-desaparece-seis-meses-despues-segun-Kaspersky-Lab.html>
 - [2] González Martínez, J. (2019). *Innovación en Ciberseguridad: Estrategia y Tendencias*. Centro Tecnológico Gradiant(Innovación en Ciberseguridad: Estrategia y Tendencias).
 - [3] Stedman, C. (2022). *The Ultimate Guide to Cybersecurity Planning for Businesses*.
 - [4] UNAM-CERT. (2024). Guía sobre ataques de phishing y su prevención. Recuperado de www.seguridad.unam.mx
 - [5] INCIBE. (2024). Phishing, ransomware y ataques DDoS: Conceptos básicos en ciberseguridad. Recuperado de www.incibe.es
 - [6] Asociación Mexicana de Ciberseguridad. (2024). ¿Qué es el phishing? Recuperado de www.ameci.org
 - [7] Lucky B.B., Ayodeji E. A. (2024). *Global Journal of Engineering and Technology Advances*, 2024, 19(02), 134–153. <https://doi.org/10.30574/gjeta.2024.19.2.0084>
1. Vélez, H.L., (2025). Modelo de gestión de riesgos laborales para instituciones de educación superior. *Educación, gestión y desarrollo: perspectivas y prácticas innovadoras*. BUAP. (págs.112-141) Recuperado de https://repositorio.buap.mx/rdgp/public/inf_public/2025/1/Educacion_gestion_y_desarrollo-_perspectivas_y_practicas_innovadoras.pdf#page=113
 2. Ibáñez J.R., Ruíz C.N., Vélez H.L, Fernández I. (2022). El plan de mejoramiento para el cierre de las no conformidades derivada de la auditoría externa FSSC 22000 para la empresa Citrusper S.A.P.I. DE C. V. INCAING, 1-5. Recuperado de <https://ojsincaing.com.mx/index.php/ediciones/article/view/144/ibanezs>
 3. Ibáñez J.R., Ruíz C.N., Vélez H.L, Mora. (2022). La Implementación de un plan de mejora en la estandarización de procedimientos de trabajo en Pyme'S. INCAING, 10-18. Recuperado de <https://ojsincaing.com.mx/index.php/ediciones/article/view/14>



Mtra. Martha Patricia Tello Cano

Licenciada en Sistemas Computacionales, Maestra en Administración y Gestión de Instituciones Educativas, Doctorante en Administración, reconocimiento como perfil PRODEP, certificación ANFECA y dos certificaciones Conocer, emprendedora en el ramo heladero y con experiencia en campo tanto en la iniciativa privada como el sector público.

ORCID: <https://orcid.org/0000-0003-3581-7718>

1. Tello, M, Boix, A. et al (2025). La inteligencia artificial en el desempeño académico de los alumnos de educación media superior en México. Capítulo 7. Entelequia Editores. ISBN: 978-970-96964-8-6
2. Hernández, N, Tello, M, et al (2025). *Educación del CEO y Desempeño Empresarial: Relación entre Formación Académica y Resultados Corporativos*. Scienceevolution. ISSN 2810-8728

Biografía Autor(es)



Dra. Laura Leticia Vélez Hernández

Licenciada en Informática, Mtra. Comunicación y Tecnologías Educativas, Dra. Administración. Investigadora con reconocimiento como Candidata en el Sistema Nacional de Investigadores e Investigadoras. SNII México, reconocimiento como perfil PRODEP, certificación Anfeca, y diversas certificaciones de la Red Conocer. Es miembro de la RED Internacional de Investigadores en Gestión y Desarrollo de las Organizaciones.

ORCID: <https://orcid.org/0000-0002-7609-2576>



Dra. Esther Tlaczani Conde

Ingeniera en Ciencias de la Computación, Licenciada en Administración de Empresas, Maestra en Educación Superior y Doctora en Administración. Esta formación multidisciplinaria le ha permitido construir una sólida trayectoria en la intersección de la tecnología, la gestión empresarial y la educación. Es investigadora con

reconocimiento como candidata por el Sistema Nacional de Investigadoras e Investigadores (SNII). Certificada por parte de la SEP-CONOCER en el Estándar de Competencia EC0366: Desarrollo de cursos de formación en línea y EC0108 de Manejo del procesador de hojas de cálculo digitales.

ORCID: <https://orcid.org/0000-0003-4077-788>

1. Tlaczani Conde, E., Vélez Hernández, L. L., Blázquez Bonilla, J., & Gordiano Soriano, E. (2025). Herramientas Digitales para la Gestión Emocional en Estudiantes de Educación Superior. [Capítulo 20] En Investigación de las tendencias digitales para el futuro de la educación. Benemérita Universidad Autónoma de Puebla. ISBN 978-968-9744-15-3. https://www.researchgate.net/publication/404181616_Herramientas_Digitales_para_la_Gestion_Emocional_en_Estudiantes_de_Educacion_Superior
2. Tlaczani Conde, E., Blázquez Bonilla, J., Blázquez Bonilla, E., Vélez Hernández, L. L., & Aparicio Francisco, M. (2025). La salud digital en las PYMES. [Capítulo 9] En Innovación, Comunicación y Divulgación de la Ciencia en las Organizaciones México - Colombia. Entelequia Editores. ISBN 978-970-96964-8-6. https://www.researchgate.net/publication/405309947_capitulo_9_la_salud_digital_en_las_pymes_libro_innovacion_comunicacion_y_divulgacion_de_la_ciencia_en_las_organizaciones_mexico_colombia

**Docentes de la Facultad de Administración BUAP
Puebla, México**



C. José Luis Cruz Palacios

Estudiante de la Licenciatura de Administración de Empresas BUAP



Dr. Carlos Roberto Ibáñez Juárez

Doctor en Ciencias de la Ingeniería Mecánica con especialidad en materiales compuestos, miembro del Capítulo Estudiantil ASME-BUAP y del Cuerpo Académico BUAP-CA-419 “Modelación, Simulación y Prototipado de Sistemas Físicos de la Ingeniería”. Sus líneas de investigación abarcan la mejora continua en cadenas productivas educativas, así como la simulación y el modelado en ingeniería industrial, mecánica y eléctrica. Profesor Investigador con perfil PRODEP, autor de capítulos de libro en educación universitaria, modelado mecánico y modelos estocásticos. Participa como evaluador en el Comité de Evaluación de programas educativos de ingeniería a nivel nacional del CACEI. Entre sus publicaciones recientes destacan: “Mechanical performance of green composites made with natural fiber of henequen”, en *Materials Research Express* (2025); “El impacto de la libertad de cátedra en el bajo índice de egreso de Ingeniería Industrial” (2025); y “Relación entre rendimiento académico e inteligencia emocional en tiempos de COVID-19” (2024). Sus perfiles académicos están disponibles en ORCID (0000-0002-2530-3345), ResearchGate, Google Scholar y Academia.edu

**Docente de la Facultad de Ingeniería BUAP
Puebla, México**