TSE'DE
Revista de Investigación Científica
ISSN 2600 - 5557

LA SEGURIDAD DEL INTERNET DE LAS COSAS (IoT) EN LAS PYMES: VULNERABILIDADES Y SOLUCIONES EMERGENTES

INTERNET OF THINGS (IoT) SECURITY IN SMES: VULNERABILITIES AND EMERGING SOLUTIONS

SEGURANÇA DA INTERNET DAS COISAS (IoT) EM PMES: VULNERABILIDADES E SOLUÇÕES EMERGENTES

Ing. Rocío Mendoza Villamar
rocio.mendoza@uleam.edu.ec
Universidad Laica Eloy Alfaro de Manabí, Ecuador
Orcid: 0000-0002-1277-7162

Karen Montalvan Loor
e1311056970@live.uleam.edu.ec
Universidad Laica Eloy Alfaro de Manabí, Ecuador
Orcid: 0009-0008-1068-6735

Julexy Castro Alava
e0929030559@live.uleam.edu.ec
Universidad Laica Eloy Alfaro de Manabí, Ecuador.
Orcid: 0009-0004-4724-7155

REVISTA TSE´DE
Instituto Superior Tecnológico Tsa´chila
ISSN: 2600-5557

Resumen

Para el siguiente estudio se hizo uso de una metodología bibliográfica con fin documental, no existió delimitación geográfica. El trabajo se centró en la recolección de información de fuentes confiables. La técnica utilizada fue una tabla comparativa de soluciones emergentes. En el marco teórico resume que las principales vulnerabilidades de IoT aplicado a PYMES son: la falta de segmentación de red, errores humanos, encriptación débil, falta de actualizaciones, entre otros. Y como soluciones emergentes a estas amenazas se propuso: mejorar segmentación de red, implementar la arquitectura zero trust, inteligencia artificial, encriptaciones cuánticas, herramientas en la nube y capacitación del personal. Para obtener los resultados se realizó la evaluación cualitativa comparando estas soluciones propuestas en: eficacia, accesibilidad, escalabilidad e innovación, identificando a las herramientas en la nube como la más equilibrada para PYMES con un puntaje de 8.5/10. Finalmente, la solución correcta depende de necesidades de la empresa y su presupuesto.

Palabras clave: Internet de las Cosas, ciberseguridad, PYMES, vulnerabilidades tecnológicas, seguridad informática

TSE'DE
Revista de Investigación Científica
ISSN 2600 - 5557

Abstract

For the following study, a bibliographic methodology was used for documentary purposes, without geographical limitations. The work focused on collecting information from reliable sources. The technique used was a comparative table of emerging solutions. The theoretical framework summarizes that the main vulnerabilities of IoT applied to SMEs are: lack of network segmentation, human error, weak encryption, lack of updates, among others. Emerging solutions to these threats were proposed: improved network segmentation, implementation of zero-trust architecture, artificial intelligence, quantum encryption, cloud tools, and staff training. To obtain the results, a qualitative evaluation was conducted comparing these proposed solutions in terms of effectiveness, accessibility, scalability, and innovation, identifying cloud tools as the most balanced for SMEs with a score of 8.5/10. Ultimately, the right solution depends on the company's needs and budget.

Keywords: Internet of Things, cybersecurity, SMEs, technological vulnerabilities, information security

Resumo

Para o presente estudo, utilizou-se metodologia bibliográfica para fins documentais, sem limitações geográficas. O trabalho concentrou-se na coleta de informações de fontes confiáveis. A técnica utilizada foi uma tabela comparativa de soluções emergentes. O referencial teórico resume que as principais vulnerabilidades da IoT aplicada a PMEs são: falta de segmentação de rede, erro humano, criptografia fraca, falta de atualizações, entre outras. Foram propostas soluções emergentes para essas ameaças: melhoria da segmentação de rede, implementação de arquitetura de confiança zero, inteligência artificial, criptografia quântica, ferramentas em nuvem e treinamento de pessoal. Para obter os resultados, foi realizada uma avaliação qualitativa comparando essas soluções propostas em termos de eficácia, acessibilidade, escalabilidade e inovação, identificando as ferramentas em nuvem como as mais equilibradas para PMEs, com uma pontuação de 8,5/10. Em última análise, a solução ideal depende das necessidades e do orçamento da empresa.

Palavras-chave: Internet das Coisas, cibersegurança, PMEs, vulnerabilidades tecnológicas, segurança da informação

Periocidad Semestral
Vol. 8, núm. 3
revistatsede@tsachila.edu.ec

Recepción: 08-11-2025
Aprobación: 01-12-2025
Publicación: 25-12-2025

URL:
http://tsachila.edu.ec/ojs/index.php/TSEDE/issue/archive

Introducción

La era digital ya es una realidad y las PYMES atraviesan un proceso de innovación dentro de sus negocios, ya que se encuentran en el dilema de, o me adapto a las nuevas tecnologías o me quedo atrás. Ya que estas llevan una presión por la digitalización que se genera por la misma competencia de mercado y por una clientela más influenciada por la innovación. Normalmente las empresas fracasan al intentar implantar nuevas tecnologías, o sufren amenazas relacionadas a la ciberseguridad. Hoy en día muchas industrias se están reinventando como, por ejemplo: áreas de la salud, moda, agropecuaria. Además, tecnologías como el internet de las cosas IoT son un ejemplo de soluciones accesibles (Do et al., 2023).

El internet de las cosas llega como una medida revolucionaria para facilitar el control de objetos haciendo uso de sensores. Podemos verlo en la cotidianidad de nuestro hogar como, por ejemplo: al prender el televisor usando el control remoto (Berrío y Sánchez, 2024)**.** Esta tecnología se ha extendido a las PYMES, donde según Garibello et al. (2021), optimiza desde logística, inventario, cultivos, y otros servicios. Sin embargo, el IoT esconde una doble cara: sus beneficios versus las amenazas por falta de estandarización, actualizaciones o desconocimiento. Por ello, la implementación requiere cuidado extremo y soluciones emergentes para protegerse. Este estudio analiza precisamente esas vulnerabilidades y respuestas efectivas para PYMES.

Las PYMES son especialmente vulnerables porque cuentan con equipos TI muy reducidos o muchas veces su personal está poco capacitado. Generalmente los dispositivos IoT no reciben actualizaciones automáticas y quedan en el olvido. Esto genera vulnerabilidades explotadas por los atacantes como: falta de parches de

seguridad, contraseñas débiles, encriptación insuficiente o puertos abiertos. Además, la falta de segmentación de red, conecta todos los dispositivos IoT con servidores y bases de datos que guardan información sensible. Los errores humanos y amenazas internas completan el panorama (Quintero et al., 2020).

Según Palo Alto Network (2020), la combinación de falta de visibilidad, planificación y herramientas inadecuadas convierte a estas empresas pequeñas o medianas en bombas de tiempo. Pues un ataque exitoso puede llegar a detener operaciones, robar datos sensibles como datos bancarios o convertir dispositivos en botnets. Por todo ello, una gestión cuidadosa de la seguridad resulta imprescindible para prevenir. Entre las vulnerabilidades más comunes destacan algunas como: falta de actualizaciones, contraseñas débiles o predeterminadas, encriptación insuficiente, sin segmentación de red, errores humanos (Jumbo et al., 2023).

Estas traen consecuencias muy graves a su paso de concretarse, como Los plasmados en la Tabla 1: Ataques físicos, ataques de reconocimiento, denegación de servicios DDoS, ataques de acceso, ciberdelitos, ataques destructivos, minería de datos, ciber espionaje, interceptación, rastreo, ataques basados en contraseña. Todos provocan interrupción operativa, secuestro o robo permanente de datos y responsabilidad legal para la empresa en caso de afectar a los clientes. En PYMES, estas consecuencias suelen ser devastadoras por su limitada capacidad de recuperación. La tabla elaborada resume claramente esta realidad (Msgna, 2022).

Ante todas estas amenazas y vulnerabilidades surgen soluciones emergentes. Entre algunas de las destacadas tenemos: la arquitectura zero trust, que trata de desconfiar de cualquier dispositivo que se conecte; Otra es la capacitación del personal de TI

para evitar tener tantas puertas abiertas a ataques; También está la autenticación usando blockchain de manera descentralizada; La inteligencia artificial es otra solución que de la mano de Deep Learning y Machine Learning para detectar amenazas antes de que ocurran; El monitoreo constante; La encriptación cuántica busca proteger de ataques cuánticos con métodos como distribución de llaves; Y la segmentación de redes para separar los dispositivos de los servidores (Rosin et al., 2024).

Se puede ver en la Tabla 2, para evaluar las soluciones emergentes propuestas, donde cada solución fue evaluada en escala del 1 al 10 según los parámetros de eficacia, accesibilidad, escalabilidad e innovación. La solución de mayor puntuación en la tabla fue herramientas en la nube con monitoreo continuo con un 8.5/10, seguido de arquitectura zero trust e IA empataron en 8.25/10. Luego con puntajes 6.25/10 y 6.75/10 quedaron las soluciones de capacitación del personal, blockchain y al final quedo la encriptación cuántica con puntaje de 5.75/10. Con esto el análisis de una solución emergente en IoT para PYMES es más claro.

Con los datos obtenidos de las fuentes de investigación se pudo revelar que cada solución tenía su área para destacar. Por ejemplo: la de herramientas en la nube y monitoreo contante según Amazon AWS (2025) y Microsoft (2025), reduce un 75% aproximadamente del tiempo de detección, mientras que la capacitación del personal reducía un 40% de las brechas según Verizon (2024). Pero también la ciberseguridad con las soluciones emergentes en las PYMES va más allá de lo tecnológico, pues requiere esfuerzo colaborativo humano es decir trabajo en equipo. Por ello usar planes de contingencia, auditorías periódicas y cumplimiento ISO 27001/NIST son fundamentales.

Los resultados de la tabla comparativa nos arrojan que todas las soluciones tienes un buen grado de eficiencia, unas más que otras, la mayor diferencia se vio en la accesibilidad debido a que el costo de algunas soluciones es muy alto algo no viable para aplicarse en una PYME, como el caso de la encriptación cuántica con valores exorbitantes de implementación, pero con una eficiencia mayor a todas las demás. Sin embargo, las que quedaron con menor puntaje son más accesibles, pero no tan escalables e innovadoras; Sabiendo escoger las soluciones podemos hasta protegernos de manera económica solo capacitándonos en algunos campos, por ejemplo, siguiendo Normativas de riesgos como las planteadas por el NIST o la ISO 27001.

Finalmente se concluyó, que la tecnología avanza y los atacantes también, pero las soluciones emergentes evolucionan más rápido. La IA con el Machine Learning, Deep Learning, blockchain y la encriptación cuántica tienen un campo muy amplio por explorar y mejorar. Las PYMES que adopten hoy monitoreo en la nube junto con Zero Trust y capacitación del personal constante estarán preparadas para futuras amenazas. Cabe recalcar que la seguridad no es un gasto, más bien debe verse como una inversión que genera continuidad del negocio. Un IoT seguro y sostenible es posible incluso para la PYME más pequeña. Solo requiere planificación, conciencia y uso inteligente de herramientas accesibles. Así, el internet de las cosas ya no será una amenaza y se convertirá en un aliado.

Metodología

La metodología implementada fue de carácter documental bibliográfica, sin un área de delimitación geográfica especifica. Se reviso diferentes fuentes confiables enfocadas

al tema de la seguridad del internet de las cosas en el entorno de las PYMES o pequeñas empresas con el objetivo de estudiar sus vulnerabilidades y soluciones emergentes. Este enfoque permitió estudiar y mostrar las mejores soluciones ante las vulnerabilidades posibles en el internet de las cosas, basándose en teoría publica y actualiza de distintos puntos de internet.

Población, Muestra y Muestreo

No existe una población gentilicia, pero si una población de estudio que incluye fuentes académicas enfocadas al tema de la seguridad en el internet de las cosas y su doble acción sobre las pequeñas empresas, esta abarca libros y artículos científicos de revistas que se encuentren el rango de los últimos 5 años de publicación. Se uso una muestra por afinidad donde se seleccionaron paginas Y publicaciones de organismos de confianza como: NIST, IEEE Xplore, ScienceDirect y ResearchGate.

Variables de Estudio

Las variables que se analizaron en este proyecto fueron: 1) Vulnerabilidades: enfocada a sus puntos débiles al ser utilizados en empresas en crecimiento y 2) Soluciones: que se enfoca en cómo evitar que esos puntos débiles se conviertan en un perjuicio de alto nivel en la empresa. del internet de las cosas en las PYMES.

Métodos y Técnicas

Se uso un método sistemático de investigación bibliográfica, donde se siguió una estructura que cuenta inicialmente con la búsqueda de fuentes confiables usando la técnica de investigación bibliográfica, seguido por la selección del temario con el que contara el artículo, luego la conceptualización de los temas seleccionados usando las

fuentes seleccionadas, para finalmente evaluar los resultados obtenidos y concluir dando los resultados del estudio.

Métodos de Análisis

El análisis utilizado en los resultados fue de carácter cualitativo, usado para la interpretación personal y crítica de los datos en base a la información obtenida de las fuentes de investigación. Se hizo uso de tablas comparativas de las mejores soluciones, datos tomados de otras investigaciones citadas. Estos datos fueron presentados en la tabla de los resultados.

Internet de las cosas

El internet de las cosas llega como una medida revolucionaria para facilitar el control de objetos haciendo uso de sensores. Podemos verlo en la cotidianidad de nuestro hogar como por ejemplo al prender el televisor, prender el aire acondicionado o abrir la puerta del garaje en todos esos casos haciendo uso del control remoto. Esto se ha extendido con el pasar de los años y son cada vez más los objetos que pueden ser controlados de manera simple a través de pequeños sensores que pueden ser de: luz, temperatura, humedad, movimiento entre muchos más (Berrío y Sánchez, 2024)**.**

Internet de las cosas aplicado a las PYMES

Según lo planteado por Garibello et al. (2021), las PYMES tienden a crecer mucho en países con mayor poder adquisitivo y son cada vez más abiertas a la integración de nuevas tecnologías, aun en Latinoamérica donde la economía es menor, ya se ve cada vez más negocios interesados en un ecosistema digital. En el artículo se pronuncia que ya es una realidad en crecimiento el uso del internet de las cosas en las PYMES, su uso va desde gestión inteligente ya sea de logística o inventario, como también es

usado en pymes de agricultura o manufactura para monitorización y optimización áreas o maquinarias, y hasta en salud y empresas de servicio para mejorar su eficiencia en procesos o en consumo energético.

La doble cara del internet de las cosas en la PYMES

El internet de las cosas, así como trae muchos beneficios, también tiene problemas que hay que tomar en cuenta antes de su implementación en las PYMES, estas amenazas nacen de muchos factores como la falta de estandarización de protocolos que arrastra consigo vulnerabilidades. El desconocimiento de los dueños de los negocios lleva a que no tomen acciones para proteger estos dispositivos y quedan expuestos al robo de información u otros ataques. Se concluye que su funcionamiento no es garantizado se necesita una implementación cuidadosa y tomar en cuenta que si existen soluciones emergentes para protegerse (Quintero et al., 2020).

Principales Vulnerabilidades del internet de las cosas en entornos PYMES

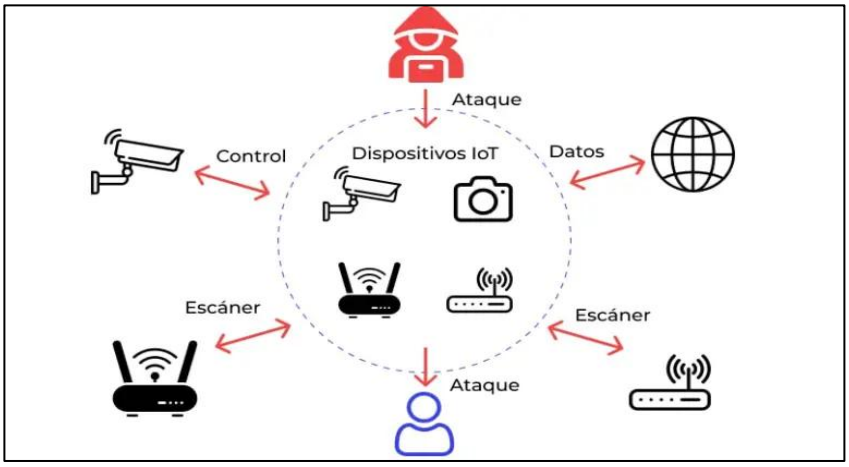

Figura 1

Esquema de ataques en IoT

Fuente: Cualquier ingreso e salida de una red, cuenta como ataque. Fuente: (Wallarm, 2025)

La seguridad es una pieza clave en el internet de las cosas, los encargados de la ciberseguridad de estos sistemas la tienen cada vez más difícil, por el aumento de dispositivos digitales y además los atacantes de los sistemas buscan vulnerabilidades tanto en hardware, software y hasta en los miembros de las empresas, para hacer daños que causan pérdidas económicas graves. Existen una gran variedad de ataques que van desde rasomware que son aquellos basados en el secuestro de información, otros como el phishing que son ataque que buscan robar datos de acceso como contraseñas y los más comunes que son los accesos no autorizados que se dan por explotar vulnerabilidades (Jumbo et al., 2023)**.**

Entre las vulnerabilidades más conocidas en el internet de las cosas enfocado al sector PYMES podemos destacar algunas como:

- Falta de actualizaciones o parches no actualizados: Las PYMES por lo general cuentan con equipos de TI muy reducidos, y debido a que muchos dispositivos no reciben actualizaciones automáticas, muchos olvidan actualizar o lo dejan pasar. Esto causa vulnerabilidades que son explotadas por los atacantes (Quevedo, 2024)**.**
- Datos débiles de identificación (contraseñas) o ataques forzados: El uso de credenciales muy genéricas o el uso de datos como fechas de cumpleaños o nombres facilitan los ataques, también los ataques cuánticos pueden romper contraseñas cortas y fáciles para acceder a datos sensibles (Jumbo et al., 2023)**.**
- Encriptación débil y comunicación expuesta: La falta de estandarización de protocolos lleva a hacer uso de protocolos inseguros, también el escaso

conocimiento lleva a dejar puertos abiertos por donde pueden entrar visitantes inesperados. También el uso de encriptaciones débiles o sin cifrado lleva al mismo camino (García et al., 2025).

- Falta de Segmentación de Red: el uso de los dispositivos en la misma red que los servidores y bases de datos. Puede comprometer la información de toda la empresa (INCIBE, 2020).
- Errores Humanos y amenazas internas: Empleados o personas sin el conocimiento necesario hace configuraciones y deja puertas abierta a los ciber delincuentes o personas mal intencionadas hacen configuraciones no permitidas por falta de supervisión (Instituto federal de telecomunicaciones, 2022).

¿Por qué las PYMES son vulnerables al internet de las cosas?

La razón principal de las vulnerabilidades en el internet de las cosas es la falta de visión y planificación de parte de las PYMES al momento de gestionar los dispositivos conectados. Estos pequeños negocios muchas veces cuentan con departamento TI muy reducidos, personal poco capacitado que carece de capacidades efectivas; Esto impide que la gestión de la seguridad no sea su punto fuerte. Entre las razones existente de los sistemas tradicionales de seguridad implementados por estos negocios en crecimiento son: estos dispositivos IoT no reciben actualizaciones y sus sistemas operativos con el tiempo se tornan obsoletos, por lo que ellos equipos TI de las empresas suelen darles mantenimiento como limpieza, pero se olvidan de mantener sus sistemas operativos por lo que se vuelven vulnerables. La combinación de la falta de visibilidad, una planificación y herramientas inadecuadas es la razón por

la que las PYMES que usan el internet de las cosas, muchas veces se convierten en bombas de tiempo de la seguridad (Palo Alto Networks, 2020)**.**

1.1 Consecuencias de un ataque exitoso al internet de las cosas

Los ataques destinados al internet de las cosas arrastran consecuencias que para las empresas que van en crecimiento suelen ser un duro golpe, entre algunas de los las consecuencias devastadoras están:

- **Interrupción de las operaciones de la empresa:** puede detener por completo el trabajo del negocio por tiempos indefinidos, esto lleva a perdidas económica inmediatas (Waqdan et al., 2025)**.**
- **Secuestro o robo permanente de datos importantes:** puede ir desde datos sensibles de los clientes, como a datos privados de la empresa y en casos perores datos bancarios; Todos estos afectarían negativamente la reputación de la empresa (Msgna, 2022).
- **Denegación de servicios DDoS y botnets en redes IoT:** pueden darse secuestros de objetos de la empresa, para realizar acciones indebidas, y causar pérdidas económicas, además de hacer a la empresa responsable de cualquier acción (Waqdan et al., 2025)**.**

Basándonos en los datos propuestos por Msgna (2022), se elaboró una tabla donde se aprecian las vulnerabilidades, los ataques de seguridad más comunes y los ataques de privacidad.

Tabla 1

Vulnerabilidades en Iot

Marco de referencia del riesgo	IoT (Internet de las Cosas)
Vulnerabilidades del IoT	Seguridad física insuficiente Dispositivos con energía restringida
Ataques de seguridad del IoT	Ataques físicos Ataques de reconocimiento Denegación de servicios (DDoS) Ataques de acceso Ciberdelitos Ataques destructivos
Ataques a la privacidad del IoT	Minería de datos Ciber espionaje Interceptación Rastreo Ataques basados en contraseña

Fuente: Elaboración propia basada en (Msgna, 2022)

Soluciones emergentes: innovaciones para fortalecer la seguridad en IoT

Con el tiempo y ante todas las nuevas maneras de atacar estos sistemas, han ido apareciendo gradualmente soluciones; Unas más accesibles que otras, pero la gran mayoría con una eficacia alta, algunas de estas se muestran a continuación:

- **Architectura Zero Trust:** Este modelo sigue tiene la ideología de no confiar en ningún dispositivo que sea conectado dentro de la red, sin que este inicialmente sea verificado. Puede ser aplicado mediante configuraciones de red o mediante herramientas en la nube que la ofrecen como servicio. Se vuelve una herramienta muy necesaria en entornos del internet de las cosas, por lo que cualquier dispositivo es tratado como enemigo hasta que demuestre lo contrario (Ismail y El-Gawad, 2023).

- **Capacitación y concienciación en ciberseguridad:** Los empleados son parte fundamental en las PYMES y en la seguridad los equipos de TI, junto con los administradores son parte clave para evitar amenazas ya mencionadas como el rasomware y el phishing. La capacitación contante sobre actualizaciones, protección de puertos, segmentación de red, firewalls es importante para formar un entorno más seguro (García, 2025).
- **Blockchain para autenticación descentralizada:** Esta solución propone usar blockchain (registro descentralizado seguro), para proteger la información de autenticación. Al esta no estar almacenada de manera centralizada será muy difícil llegar a esta. Este proceso ya no se haría desde un solo servidor, sino que es ejecutado de forma descentralizada por todos los nodos de la red de la empresa (Kanjanapruthipong y Boonkrong, 2025).
- **Inteligencia Artificial:** Esta herramienta proporciona una seguridad robusta ya que es adaptable a distintos tipos de amenazas; Ejemplo: Deep Learning para detecciones precisas usando redes neuronales, Machine Learning cuando se busca analizar cantidades grandes de datos, blockchain para monitorear los comportamientos, entre otras funciones. Y no es todo la IA es un motor de gran poder y un potencial crecimiento que permite identificar infiltraciones, malware, fraudes y hasta gestionar amenazas. Su desventaja fuerte es el precio de acceder a ella (Rosin et al., 2024)**.**
- **Monitoreo continuo y herramientas en la nube:** El monitoreo contaste es una medida eficiente ya que la gran mayoría de amenazas nacen o pueden ser identificadas de esa forma. Esta función es muy común en herramientas en la

nube que ofrecen este servicio y muchos otros. Entre algunas herramientas se puede mencionar: IBM QRadar, Microsoft Azure Sentinel y Darktrace. Muchas implementan IA para mejorar procesos de monitorización, identificación, y control (García, 2025).

- **Encriptación cuántica:** El uso de algoritmos cuánticos para descifrar sistemas actuales es impresionante, pero a su vez nacen soluciones de seguridad cuántica como distribución de claves QKD y QKR que detecta inmediatamente intercepciones. La criptografía cuántica llega a remplazar las criptografías tradicionales como shor y grover, que terminan siendo débiles ante esta nueva tecnología ya que implementa los ataques de prueba y error (Rosin et al., 2024)**.**
- **Segmentación de redes:** La segmentación de redes es una técnica que busca dividir la red en partes más pequeñas para mejorar su administración y seguridad. Estas hacen uso de switches, para manejar el ancho de banda y por otro lado usa los firewalls filtran todo lo que entra y sale según los protocolos que se configuren. En el internet de las cosas es muy normal la segmentación usando VLAN, para aislar los dispositivos IoT en una red aparte. En segmentaciones más avanzadas se hace uso de diodos de datos y dispositivos IPS, esto para una protección más especializada (García, 2025).

Hacia un internet de las cosas seguro y sostenible para Pymes

La ciberseguridad en las PYMES va más allá de lo tecnológico, sino que se mete también en lo humano, las empresas afrontan las amenazas con esfuerzo colaborativo, es decir que para afrontar estos retos se necesita de planes de contingencia para dar respuesta a las amenazas que se aparezcan en el camino,

además de auditorías y regirse a normativas como la ISO 27001 las propuestas por el NIST. Todo esto de la mano de las medidas de seguridad que mejor se acomoden a la economía de la empresa como puede ser la arquitectura Zero Trust, la segmentación de redes y uso de firewalls. Y para PYMES con mayor poder económico están las herramientas en la nube que ofrecen más eficiencia (Jumbo et al., 2023)**.**

Resultados y Discusión

Evaluación de soluciones emergentes

Se usarán parámetros para calificar las soluciones emergentes previamente estudiadas y cada punto será medido en una escala de 1-10 siendo 1 la menor calificación y 10 la más alta; Estos parámetros son:

- Eficacia, para medir su reducción de brechas que genera la solución frente las amenazas.
- Accesibilidad, que califica la posibilidad adquisitiva sobre la solución sabiendo que hablamos de PYMES.
- Escalabilidad, califica su crecimiento tanto a futuro como a medida de aumento de dispositivos.
- Innovación, califica si la tecnología es relativamente nueva o es un nuevo enfoque de una tecnología que ya tiene tiempo.
- Resultados, resume lo más destacado de la solución emergente.

Finalmente, esta total y fuente, el total es la calificación final que obtuvo cada solución y la fuente es la cita bibliográfica de donde se obtuvo la información plasmada.

Tabla 2

Evaluación de soluciones emergentes en ciberseguridad para IoT.

Solución Emergente	Eficacia (1-10)	Acceso (1-10)	Escalable (1-10)	Innovación (1-10)	Resultado	Total
Arquitectura zero trust	**9** (detiene la mayoría de ataques laterales)	**7** (requiere reconfiguración de red, pero las herramientas están disponibles)	**9** (funciona igual de bien para 5 o 500 dispositivos)	**8** (enfoque moderno, no una tecnología nueva)	Reducción del 90% en ataques laterales.	**8.25**
Plataformas en la nube, monitoreo continuo	**8** (alta detección de anomalías)	**8** (herramientas accesibles- Azure IoT Defender, AWS IoT Device Defender)	**10** (diseñadas para crecer continuame nte)	**8** (Monitoreo automatizado con ML/IA)	Reducción del 75% del tiempo medio de detección.	**8.5**
Encriptación cuántica	**10** (seguridad criptográfic a máxima)	**1** (costosa/deman da infraestructura)	**2** (tecnología en fase experimenta l)	**10** (tecnología disruptiva)	Inmunidad teórica a futuros ataques.	**5.75**
Blockchain para autenticación descentralizad a	**7** (resistenci a a ataques Man-in-the-Middle)	**3** (requiere infraestructura distribuida)	**6** (la latencia puede ser un problema a gran escala)	**9** (Modelo de autenticación muy innovador)	Inmutabilida d del registro de identidades	**6.25**
IA Inteligencia Artificial	**9** (eficacia en detección de ataques de día cero)	**6** (Requiere hardware potente o servicios costosos)	**9** (escala bien en la nube)	**9** (motor clave de la nueva seguridad IoT)	Precisión de detección del 95% de malware desconocido .	**8.25**
Capacitación y concientizació n en ciberseguridad	**6** (reduce el error humano)	**10** (bajo costo: cursos, webinars)	**8** (fácilmente replicable para nuevos empleados)	**3** (es una práctica fundamental, no una innovación tecnológica)	Reducción del 40% en incidentes causados por error del humano.	**6.75**
Segmentación de redes	**9** (excelente contención de ataques)	**7** (requiere configuración de VLANs y Firewalls)	**8** (la complejidad aumenta con el número de segmentos)	**5** (técnica clásica, pero esencial para IoT)	Aislamiento del 100% de dispositivos IoT.	**7.25**

fuente: Elaboración Propia basada en: (Gartner, 2025), (Amazon AWS, 2025), (microsoft, 2025), (Liu et al., 2024), (Li et al., 2018), (Reis y Serôdio, 2025), (Verizon, 2024), (Al-Ateeq, 2021)

La mejor solución emergente para la seguridad IoT en PYMES

Analizando los datos obtenidos del estudio realizado se puede observar que destacan 3 soluciones emergentes para la seguridad del internet de las cosas en las PYMES. La que obtuvo mayor puntaje con 8.5/10 fue la de monitoreo constante y herramientas en la nube, por su alta detención de amenazas, sus planes accesibles para las pequeñas empresas, posibilidad de crecimiento altísimo, buena innovación con su motor de IA; todo esto la hace una herramienta eficiente para las PYMES.

Otras dos soluciones emergentes con un puntaje relativamente bueno de 8.25/10 fueron la arquitectura zero trust, que tiene mayor eficiencia y escalabilidad que las herramientas en la nube, pero es menos accesible debido a que requiere ardua configuración y por otro lado está la inteligencia artificial que su mayor defecto es la accesibilidad a todos sus servicios, si bien servicios como identificación están disponibles en herramientas en la nube. Hay otros servicios que tienen costos más elevados.

Pero, aunque no obtuvieron buenas calificaciones hay que destacar a la segmentación de redes, que es una solución muy buena cuando los recursos son escasos, no es innovadora, pero es clásica y funcional. La capacitación del personal, es una solución simple, pero con resultados inmediatos, de gran aporte para las empresas y finalmente la encriptación cuántica, es la más segura de todas y la más innovadora pero su precio de implementación es excesivo para ser una PYME.

Conclusiones

Como conclusión, queda claro que esta no es una directriz de que solución es la definitiva, más bien eso va depender de muchas cuestiones como las necesidades de

la empresa, el presupuesto previsto a invertir en la seguridad, la capacidad de su departamento de TI y muchos otros factores que influyen en la elección idónea. Mas bien son recomendaciones y sugerencias de las soluciones propuestas en este artículo.

Se puede concluir que se pueden implantar soluciones eficientes aun sin invertir un centavo, solo con una organización mejor basada en normas como la ISO 27001 o las propuestas por el NIST para gestionar los riesgos. Además, se pueden hacer capacitaciones y configuraciones como segmentación de red con Vlan y firewalls para filtrar las entradas y salidas.

Finalmente se concluye que la tecnología sigue avanzando y así como avanzan los atacantes las soluciones también son cada vez más precisas, la IA con sus distintas ramas como: machine learning, deep learning y la encriptación cuántica. Todas tienen un campo muy amplio aun por explorar.

Referencias Bibliográficas

Al-Ateeq, I. (2021). *Design Secure Network Segmentation Approach.* SANS. https://sansorg.egnyte.com/dl/kPFQdgrBhfKk

Amazon AWS. (2025). *Amazon AWS*. Amazon AWS: https://www.gartner.com/reviews/market/zero-trust-network-access

Berrío, J. y Sánchez, R. (2024). *Internet de las cosas .* Mexico: RED Descartes. https://proyectodescartes.org/iCartesiLibri/PDF/IoT.pdf

Do, A., Villagra, A. y Pandolfi, D. (2023). Desafíos de la Transformación Digital en las PYMES. *ICT UNPA*, 30.

https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://dialnet.unirioja.es/descarga/articulo/8901467.pdf&ved=2ahUKEwjQoJe43OCQAxWeSzABHdPCG0kQFnoECBgQAQ&usg=AOvVaw3N2YEXG6TkhhcdO0axnYPc

García, H. (2025). Ciberseguridad en la era del IoT: Riesgos, desafíos y soluciones para la protección de redes domésticas y empresariales. *Revista de ingenieria y futuro*, 15. https://www.researchgate.net/publication/391585005_Ciberseguridad_en_la_era_del_IoT_Riesgos_desafios_y_soluciones_para_la_proteccion_de_redes_domesticas_y_empresariales

García, H., Nepas, A. y Araujo, H. (2025). Ciberseguridad en la era del IoT: Riesgos, desafíos ysoluciones para la protección de redes domésticas yempresariales. *FIC FUTURE*, 15. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://editorialscientificfuture.com/index.php/riif/article/download/119/311/1005&ved=2ahUKEwiu2tDXytyQAxVVRDABHX6ZFWcQFnoECBoQAQ&usg=AOvVaw3KJFXcv42ljfWSSQ2LQuhJ

Garibello, J., Guerrero, L. y Amado, W. (2021). La IoT una nueva ventana de oportunidad para pymes latinoamericanas en tiempos de covid-19. *Revista RETO*, 15. https://www.researchgate.net/publication/367940969_La_IoT_una_nueva_ventana_de_oportunidad_para_pymes_latinoamericanas_en_tiempos_de_la_covid-19

Gartner. (2025). *Gartner* . Gartner : https://www.gartner.com/reviews/market/zero-trust-network-access

INCIBE. (2020). *Seguridad en la instalación y uso de dispositivos IoT.* España: Gobierno de España. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-de-seguridad-iot.pdf

Instituto Federal de Telecomunicaciones, (2022). *Código de mejores prácticas para la ciberseguridad de los dispositivos iot.* Mexico: Instituto federal de telecomunicaciones. https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

Ismail, M. y El-Gawad, A. (2023). Revisiting Zero-Trust Security for Internet of Things. *SMIJ*, 8. www.researchgate.net/publication/377021858_Revisiting_Zero-Trust_Security_for_Internet_of_Things

Jumbo, E., Llumiquinga, J., Uyaguari, F., Tenezaca, A., Pazmiño, L. y Rivera, R. (2023). Un breve Análisis de Vulnerabilidades en dispositivos IOT en Ecuador. *Ciencia Latina Revista Científica Multidisciplinar*, 15. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://ciencialatina.org/index.php/cienciala/article/download/5763/8722/&ved=2ahUKEwiu2tDXytyQAxVVRDABHX6ZFWcQFnoECCIQAQ&usg=AOvVaw0ad70_70aH_g-1HpkMRm-8

Kanjanapruthipong, W. y Boonkrong, S. (2025). Blockchain-Based Decentralised Authentication in Closed Environments. *Institute of Digital Arts and Science*, 15. https://www.mdpi.com/1999-5903/17/3/98

Li, D., Deng, W., Peng, W. y Gai, F. (2018). A Blockchain-based Authentication and Security Mechanism for IoT. *IEEE*, 20. https://www.researchgate.net/publication/328247073_A_Blockchain-Based_Authentication_and_Security_Mechanism_for_IoT

Liu, T., Ramachandran, G. y Jurdak, R. (2024). Post-Quantum Cryptography for Internet of Things. *arxiv*, 13. https://arxiv.org/pdf/2401.17538

Microsoft, (2025). *microsoft*. microsoft: https://www.microsoft.com/es-es/security/business/endpoint-security/microsoft-defender-iot

Msgna, M. (2022). Anatomía de los ataques a sistemas IoT: revisión de ataques, impactos y contramedidas. *oaepublish*, 16. https://www-oaepublish-com.translate.goog/articles/jsss.2022.07?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc&_x_tr_hist=true

Palo Alto Networks. (2020). *Informe de amenazas IoT.* Palo Alto Networks. https://info.smartekh.com/hubfs/IoT/Informe%20de%20Amenazas%20IoT%202020.pdf

Quevedo, A. (2024). *Guía sobre Seguridad en Dispositivos IoT.* España: Ministerio del interior. https://occ.ses.mir.es/publico/occ/dam/jcr:a97a3ac9-1a92-4af0-a5c0-3ac8557244ba/Gu%C3%ADa%20sobre%20Seguridad%20en%20Dispositivos%20IoT.pdf

Quintero, D., Silva, E., López, K., Mojica, K., Casadiego, S. y Mateus, J. (2020). Vulnerabilidad en la seguridad del internet de las cosas. *Mundo Fesc*, 19. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://dialnet.unirioja.es/descarga/articulo/10244411.pdf&ved=2ahUKEwjMltTZxtyQAxVtSTABHZnYEAgQFnoECBoQAQ&usg=AOvVaw2UG2jCUeF1_G3Q3G0Prxi9

Reis, M. y Serôdio, C. (2025). Edge AI for Real-Time Anomaly Detection in Smart Homes. 20. https://www.researchgate.net/publication/390924039_Edge_AI_for_Real-Time_Anomaly_Detection_in_Smart_Homes

Rosin, Z., Pujalte, D. y Bolatti, D. (2024). Tecnologías Emergentes para la Ciberseguridad de dsipositivos IoT. *UTN*, 5. https://sedici.unlp.edu.ar/handle/10915/177556

Verizon, (2024). *2024 Data BreachInvestigations Report.* Verizon. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

Wallarm, (2025). *Wallarm*. Wallarm: https://lab.wallarm.com/what/ataque-de-iot/?lang=es

Waqdan, M., Louafi, H. y Mouhoub, M. (2025). Security risk assessment in IoT environments: A taxonomy and survey. *ScienceDirect*, 16. https://pdf.sciencedirectassets.com/271887/1-s2.0-S0167404825X00043/1-s2.0-S0167404825001452/main.pdf?X-Amz-Security-

Token=IQoJb3JpZ2luX2VjEOP%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaCXVzLWVhc3QtMSJIMEYCIQD15Cz8Vo%2B4YtTYYWcz7b1UYn0GvuViRvLqklW8XxsuhAIhALVb9l33f0