Revista Ciencia, Tecnología e Innovación en Ingeniería y Arquitectura
1*(1)* (2025), pp. 17-24
Facultad de Ingeniería y Arquitectura
Universidad de El Salvador
https://revistas.ues.edu.sv/index.php/cti-fia

CTI-FIA

Artículo | Article

Alternativas de Seguridad de Datos en la Red Local para Medianas y Pequeñas Empresas

Local Network Data Security Alternatives for Small and Medium-Sized Enterprises

Cristhian Alberto Buendía Ardón[1,2], Carlos Osmín Pocasangre Jiménez[1,3]

1 Facultad de Ingeniería y Arquitectura, Universidad de El Salvador
2 https://orcid.org/0009-0007-4997-389X
3 https://orcid.org/0000-0002-7463-9873

Correspondencia: ***carlos.pocasangre@ues.edu.sv***
Enviado: ***29 de agosto de 2025*** Aceptado: ***23 de octubre de 2025***

PALABRAS CLAVE

Equipo Gateway
Seguridad informática
Laboratorios
ISO/IEC 27001:2022
NIST SP 800-53

RESUMEN

Este artículo se ha llevado a cabo debido a que la ciberseguridad es la práctica de proteger sistemas, redes y datos del acceso no autorizado, así como del uso, divulgación, interrupción, modificación o destrucción. En pocas palabras, es la seguridad de todo lo que está conectado a Internet. Nuestro país ha reconocido la importancia de la ciberseguridad y ha implementado diversas iniciativas para proteger la infraestructura crítica y los datos de sus ciudadanos. Algunas de estas iniciativas incluyen: la Estrategia Nacional de Ciberseguridad, los Centros de Operaciones de Seguridad (SOC) y los programas de capacitación. Las pequeñas y medianas empresas en nuestro país se ven expuestas a este tipo de problemas y no tienen la capacidad ni el acceso a estos recursos; por lo tanto, el presente trabajo tiene como finalidad proponer alternativas de bajo costo. Se pretende en el documento proporcionar las mejores propuestas en ciberseguridad, reflejando las mejores prácticas comunes disponibles públicamente, derivadas de un consenso entre expertos internet superiores a 50 Mbps, integrarse con otros sistemas y poder instalarlo y configurarlo, mostrando su generalidad y funcionalidad, así como su descripción. Se presentó el uso del equipo de protección para la red de seguridad, así como su explicación y su concientización sobre su importancia, dirigidos a pequeñas y medianas empresas.

KEYWORDS

Gateway hardware
Cybersecurity
Laboratory
ISO/IEC 27001:2022
NIST SP 800-53

ABSTRACT

This article has been carried out because Cybersecurity is the practice of protecting systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. In short, it is the security of everything connected to the internet. Our country has recognized the importance of cybersecurity and has implemented several initiatives to protect its citizens' critical infrastructure and data. These initiatives include the National Cybersecurity Strategy, Security Operations Centers (SOCs), and training programs. Small- and medium-sized enterprises in our country are exposed to these problems and lack the capacity or access to these resources; therefore, the present work proposes low-cost alternatives. The paper aims to provide best-in-class cybersecurity proposals that reflect publicly available standards and best practices, resulting from consensus among international experts with a wide range of skills, Knowledge, and experience in the field. Additional guidance for implementing the requirements of ISO/IEC 27001:2022 and NIST SP 800-53, as defined by Information Security Management Systems (ISMS), will also be added. Adoption will benefit the company by increasing its resistance to cyberattacks. Preparation for new threats, Integrity, confidentiality, and availability of information, Security on all media, Protection throughout the company, and Cost savings. The proposed equipment must handle internet speeds exceeding 50 Mbps and be integrated with other systems, with installation and configuration details provided to demonstrate its general functionality. The use of protective equipment for the safety net, its explanation, and awareness of its importance are targeted at small and medium-sized enterprises.

INTRODUCCIÓN

En la era digital actual, la protección de la información se ha convertido en un pilar fundamental para el éxito y la sostenibilidad de las empresas. Las medianas y pequeñas empresas (PYMES) en El Salvador, aunque son el motor de la economía nacional, enfrentan desafíos significativos en materia de seguridad de datos debido a la falta de recursos, de conocimiento técnico y de estrategias adecuadas para proteger sus redes locales. Este contexto ha generado un aumento de los riesgos asociados a ciberataques, pérdida de información confidencial y vulneración de la privacidad, lo que puede tener consecuencias devastadoras para estas organizaciones.

Este artículo tiene como objetivo explorar y proponer alternativas viables y accesibles de seguridad de datos para las PYMES en El Salvador, enfocándose en la protección de sus redes locales. Mediante el análisis de las amenazas cibernéticas más comunes, las vulnerabilidades presentes en estas empresas y las soluciones tecnológicas disponibles, se busca proporcionar un marco de referencia que permita a las PYMES implementar medidas de seguridad efectivas sin incurrir en costos excesivos. La relevancia de este estudio radica en su contribución al fortalecimiento de la resiliencia digital de las PYMES, un sector que, aunque vital para la economía, ha sido históricamente subestimado en su preparación frente a riesgos tecnológicos. Además, este trabajo pretende servir de guía práctica para empresarios, técnicos y tomadores de decisiones, ofreciendo recomendaciones adaptadas al contexto salvadoreño y a las particularidades de las empresas de menor escala.

En las siguientes secciones, se abordarán los fundamentos teóricos de la seguridad de datos, se analizarán las amenazas más recurrentes en el ámbito local y se presentarán alternativas de seguridad que combinen eficacia, facilidad de implementación y accesibilidad económica. Con este enfoque, se espera contribuir a crear un entorno digital más seguro y confiable para las PYMES en El Salvador.

METODOLOGÍA

La selección del equipo de seguridad informática, que constituye el núcleo central de esta investigación, se basó en un riguroso análisis preliminar que abarcó un amplio espectro de organizaciones. El objetivo fue establecer el nivel de madurez en ciberseguridad y determinar las principales vulnerabilidades del ecosistema empresarial. Este análisis inicial implementó criterios de evaluación específicos que incluían la naturaleza del sistema de seguridad interna ofrecido, la robustez de la infraestructura de hardware implementada y el nivel de conocimiento técnico sobre las medidas preventivas. De manera crucial, se investigaron la frecuencia y la tipología de los ciberataques experimentados, así como la efectividad de la protección de la red y de las políticas vigentes de limitación de acceso.

Los resultados de este análisis confirmaron que las PYMES son un objetivo desproporcionadamente vulnerable. En este sector, la limitación de recursos financieros y la ausencia de personal especializado incrementan significativamente la superficie de ataque, lo que dificulta la implementación y mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI) efectivo (ISACA, 2022)

Este diagnóstico condujo a la identificación de un caso de estudio crítico: una empresa que había experimentado múltiples incidentes de ciberseguridad con pérdidas financieras cuantificables, la cual era un bufete de abogados. Esta problemática sirvió de catalizador para seleccionar una solución técnica integral y escalable. La elección se decantó por un equipo Gateway con funcionalidad de Gestión Unificada de Amenazas (UTM), dada su capacidad intrínseca para consolidar múltiples funciones esenciales, como el firewall, la detección y prevención de intrusiones (IDS/IPS) y los servicios de VPN en un único dispositivo. Esta consolidación simplifica drásticamente el despliegue y la gestión en entornos PYME con escasos recursos.

Finalmente, el equipo fue seleccionado bajo el estricto criterio de compatibilidad y alineación con los principios y controles de la norma internacional ISO/IEC 27001:2022 (ISO , 2023). Este enfoque garantiza que la solución adoptada no solo sea técnicamente sólida, sino también operativa y legalmente coherente, promoviendo un modelo de seguridad basado en riesgos. El producto de esta investigación es un plan de mitigación completo que integra el hardware seleccionado con guías de implementación detalladas para su correcta instalación, configuración y operación. Este proceso culmina con la transformación del estado de seguridad de la PYME de un modelo meramente reactivo a uno proactivo, estandarizado y continuamente mejorable en la medida en que se resuelvan los problemas (Cleri, C. ,2007).

RESULTADOS

La elección del UniFi Cloud Gateway Fiber (UCG-Fiber) se fundamenta en su arquitectura de hardware y software, diseñada para ofrecer un nivel de seguridad empresarial a un coste accesible para las PYMES (Stewart, J. M., 2019; Delgado, R.,

2021). Este dispositivo actúa como la principal capa de defensa perimetral, destacando por su capacidad para integrar el control de acceso basado en roles (RBAC) y las funcionalidades avanzadas de segmentación de red mediante VLANs. Además de sus capacidades como firewall de inspección de estado, el UCG-Fiber facilita la implementación de controles tecnológicos (A.8 de la ISO 27001) al soportar túneles cifrados para IPSec VPN y SSL/TLS, cruciales para garantizar la confidencialidad de la información y permitir el teletrabajo seguro. Su gestión centralizada mediante el software UniFi Network permite una monitorización continua y la generación de alertas detalladas, lo cual resulta imprescindible en las fases de Verificación y Actuación del ciclo PDCA, asegurando que la gestión de endpoints y el cifrado cumplan con los requisitos normativos. La Figura 1 muestra un equipo UCG-FIBER con 4 puertos LAN, 1 puerto WAN y 2 puertos de entrada y salida de fibra.

Figura 1

Equipo UCG-FIBER con 4 puertos LAN, 1 WAN y 2 de entrada y salida de fibra

Nota. En la figura se observa un equipo Gateway en fibra óptica.

La justificación inicial para la selección del equipo UniFi Cloud Gateway Fiber (UCG-Fiber), si bien cumplía con los más altos estándares técnicos reflejados en la Declaración de Aplicabilidad (SoA) de la ISO/IEC 27001:2022, se vio comprometida por su elevado coste, lo que lo hacía inviable en la realidad presupuestaria de las PYMES. Esta limitación económica obligó a la investigación a optar por un equipo de menor gama que permitiera cumplir los controles esenciales de la norma. El dispositivo finalmente seleccionado para la implementación fue el UniFi Cloud Gateway Ultra (UCG-Ultra), como se muestra en la Figura 2. La fundamentación de esta elección radica en que el UCG-Ultra cumple cabalmente con los propósitos del SGSI para empresas medianas y pequeñas. Actúa como la principal capa de defensa perimetral, destacando por su balance entre coste, especificaciones de seguridad (control de acceso basado en roles y segmentación de red mediante VLANs) y velocidad de puerto, asegurando una solución UTM eficaz que permite la gestión de endpoints y la implementación de túneles cifrados (IPSec VPN y SSL/TLS) de manera eficiente, lo cual es imprescindible para la coherencia operativa y el cumplimiento normativo.

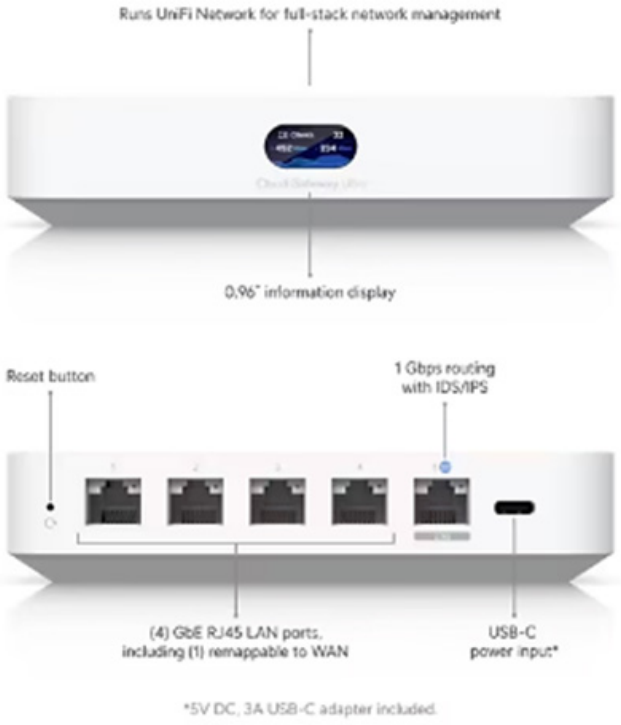
Como se puede observar en comparación con los equipos de las Figuras 1 y 2, este es un poco más pequeño y, por supuesto, es de menor precio, más accesible a su propósito: la seguridad de las empresas con un equipo de bajo costo.

Este equipo, UCG-Ultra, según su eslogan, es específicamente para pequeñas y medianas empresas, ya que ofrece características específicas, como la seguridad en sus puertos, bloqueo de aplicaciones, monitoreo en la red interna por usuario y VPN para equipos específicos o de búsqueda específica; todos optan por la seguridad de la red local.

Para asegurar la correcta adopción del SGSI por parte del personal de la PYME, se diseñaron seis guías de implementación consecutivas y metodológicas que cubren el ciclo completo de vida de la seguridad con el UCG-Ultra, desde el

Figura 2

Equipo UCG-Ultra con 4 puertos LAN y uno WAN



Nota. En la figura anterior se muestra el equipo Gateway utilizado.

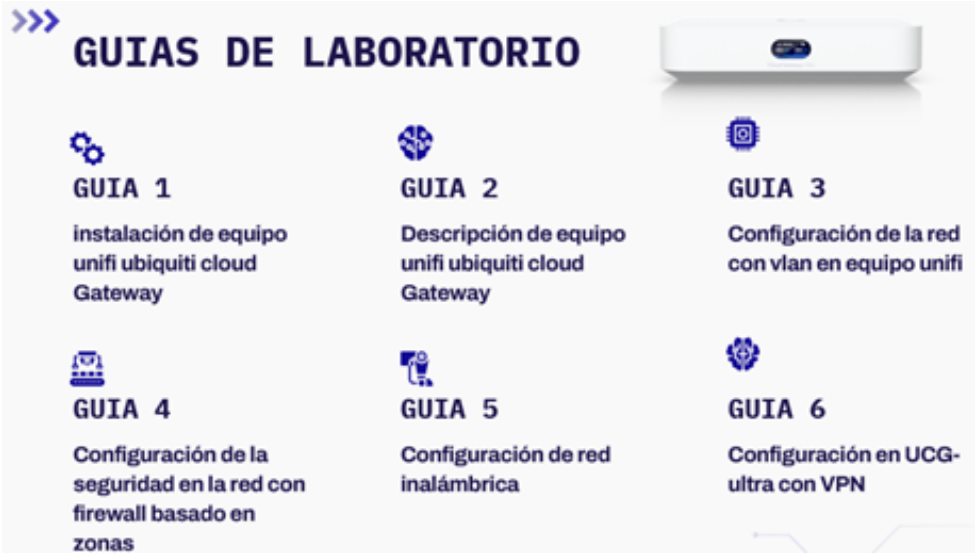
despliegue físico hasta la gestión de incidentes. Estas guías están estructuradas para mapear los controles de la ISO/IEC 27001:2022 a acciones concretas en el hardware (Buendía, 2025). En la Figura 3 se muestra una representación gráfica de las guías planteadas. La Guía 1 cubre la instalación y configuración inicial de red; la Guía 2 se centra en la implementación de las políticas de firewall y el filtrado de contenido para el control de acceso a la red (A.8.1 y A.8.5); la Guía 3 aborda la segmentación de red mediante VLANs, estableciendo zonas de confianza diferenciadas (A.8.20); la Guía 4 detalla la configuración de túneles VPN (IPSec y SSL/TLS) para la seguridad de las comunicaciones (A.8.24 y A.8.25); la Guía 5 se dedica a la monitorización y revisión de logs y alertas, fundamental para la fase de Verificación del PDCA; y, finalmente, la Guía 6 proporciona el protocolo de respuesta y actuación frente a incidentes de seguridad, cerrando el ciclo de gestión y garantizando la mejora continua.

La validación empírica de las guías de implementación se realizó en un entorno real de PYME, específicamente en un bufete de abogados que, por motivos de confidencialidad y de cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP), requiere mantener su anonimato. Este entorno, caracterizado por el manejo de información sensible, resultó ideal para evaluar la eficacia de los controles propuestos mediante el UCG-Ultra. En primer lugar, se aplicaron la Guía 2 para la Gestión de Endpoints (A.8.1) y el Control de Acceso (A.8.5), realizándose pruebas de seguridad que demostraron el bloqueo satisfactorio de enlaces maliciosos y la restricción de acceso a la base de datos mediante políticas de firewall rigurosas. Además, tanto para las conexiones cableadas (Ethernet) como para las inalámbricas (Wi-Fi) de los colaboradores, se implementaron políticas de filtrado estrictas para bloquear sitios web y aplicaciones de redes sociales no relacionados con el ámbito laboral. Esta acción no solo mitiga la distracción y maximiza la concentración en la firma, sino que también reduce la superficie de ataque frente a amenazas de phishing y descargas de contenido no deseado, cumpliendo con los controles de Uso Aceptable (A.8.13).

En cumplimiento de los controles de seguridad de la red (A.8.20), se implementó una arquitectura de segmentación de red mediante VLANs (Guía 3). Esta segmentación fue crítica para aislar los sistemas sensibles, como el circuito cerrado de televisión (CCTV). La configuración asignó direcciones IP estáticas específicas a las cámaras y, mediante políticas de firewall aplicadas a la VLAN de videovigilancia, el UCG-Ultra se programó para bloquear cualquier intento de acceso o control de las cámaras proveniente de agentes externos o de empleados internos no autorizados. Este control estricto de acceso basado en la dirección IP cumple con la necesidad de Protección contra Códigos Maliciosos (A.8.7) y asegura la integridad y la confidencialidad de la videovigilancia. La verificación de la efectividad de estos controles de segmentación y monitoreo se realizó mediante la aplicación práctica de las directrices de las Guías 3 y 5, lo cual se documenta y se visualiza en los resultados presentados en la Figura 4. Con este gráfico se valida la implementación de la Guía 3 (Segmentación de Red mediante VLANs) y de la Guía 5 (Monitorización) del proyecto. El objetivo es confirmar la efectividad del Uni-

Figura 3

Guías de implementación para el uso del equipo UCG-Ultra.



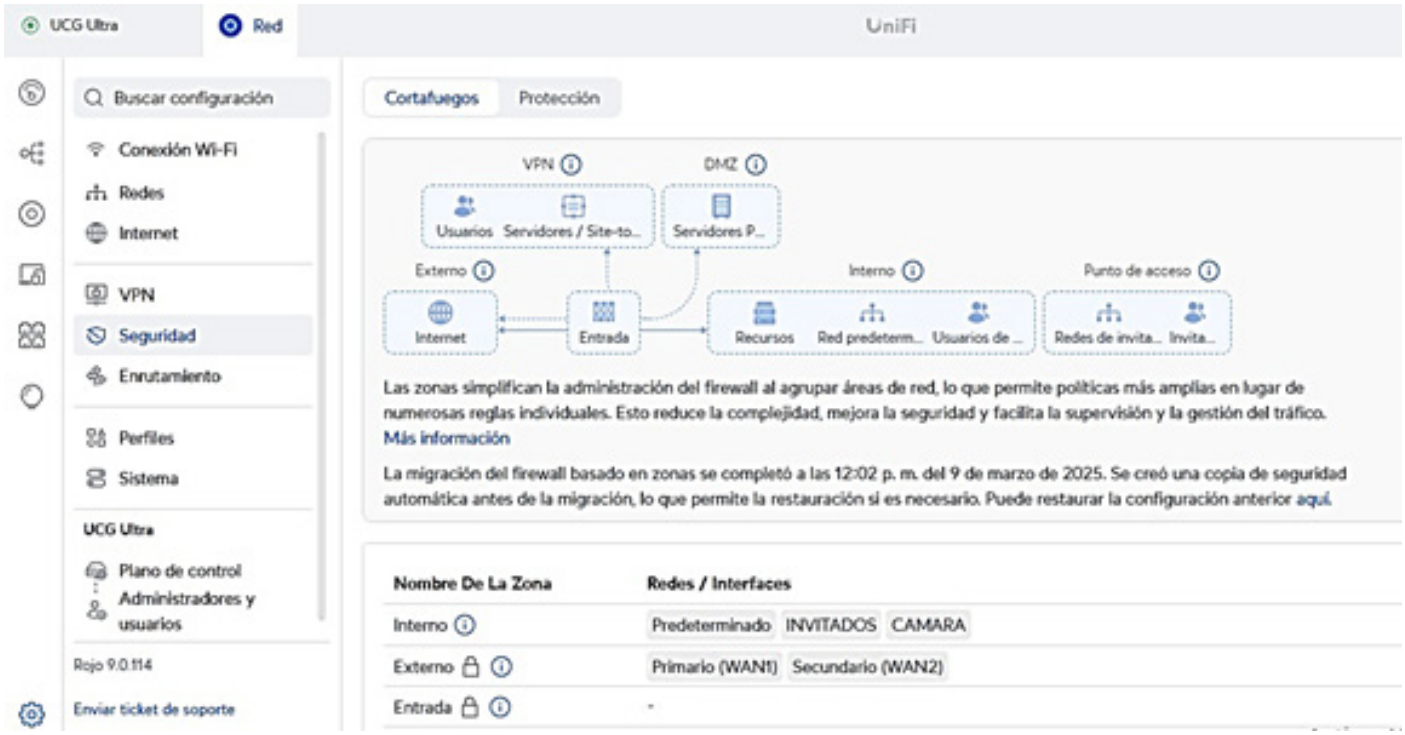
Fi Cloud Gateway Ultra (UCG-Ultra) para restringir el tráfico no autorizado en una red sensible. Se muestran los resultados de las pruebas realizadas al intentar acceder a distintos tipos de recursos web (etiquetados con colores) desde la VLAN dedicada al circuito cerrado de televisión (CCTV) del bufete de abogados. El eje vertical representa el número de intentos de conexión, mientras que el eje horizontal clasifica los recursos probados en categorías como “Redes Sociales”, “Páginas de Video/Streaming”, “Portales de Noticias” y “Sitios Web Genéricos”. Los resultados demuestran una eficacia del bloqueo cercana al 100% en todas las categorías de tráfico externo. Se observa que los intentos de acceso a redes sociales y portales de noticias fueron completamente neutralizados por las políticas de filtrado del firewall configuradas en el UCG-Ultra, lo cual es vital para el cumplimiento del control A.8.13 (Uso Aceptable) al evitar distracciones y mitigar riesgos de phishing. Este patrón de bloqueo exitoso confirma que la segmentación de red mediante VLAN de videovigilancia aísla de manera efectiva los sistemas sensibles del acceso a internet externo, un requisito fundamental del control A.8.20 (Seguridad de la Red). Estos resultados confirman que el equipo seleccionado puede garantizar la confidencialidad e integridad de los flujos de videovigilancia al impedir la exfiltración de datos y el control de las cámaras desde dominios no autorizados.

Asimismo, para acceder específicamente a la información de sus clientes, utilizan las VPN de manera sistemática en una PC seleccionada y monitorizada. Gracias a ella, pude realizar muchas pruebas con una VPN creada por el mismo equipo.

La implementación de controles específicos continuó con el cumplimiento de la Guía 4, enfocada en la Seguridad de las Comunicaciones (A.8.24) y el Cifrado (A.8.2). Para el acceso remoto y seguro a la información sensible de los clientes, se configuraron Túneles VPN directamente en el UCG-Ultra, asignando el acceso privilegiado a un endpoint específico para el manejo de la base de datos de la firma. La robustez de la conexión Wi-Fi, esencial para la productividad, fue ampliada y asegurada mediante un replicador Huawei AX3 Pro que la empresa ya poseía, el cual fue integrado exitosamente en una VLAN específica para tráfico inalámbrico, cumpliendo con las políticas de segmentación definidas en la Guía 3 y garantizando que cada puerto del UCG-Ultra se configurara con el nivel de seguridad apropiado. Este enfoque integral es una respuesta directa a la realidad de la ciberseguridad en El Salvador, donde muchas PYMES, como el bufete de tres em-

Figura 4

Menú de seguridad especificado en cortafuegos explicado



Nota. Como se muestra en la figura, se observan las características de los cortafuegos en sus respectivas zonas.

pleados —un supervisor y el dueño—, se limitan a depender de la conectividad básica de un router estándar. El análisis de su situación inicial reveló que la ausencia de protección perimetral, sumada a la falta de concienciación ("No sabemos cómo proteger nuestro sistema"), los había expuesto a múltiples ataques de malware por correo electrónico y a intentos de robo de información, lo que demuestra que son víctimas de la vulnerabilidad generalizada en el sector. Tras la exitosa implementación del UCG-Ultra y la capacitación mediante las guías, el bufete ha reportado la ausencia total de incidentes cibernéticos, lo que confirma la efectividad del modelo propuesto. La satisfacción de la dueña de la firma, que incluso decidió adquirir un segundo equipo UCG-Ultra, subraya la viabilidad económica y técnica de la solución. Este caso de estudio valida la necesidad imperante de elaborar el manual de buenas prácticas y las guías de implementación (A.6.8: Concienciación sobre seguridad) para empoderar a las empresas salvadoreñas en materia de protección adecuada.

Correspondiente a la problemática identificada de vulnerabilidad, se realizó, con base en los estudios demostrados, una comparación de las características de la norma ISO/IEC 27001:2022, aplicándolas en los equipos de esta pequeña empresa en la que se desempeñó. La tabla 1 presenta una comparación fundamental en la gestión de la seguridad de la información, contrastando un enfoque sin la norma ISO/IEC 27001:2022 con su implementación (European Union Agency for Cybersecurity, 2020). Sin la norma, el Enfoque es meramente Reactivo (actuando tras incidentes), la Estructura carece de un marco definido (medidas ad hoc) y la Gestión de Riesgos es informal o inexistente. La documentación se compone de políticas y procedimientos no estandarizados y el riesgo de incumplimiento legal es alto debido al desconocimiento de los requisitos. Los roles y responsabilidades son difusos; no hay auditorías sistemáticas ni mejora continua mediante revisiones periódicas, lo que se traduce en una menor credibilidad sin certificación externa. En contraste, la implementación de ISO/IEC 27001:2022 implica un enfoque proactivo basado en la gestión de riesgos y en la mejora continua. Se establece un Sistema de Gestión de Seguridad de la Información (SGSI) estandarizado, con un proceso formal de identificación, evaluación y tratamiento de riesgos. Exi-

Tabla 1

Comparación de la seguridad informática con un enfoque en la seguridad, conforme a la normativa ISO/IEC 27001:2022.

Aspecto	Sin ISO/IEC 27001:2022	Con ISO/IEC 27001:2022
Enfoque	Reactivo (se actúa tras incidentes).	Proactivo (gestión basada en riesgos y mejora continua).
Estructura	Sin marco definido; medidas ad hoc.	Sistema de Gestión de Seguridad de la Información (SGSI) estandarizado.
Gestión de Riesgos	Informal o inexistente.	Proceso formal: identificación, evaluación y tratamiento de riesgos (Anexo A).
Documentación	Políticas y procedimientos no estandarizados.	Documentación obligatoria (alcance, políticas, registros, etc.).
Cumplimiento Legal	Riesgo de incumplimiento por desconocimiento de los requisitos.	Alineación con las regulaciones (GDPR, LOPDGDD, etc.) mediante controles.
Roles y Responsabilidades	Difusos o asignados informalmente.	Definidos claramente (p. ej.: "responsable del SGSI").
Auditorías	Sin verificaciones sistemáticas.	Auditorías internas/externas para certificación y mejora.
Mejora Continua	Sin revisiones periódicas.	Ciclo PDCA (Plan-Do-Check-Act) para optimización.
Certificación	Sin reconocimiento externo.	Certificación internacional que aumenta la confianza de los clientes y de los socios.
Ventaja Competitiva	Menor credibilidad en el mercado.	Diferenciación frente a los competidores y acceso a licitaciones públicas.

Nota. Explicación resumida de la importancia de la normativa ISO/IEC 27001:2022

ge documentación obligatoria (alcance, políticas, registros) y asegura el cumplimiento legal mediante la alineación con las regulaciones vigentes (GDPR, LOPDGDD, etc.). Los roles están claramente definidos ("responsable del SGSI"); las auditorías internas/externas son sistemáticas para la certificación y la mejora. El ciclo PDCA (Plan-Do-Check-Act) garantiza la mejora continua. Finalmente, la certificación internacional obtenida es una ventaja competitiva crucial que incrementa la confianza de los stakeholders y permite acceder a licitaciones públicas.

Es imperativa la necesidad de concientizar al sector empresarial sobre la creciente frecuencia y el considerable impacto económico de los ciberataques, lo cual justifica plenamente la adopción de medidas proactivas y de equipos de protección perimetral para la red local.

DISCUSIÓN

La seguridad de los datos en la red local es un desafío crítico para las pequeñas y medianas empresas (PYMES) en El Salvador, especialmente en un entorno donde las ciberamenazas son cada vez más sofisticadas y frecuentes. Esta investigación abordó dicho desafío explorando alternativas de seguridad viables y efectivas, centrándose en la implementación del equipo Ubiquiti Cloud Gateway Ultra (UCG-Ultra) como solución integral para proteger los activos de información en redes locales.

A lo largo de la investigación, se demostró que el UCG-Ultra es una herramienta robusta y económicamente viable que cumple con las funciones de un sistema de Unified Threat Management (UTM). Sus funcionalidades, que incluyen firewalls avanzados, segmentación de red mediante VLANs (A.8.20), control de acceso basado en políticas (A.8.5) y monitoreo en tiempo real, lo posicionan como una opción ideal para PYMES que buscan proteger sus datos sin incurrir en los costos y complejidades técnicas asociados a soluciones empresariales de alta gama. Además, la capacidad del equipo para gestionar túneles VPN (A.8.24) y permitir el cifrado (A.8.2) de las comunicaciones responde directamente a la necesidad de asegurar la confidencialidad de la información de los clientes, como se evidenció en el caso de estudio del bufete de abogados.

La validación empírica en el contexto salvadoreño, donde muchas PYMES carecen de protección perimetral, confirmó la transformación de la postura de seguridad de un estado reactivo a uno proactivo. El UCG-Ultra demostró ser capaz de mitigar los vectores de ataque comunes, como el malware por correo electrónico, al bloquear automáticamente el tráfico malicioso y filtrar contenido no deseado, eliminando la vulnerabilidad de depender de un simple router del proveedor de servicios.

La implementación exitosa del UCG-Ultra, sumada a la elaboración de las seis Guías de implementación y el Manual de Buenas Prácticas (A.6.8), no solo protegió los datos críticos de la firma, sino que también contribuyó al cumplimiento de los controles esenciales de la ISO/IEC 27001:2022. Este hallazgo es crucial: la solución técnica de bajo costo proporciona el hardware necesario para la Declaración de Aplicabilidad (SoA), mientras que las guías aportan el componente de Gestión y Concienciación fundamental para la sostenibilidad del Sistema de Gestión de Seguridad de la Información (SGSI).

En resumen, la combinación de la tecnología accesible del Ubiquiti Cloud Gateway Ultra con un enfoque metodológico basado en la ISO/IEC 27001:2022 demuestra ser una alternativa eficaz y al alcance de las PYMES en El Salvador. La adopción de este modelo, que integra tecnología, procesos y concienciación, transforma la seguridad de las redes locales, mejorando la confianza de los stakeholders y garantizando la sostenibilidad de las operaciones a largo plazo. Se recomienda firmemente a las empresas considerar implementar esta solución como el primer paso hacia una postura de seguridad robusta y alineada con los estándares internacionales.

AGRADECIMIENTOS

Esta investigación fue posible gracias a la invaluable colaboración del Bufete de Abogados de San Salvador, El Salvador. Su compromiso al participar como caso de estudio crucial y al permitir la implementación integral del modelo de seguridad basado en el UniFi Cloud Gateway Ultra fue esencial. Su disposición a someter su red interna a rigurosas pruebas de seguridad y conectividad no solo facilitó la validación empírica de las guías de laboratorio y el UCG-Ultra, sino que también permitió demostrar el funcionamiento efectivo de un Sistema de Gestión de Seguridad de la Información (SGSI) en un entorno real de PYME. Reconocemos especialmente el apoyo continuo del dueño y del personal, cuyo anonimato se ha mantenido en cumplimiento de los estándares de confidencialidad y de la Ley Orgánica de Protección de Datos Personales (LOPDP).

REFERENCIAS

Buendía, A. C. A. (2025). Alternativas de seguridad de datos en la red local para medianas y pequeñas empresas. Universidad de El Salvador, https://hdl.handle.net/20.500.14492/31431

ISACA (2022). Guía práctica para la implementación de la gestión de la seguridad de la información según la ISO/IEC 27001:2022. Consultado el 10 de octubre de 2024.

ISO (2023) Manual de implementación de la norma ISO/IEC 27001:2022. Consultado el 10 de mayo de 2025, ISO/IEC 27001:2022 - Information security management systems (27001:2022) (1) (5)

Cleri, C. (2007). El libro de las PYMES (1.ª ed., pp. 1-44). Buenos Aires: Cleri Carlos A.R. Buenos Aires: Cleri Carlos A.R.

European Union Agency for Cybersecurity. (2020). Cybersecurity for SMEs: Challenges and Recommendations. ENISA. https://www.enisa.europa.eu. (Tabla 1) (1) (4-5)

Stewart, J. M. (2019). Cybersecurity for Small and Medium Businesses. Syngress.

Delgado, R. (2021). Ciberseguridad para PYMES: Guía práctica. Ediciones Díaz de Santos.