Mejorando la resiliencia cibernética en las pymes del sector retail y comercio electrónico a través de Blockchain

Freddy Julian Leyton Erazo

Asesor

Yenny Stella Núñez Álvarez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Dedicatoria

A Dios, fuente de sabiduría y fortaleza, por ser mi guía en cada paso que doy y en este camino, brindándome la paciencia y la claridad para alcanzar mis metas.

A mi padre Samuel Leyton, que, aunque no esté físicamente, su recuerdo y enseñanzas siguen iluminando mi vida, por su amor y ejemplo de vida, han sido mi mayor inspiración.

A mi madre, Luz Herminda Erazo, por su infinito amor, sacrificio y apoyo incondicional en todas las etapas de mi vida. Gracias por ser mi pilar y mi mayor motivación para seguir adelante.

A mi hermano, Robinson Leyton, por su compañía, palabras de aliento y confianza en mis capacidades. Su apoyo ha sido fundamental en este proceso.

A mis amigos y compañeros de estudio, quienes con su amistad y colaboración hicieron que este camino fuera más enriquecedor. Cada conversación, cada reto y cada logro compartido han sido parte esencial de esta etapa.

A todos ustedes, mi más profundo agradecimiento.

Freddy J. Leyton E

Agradecimientos

Agradecimiento profundo a Dios por ser mi luz en cada paso que doy, a mi señora madre que siempre ha estado en las buenas y en las malas, a mi hermano y familia que han hecho parte de este trabajo. A mi tutora Yenny Stella Núñez Álvarez por la guía a este desarrollo de proyecto y a todas las personas que, directa o indirectamente, contribuyeron a la culminación del proceso.

Resumen

En un mundo cada vez más digitalizado, las pequeñas y medianas empresas (PYME) se han convertido en el pilar de la economía, pero también en uno de los sectores más vulnerables ante los crecientes ciberataques. La falta de recursos, el desconocimiento en seguridad informática y la rápida evolución de las amenazas han expuesto a estas empresas a riesgos que pueden comprometer su sostenibilidad. En este contexto, Blockchain se presenta como una tecnología innovadora que podría transformar la resiliencia cibernética en las PYME, gracias a sus propiedades de descentralización, inmutabilidad y transparencia.

Este estudio adopta un enfoque cualitativo y descriptivo, basado en una revisión documental exhaustiva de normativas, investigaciones previas y casos de estudio, complementada con un análisis comparativo de soluciones Blockchain aplicables a las PYME. A través de este análisis, se identifican los principales desafíos en la adopción de esta tecnología, como la percepción de costos elevados, la falta de formación especializada y la ausencia de modelos adaptados a la realidad de estas empresas. Sin embargo, los hallazgos también evidencian que Blockchain no solo fortalece la seguridad de los datos, sino que también fomenta una cultura de confianza digital, permitiendo a las PYME ser más resilientes ante incidentes cibernéticos.

Este trabajo no solo busca demostrar el potencial de Blockchain en la ciberseguridad de las PYME, sino también ofrecer un modelo práctico y recomendaciones estratégicas para facilitar su implementación. Al hacerlo, se espera contribuir a la construcción de un entorno empresarial más seguro, donde la tecnología deje de ser un obstáculo y se convierta en un aliado para el crecimiento y la sostenibilidad de las pequeñas y medianas empresas en la era digital.

Palabras clave: Blockchain, Ciberseguridad, Vulnerabilidad, Pyme.

Abstract

In an increasingly digitalized world, small and medium-sized enterprises (SMEs) have become the backbone of the economy but also one of the most vulnerable sectors to growing cyber threats. The lack of resources, limited cybersecurity knowledge, and the rapid evolution of cyber threats have exposed these businesses to risks that could jeopardize their sustainability. In this context, Blockchain emerges as an innovative technology capable of transforming cyber resilience in SMEs, thanks to its properties of decentralization, immutability, and transparency.

This study adopts a qualitative and descriptive approach, based on a comprehensive documentary review of regulations, previous research, and case studies, complemented by a comparative analysis of Blockchain solutions applicable to SMEs. Through this analysis, key adoption challenges are identified, including the perception of high costs, the lack of specialized training, and the absence of models tailored to these companies' realities. However, findings also reveal that Blockchain not only enhances data security but also fosters a culture of digital trust, allowing SMEs to be more resilient against cyber incidents.

This research aims not only to demonstrate the potential of Blockchain in SME cybersecurity but also to provide a practical model and strategic recommendations for its implementation. By doing so, it seeks to contribute to the creation of a more secure business environment, where technology ceases to be a barrier and becomes an enabler for growth and sustainability in the digital age.

Keywords: Blockchain, Cybersecurity, Vulnerability, Sme.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

En la era digital, las pequeñas y medianas empresas (PYME) han encontrado oportunidades para expandir sus operaciones mediante el uso de tecnologías como plataformas de comercio electrónico, pasarelas de pago y sistemas de atención al cliente en línea. No obstante, este avance también las ha expuesto a un entorno cada vez más complejo en términos de ciberseguridad. Las estadísticas evidencian esta realidad: el informe Cost of a Data Breach 2023 de IBM reporta que una violación de datos en una PYME puede costar en promedio más de 3 millones de dólares, mientras que el 43 % de los ciberataques en el mundo tienen como objetivo principal a estas empresas (Verizon, 2023).

Las PYMEs del sector retail y comercio electrónico, debido a su naturaleza altamente digital, están especialmente expuestas a amenazas como el ransomware, el phishing y el robo de credenciales, lo que compromete la continuidad operativa y la confianza del cliente. Casos como el ataque a la cadena chilena Alvi en 2023, que interrumpió sus operaciones por varios días, o la filtración masiva en BigBasket, donde se expuso información de más de 20 millones de usuarios, ilustran que estas amenazas tienen un impacto real y creciente.

Frente a este panorama, es imprescindible que las PYMEs fortalezcan su postura de seguridad digital, adoptando tecnologías que les permitan anticipar, resistir y recuperarse de incidentes cibernéticos. En este contexto, la tecnología Blockchain se presenta como una alternativa innovadora para mejorar la resiliencia cibernética. Sus propiedades de descentralización, inmutabilidad y trazabilidad pueden contribuir significativamente a proteger los activos digitales, automatizar procesos de autenticación y reducir la dependencia de intermediarios.

Este estudio tiene como objetivo principal evaluar el uso de Blockchain como herramienta para mejorar la seguridad digital en las PYMEs del sector retail y comercio electrónico, identificando sus ventajas, desafíos y condiciones necesarias para su implementación. A través de una revisión documental y un análisis comparativo de casos reales, se busca proponer estrategias viables y adaptadas a las capacidades de este sector, fomentando así un entorno empresarial más seguro, resiliente y competitivo.

Planteamiento del Problema

En el contexto de la transformación digital, las pequeñas y medianas empresas (PYME) del sector retail y comercio electrónico han encontrado nuevas oportunidades de crecimiento gracias a la adopción de plataformas en línea, pasarelas de pago y sistemas de atención automatizados. No obstante, esta evolución también ha ampliado su exposición a amenazas cibernéticas cada vez más sofisticadas, como el ransomware, el robo de credenciales, el phishing o los ataques de denegación de servicio (DDoS). A diferencia de las grandes corporaciones, las PYMEs suelen carecer de recursos humanos, financieros y tecnológicos para implementar estrategias de ciberseguridad robustas, lo que las convierte en blancos recurrentes de ciberataques. Según datos citados por ISACA (2023), el 43 % de los ciberataques a nivel mundial tienen como objetivo a pequeñas empresas, de las cuales el 60 % se ve obligada a cerrar sus operaciones en los seis meses posteriores al incidente. Además, los costos asociados a estas brechas pueden variar entre 826 y 653,587 dólares por evento, con una tendencia proyectada de aumento del 15 % en los próximos dos años. Estas cifras evidencian la gravedad del impacto que los ataques cibernéticos pueden tener sobre la sostenibilidad de las PYMEs.(ISACA, 2023)

Casos recientes en América Latina confirman esta tendencia. Por ejemplo, el ataque de ransomware a IFX Networks en 2023 afectó a cientos de organizaciones públicas y privadas, paralizando servicios esenciales en países como Chile, Colombia y Panamá(Botero Maria Camila, 2023). Asimismo, la interrupción provocada por un ciberataque al Grupo GTD en Chile dejó sin servicios digitales a miles de clientes del sector empresarial(Welivesecurity By Eset & Bocconi Maria, 2023). Estos incidentes evidencian que la amenaza no distingue tamaño ni industria, pero afecta con mayor severidad a las empresas con menor capacidad de respuesta.

Frente a este panorama, la tecnología Blockchain surge como una alternativa prometedora para fortalecer la seguridad digital de las PYMEs. Gracias a su descentralización, inmutabilidad y trazabilidad, permite blindar la integridad de los datos, mejorar los procesos de autenticación y automatizar validaciones mediante contratos inteligentes. Sin embargo, su adopción aún es limitada debido a la falta de conocimiento técnico, la percepción de altos costos y la escasa oferta de modelos adaptables a la realidad de estas empresas.

En consecuencia, se hace necesario analizar cómo tecnologías emergentes como Blockchain pueden integrarse de forma efectiva en el entorno de las pequeñas y medianas empresas del sector retail y comercio electrónico, tomando en cuenta sus restricciones operativas y su creciente exposición a amenazas cibernéticas.

A partir de este contexto, surge la siguiente pregunta problémica que orienta el desarrollo del presente estudio:

¿Cómo pueden las pequeñas y medianas empresas (PYMEs) del sector retail y comercio electrónico fortalecer su resiliencia frente a ciberataques mediante la adopción de tecnologías emergentes como Blockchain, considerando sus limitaciones de infraestructura, recursos y capacidades técnicas en un entorno digital cada vez más amenazado por ataques como ransomware, phishing y fraude en transacciones electrónicas?

Justificación

Las pymes del sector retail y comercio electrónico desempeñan un papel crucial en la economía latinoamericana, ya que no solo representan una fuente importante de empleo e innovación, sino que también están en la primera línea del proceso de digitalización. Sin embargo, su crecimiento en entornos digitales no ha sido acompañado por mecanismos de protección equivalentes, lo que las expone a riesgos cibernéticos significativos.

La infraestructura tecnológica de mucha pyme carece de herramientas avanzadas de seguridad, políticas de protección de datos o planes de respuesta ante incidentes. A esto se suma la creciente sofisticación de las amenazas digitales y el aumento de transacciones electrónicas que requieren altos niveles de confianza por parte del consumidor. La consecuencia es una alta vulnerabilidad que afecta su operatividad, reputación e incluso su sostenibilidad a largo plazo.

En este contexto, Blockchain representa una alternativa innovadora que puede transformar el enfoque tradicional de la ciberseguridad. A través de su arquitectura descentralizada, permite eliminar puntos únicos de falla, verificar identidades digitales, garantizar la integridad de la información y facilitar auditorías en tiempo real. Soluciones como Blockchain-as-a-Service (BaaS), ofrecidas por empresas como IBM, Microsoft y Hyperledger(Mansa Julio, 2024), hacen posible su implementación sin requerir infraestructura costosa, haciéndola accesible incluso para organizaciones de menor escala.

La relevancia de este estudio radica en la necesidad urgente de brindar a las PYMEs herramientas prácticas y eficaces para enfrentar el escenario actual de amenazas digitales. Al proponer estrategias concretas de adopción de Blockchain adaptadas a las capacidades del sector, se busca no solo mejorar la protección de los activos digitales, sino también fortalecer la

confianza del consumidor y promover una cultura organizacional orientada a la resiliencia cibernética.

Además, el trabajo contribuye al cumplimiento de marcos normativos como la Ley 1581 de 2012 en Colombia y estándares internacionales como ISO/IEC 27001, apoyando a las PYMEs en su proceso de madurez digital y legal. Así, esta investigación no solo responde a un reto técnico, sino también a una necesidad económica y social, fortaleciendo la competitividad de un sector clave para el desarrollo del país.(Ley 1581 de 2012 - Gestor Normativo - Función Pública, 2012)

Objetivos

Objetivo General

Evaluar las distintas tecnologías Blockchain que contribuyan a la resiliencia cibernética en Pymes del sector retail y comercio electrónico, proporcionando un marco para la protección de datos y la mitigación de riesgos.

Objetivos Específicos

Establecer las prácticas actuales de ciberseguridad en Pymes del sector retail y comercio electrónico, identificando vulnerabilidades y amenazas comunes que enfrentan en sus entornos digitales.

Analizar las propiedades fundamentales de Blockchain, como la descentralización, inmutabilidad y transparencia, mediante el estudio de literatura académica y casos de aplicación en el ámbito empresarial, con el propósito de evaluar su impacto en la seguridad y confiabilidad de los entornos digitales.

Proponer estrategias que integren soluciones de Blockchain para las vulnerabilidades específicas identificadas en Pymes de retail y comercio electrónico, mejorando su capacidad de respuesta ante incidentes cibernéticos.

Marco Referencial

Antecedentes

La ciberseguridad representa un reto importante para las pymes del sector retail y comercio electrónico, dado el crecimiento de amenazas digitales y la sensibilidad de los datos que manejan; Según Fátima Báñez, presidenta de la Fundación CEOE, seis de cada diez empresas que sufren un ciberataque grave no logran recuperarse y terminan cerrando en los seis meses posteriores al incidente. Esta cifra refleja la alta vulnerabilidad de las pequeñas y medianas empresas ante las amenazas digitales. Solo en el último año, se registraron en España cerca de 120.000 ciberataques, siendo las PYMEs las más afectadas, principalmente por los altos costos que implican estos incidentes y las limitaciones que enfrentan para mantener sus operaciones. Además del impacto económico, estos ataques suelen comprometer la reputación y la confianza del cliente, lo que agrava aún más las consecuencias(Ingefor & Bellanato Rodriguez Oscar, 2025).Esta situación ha impulsado la búsqueda de tecnologías emergentes como Blockchain para fortalecer su resiliencia digital.

Blockchain ha demostrado ser una alternativa eficaz gracias a características como la descentralización, la inmutabilidad y la transparencia, permitiendo prevenir fraudes, garantizar la trazabilidad de transacciones y proteger identidades digitales. Aunque ampliamente adoptada en sectores como finanzas o logística, su implementación en PYMES del comercio electrónico aún es limitada, en parte por desconocimiento, percepciones erradas sobre costos y falta de modelos adaptados a su realidad.

Investigaciones recientes han resaltado el potencial de Blockchain frente a amenazas como suplantación de identidad, fraudes digitales y pérdida de datos. El uso de contratos inteligentes e identidades digitales descentralizadas ha permitido mejorar los niveles de

seguridad y trazabilidad en entornos digitales. Casos como OpenBazaar, VeChain o CoffeeChain evidencian aplicaciones reales que han optimizado procesos y reducido vulnerabilidades.

Entre los principales riesgos que Blockchain puede abordar se encuentran la falsificación de datos, el robo de identidad, ataques DoS y la pérdida de información, y que gracias a su estructura distribuida y uso de funciones hash, esta tecnología garantiza registros inalterables, protección contra accesos no autorizados y continuidad operativa ante fallos técnicos o ciberataques.

Además, Blockchain permite establecer sistemas de identidad digital descentralizada, donde los usuarios tienen control sobre sus datos y se mejora el proceso de verificación segura. A través de contratos inteligentes, se automatizan acciones críticas como validación de accesos y pagos, reduciendo errores humanos y mejorando la respuesta ante incidentes.

La trazabilidad que ofrece también facilita procesos de auditoría en tiempo real, permitiendo detectar anomalías, reforzar el cumplimiento normativo y mejorar la gobernanza de datos. Incluso, el almacenamiento de información crítica en Blockchains privadas, combinado con soluciones off-chain, ofrece una forma escalable y segura de proteger la integridad de los datos sin comprometer rendimiento.

Sin embargo, para que estas soluciones sean efectivas en las PYMES, se requiere un enfoque integral que no solo considere la tecnología, sino también el factor humano. La formación en cultura digital y la concientización sobre ciberseguridad son claves para una adopción efectiva y sostenible de Blockchain.

Este estudio busca cerrar la brecha de conocimiento y accesibilidad tecnológica, proponiendo estrategias de integración de Blockchain que se ajusten a las capacidades reales de las PYMES del sector retail. La meta es contribuir al fortalecimiento de su seguridad informática

sin comprometer su viabilidad operativa ni incurrir en inversiones desproporcionadas(Hanafizadeh & Alipour, 2024)

Marco Teórico

La tecnología Blockchain ha emergido como una innovación disruptiva que redefine la forma en que se gestionan y protegen los datos digitales. Se basa en una estructura de registros distribuidos e inmutables, organizados en bloques enlazados criptográficamente, que permiten validar y almacenar transacciones sin requerir intermediarios ni autoridades centrales. Esta arquitectura ofrece beneficios significativos en términos de integridad, disponibilidad, trazabilidad y seguridad, aspectos fundamentales en entornos digitales cada vez más expuestos a amenazas.(IBM, 2025)

Desde su origen con Bitcoin en 2008, Blockchain ha evolucionado hacia múltiples aplicaciones más allá del ámbito financiero. Sectores como el logístico, gubernamental, educativo y especialmente el comercio electrónico han comenzado a integrar esta tecnología como una alternativa sólida frente a desafíos como el fraude, la suplantación de identidad, el robo de datos y la manipulación de registros.

En el comercio digital, Blockchain permite asegurar la integridad de las operaciones, desde el pedido hasta el pago, evitando alteraciones maliciosas o accesos no autorizados. Su naturaleza descentralizada elimina puntos únicos de falla, mejorando la resiliencia de los sistemas informáticos frente a ciberataques. Asimismo, la inmutabilidad de los registros garantiza que la información no pueda ser modificada sin consenso, lo cual es esencial en procesos de auditoría, cumplimiento normativo y resolución de disputas.

Otro componente clave de Blockchain es la transparencia. Las transacciones registradas pueden ser verificadas por las partes autorizadas, sin comprometer la confidencialidad, lo que

mejora la trazabilidad y facilita la detección de irregularidades. Esta característica es particularmente útil en cadenas de suministro digitales, donde la autenticidad y procedencia de los productos son aspectos críticos para el consumidor final. (SAP, 2025)

En materia de ciberseguridad, Blockchain aporta mecanismos criptográficos avanzados que refuerzan la confidencialidad y autenticidad de los datos. Tecnologías como la criptografía de clave pública y las funciones hash permiten validar identidades, firmar digitalmente documentos y detectar alteraciones en los registros. A esto se suman los contratos inteligentes (smart contracts), que automatizan procesos de verificación y ejecución de transacciones bajo condiciones predefinidas, reduciendo errores humanos y mejorando la eficiencia operativa.

A diferencia de los sistemas tradicionales basados en bases de datos centralizadas, Blockchain ofrece un modelo más robusto y confiable para la gestión de identidades digitales. Las PYMEs pueden beneficiarse de esta tecnología para implementar sistemas de autenticación descentralizados, donde los usuarios controlan sus datos sin depender de proveedores externos, reduciendo así el riesgo de filtraciones o suplantación de identidad.

Empresas del sector retail como Walmart, Carrefour y VeChain ya han integrado soluciones basadas en Blockchain para garantizar la trazabilidad de productos, la veracidad de transacciones y la protección de información sensible. Estos casos evidencian que la aplicación de esta tecnología no solo fortalece la seguridad, sino que también mejora la eficiencia, la transparencia y la confianza del consumidor.

Pese a sus beneficios, la adopción de Blockchain aún enfrenta desafíos, especialmente para las pequeñas y medianas empresas. Entre las principales barreras se encuentran la falta de conocimiento técnico, la percepción de altos costos y la necesidad de adaptar esta tecnología a infraestructuras existentes. No obstante, el surgimiento de soluciones como Blockchain-as-a-

Service (BaaS) ha democratizado su acceso, permitiendo a empresas de menor tamaño implementar esta tecnología de forma escalable y rentable.

Blockchain representa una herramienta estratégica para mejorar la resiliencia cibernética en las Pymes del sector retail y comercio electrónico. Su aplicación permite proteger los activos digitales, asegurar transacciones, gestionar identidades de forma segura y cumplir con estándares internacionales de seguridad de la información, como ISO/IEC 27001. Este marco teórico establece las bases para comprender su valor en el contexto de la ciberseguridad empresarial y su potencial como factor diferenciador en la economía digital.(Bistamp Learn, 2024)

Marco conceptual

Pyme

Las pequeñas y medianas empresas Pyme son organizaciones cuyo tamaño está limitado en términos de número de empleados, volumen de ventas o activos. En Colombia, la Ley 905 de 2004 las clasifica como pequeñas (hasta 50 empleados) o medianas (hasta 200 empleados). En el contexto del comercio electrónico, estas empresas enfrentan desafíos significativos en seguridad digital, debido a recursos limitados y una menor capacidad de respuesta frente a amenazas cibernéticas.

Ciberseguridad

La ciberseguridad se refiere al conjunto de políticas, tecnologías y prácticas diseñadas para proteger redes, dispositivos, sistemas y datos frente a accesos no autorizados, daños o robos. En el entorno de las PYME del comercio digital, la ciberseguridad implica la prevención y detección de amenazas como el ransomware, el phishing, y el fraude en transacciones electrónicas.

Blockchain

Blockchain es una tecnología de registro distribuido (Distributed Ledger Technology - DLT) que permite almacenar información de forma descentralizada, segura e inmutable. Cada transacción es validada por consenso y registrada en bloques criptográficamente enlazados. Su aplicación en ciberseguridad radica en su capacidad para evitar la manipulación de datos y garantizar transparencia en entornos digitales.

Figura 1

Arquitectura Básica de una Solución Blockchain

Nota. La figura ilustra la estructura fundamental de una solución Blockchain, mostrando cómo los datos se agrupan en bloques enlazados criptográficamente y distribuidos entre múltiples nodos de la red. Este modelo descentralizado garantiza la inmutabilidad de la información, la transparencia en las transacciones y la resistencia frente a alteraciones o accesos no autorizados. Tomado de. ¿Qué es el blockchain y cómo funciona? Villa A. (2024)

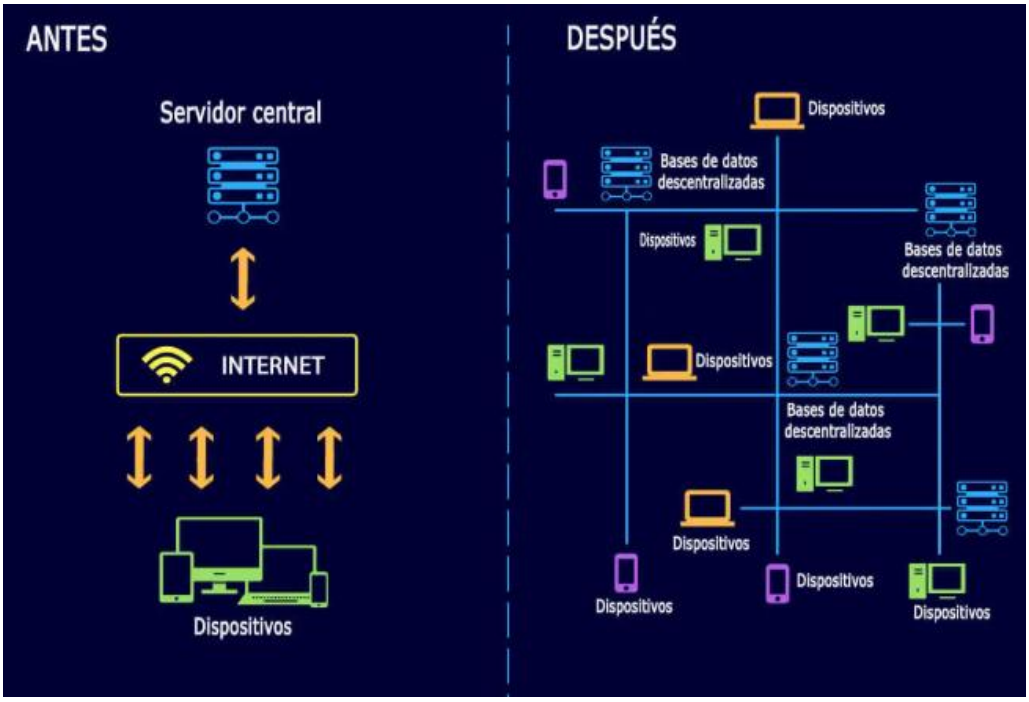
https://www.finect.com/usuario/vanesamatesanz/articulos/que-blockchain-criptomonedas-guia-facildas-guia-facil

Descentralización

La descentralización es el principio que elimina la dependencia de un único servidor o autoridad central. En Blockchain, la información se distribuye entre múltiples nodos, reduciendo puntos de falla únicos y mejorando la resistencia frente a ataques, como los de denegación de servicio (DDoS). Para las PYME, esto significa mayor robustez sin necesidad de grandes infraestructuras.

Figura 2

Arquitectura Centralizada VS Descentralizada



Nota. La figura compara el modelo de arquitectura centralizada, donde la información se gestiona desde un único servidor o autoridad, con la arquitectura descentralizada, característica

de Blockchain, en la que los datos se distribuyen entre múltiples nodos. Esta descentralización reduce los puntos únicos de falla, incrementa la disponibilidad del sistema y mejora la resistencia frente a ataques o interrupciones. Representación gráfica de funcionalidad centralizado Vs descentralizada. Tomado de. Fundamentos de la tecnología de Blockchain Rodríguez N. (2019) https://101blockchains.com/es/blockchain-para-empresas/

Inmutabilidad

Hace referencia a la imposibilidad de alterar los datos una vez han sido registrados en la cadena de bloques, sin alterar la integridad del sistema completo. Esta propiedad garantiza la confiabilidad de los registros, fortalece los procesos de auditoría y previene fraudes y manipulaciones.

Transparencia

Es la posibilidad de verificar transacciones o procesos sin necesidad de intermediarios. Blockchain permite que los actores autorizados tengan acceso a un historial auditable y trazable, sin comprometer la confidencialidad. En el comercio electrónico, esto facilita la confianza del cliente y la validación de operaciones.

Criptografía

La criptografía es el conjunto de técnicas utilizadas para proteger la información mediante el cifrado. En Blockchain, se utilizan algoritmos criptográficos como las funciones hash y la criptografía de clave pública para asegurar la integridad, autenticidad y confidencialidad de los datos.

Contratos Inteligentes (Smart Contracts)

Son programas autoejecutables basados en Blockchain que se activan cuando se cumplen condiciones predefinidas. Estos contratos eliminan la intervención de terceros, reducen el error humano y aseguran que los acuerdos digitales se ejecuten de manera segura y automática, lo cual es útil en transacciones digitales de las PYME.

Identidad Digital Descentralizada

Es un modelo en el que los usuarios controlan su identidad y sus datos personales directamente, sin depender de entidades centrales. Blockchain permite implementar sistemas de autenticación seguros que reducen los riesgos de suplantación y robo de información en el comercio electrónico.

Marco Legal

El marco legal que regula el uso de Blockchain en la ciberseguridad de las pequeñas y medianas empresas Pyme está compuesto por normativas internacionales y nacionales que buscan garantizar la integridad, confidencialidad y disponibilidad de la información. A nivel global, la ISO/IEC 27001:2022 establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI), permitiendo a las empresas adoptar buenas prácticas para la protección de sus datos. En el contexto europeo, el Reglamento General de Protección de Datos (GDPR) obliga a las organizaciones a implementar medidas de seguridad que garanticen el control sobre la información personal, aspecto fundamental cuando se utilizan tecnologías como Blockchain, donde la inmutabilidad de los registros plantea retos en cuanto a la eliminación o modificación de datos personales.(Diario Oficial de la Unión Europea 2016; 22)

En Colombia, la Ley 1581 de 2012 es el marco normativo principal para la protección de datos personales, estableciendo principios como la seguridad, confidencialidad y acceso

restringido a la información. Esta ley exige que las empresas implementen mecanismos adecuados para proteger la información de sus clientes y empleados, lo que puede complementarse con el uso de Blockchain para garantizar la integridad y trazabilidad de los datos. Además, el Conpes 3995 de 2020 fomenta la adopción de tecnologías emergentes para mejorar la seguridad digital en el país, promoviendo la incorporación de soluciones innovadoras que refuercen la resiliencia cibernética en sectores estratégicos, incluyendo las PYME.(Congreso de Colombia, 2012)

Por otro lado, la Ley 527 de 1999, que regula el comercio electrónico y las firmas digitales en Colombia, otorga validez jurídica a documentos electrónicos y contratos inteligentes basados en Blockchain. Esta normativa permite que las PYME implementen soluciones seguras para la gestión documental, autenticación de identidades y automatización de procesos sin depender de intermediarios. Asimismo, regulaciones como el Decreto 1074 de 2015, que reglamenta la protección de datos en el ámbito empresarial, refuerzan la necesidad de adoptar medidas de seguridad en la administración de la información. La correcta integración de Blockchain bajo estos marcos regulatorios no solo fortalece la seguridad informática de las PYME, sino que también facilita su cumplimiento normativo y mejora la confianza de clientes y aliados comerciales.(Congreso de Colombia, 1999)

El uso de Blockchain en la resiliencia cibernética de las pequeñas y medianas empresas (PYME) debe enmarcarse en normativas y estándares nacionales e internacionales que regulan la seguridad de la información y la protección de datos. A nivel global, el Reglamento General de Protección de Datos (GDPR) de la Unión Europea establece principios de privacidad y seguridad en el tratamiento de datos personales, mientras que la ISO/IEC 27001 proporciona directrices para la gestión de la seguridad de la información, aplicables a cualquier organización que busque

fortalecer su infraestructura digital. En Colombia, la Ley 1581 de 2012 regula la protección de datos personales, imponiendo obligaciones a las empresas en la gestión segura de la información, mientras que el Conpes 3995 de 2020 fomenta la adopción de tecnologías emergentes, como Blockchain, para mejorar la seguridad digital en el país. Además, la Ley 527 de 1999, que otorga validez jurídica a documentos electrónicos y firmas digitales, resulta clave para la implementación de Blockchain en procesos de autenticación y gestión documental en las PYME. Estos marcos normativos y estándares establecen la base para que las empresas integren soluciones de Blockchain sin comprometer el cumplimiento legal, garantizando la protección de la información y la mitigación de riesgos cibernéticos.

Marco Contextual

Las pequeñas y medianas empresas (PYME) se encuentran en un ecosistema digital donde la evolución tecnológica ha transformado sus operaciones, pero también ha incrementado su exposición a riesgos cibernéticos. La creciente interconectividad y el uso de plataformas digitales han facilitado su desarrollo, pero al mismo tiempo han generado nuevas superficies de ataque, comprometiendo la integridad y disponibilidad de sus datos. A diferencia de las grandes corporaciones, las PYME suelen contar con recursos limitados para invertir en estrategias avanzadas de ciberseguridad, lo que las convierte en objetivos atractivos para cibercriminales. Esta situación ha impulsado la búsqueda de soluciones innovadoras y accesibles, entre ellas la tecnología Blockchain, que, por sus características de descentralización e inmutabilidad, ofrece un marco sólido para reforzar la protección de la información y optimizar la gestión de riesgos en estos entornos empresariales.(Hanafizadeh & Alipour, 2024)

Si bien Blockchain ha demostrado su eficacia en sectores como las finanzas y la cadena de suministro, su aplicación en la ciberseguridad de las PYME sigue siendo incipiente. La falta

de conocimiento técnico y la percepción de que su implementación requiere una alta inversión han limitado su adopción en este segmento empresarial. No obstante, esta tecnología tiene el potencial de mejorar significativamente la resiliencia cibernética al garantizar la trazabilidad y autenticidad de la información, minimizar la manipulación de datos y ofrecer nuevos modelos de gestión de identidad digital. Superar estas barreras implica desarrollar estrategias accesibles que permitan integrar Blockchain en los esquemas de seguridad de las PYME, asegurando su viabilidad operativa y su alineación con los marcos regulatorios existentes.

Desde una perspectiva local, en Colombia se han impulsado diversas iniciativas gubernamentales para fortalecer la seguridad digital, como el Conpes 3995 de 2020, que fomenta la adopción de tecnologías emergentes para reducir vulnerabilidades en los sectores productivos. Sin embargo, las PYME siguen rezagadas en la implementación de mecanismos avanzados de protección, lo que las expone a pérdidas económicas y daños reputacionales. La ausencia de regulaciones específicas sobre Blockchain en el país también representa un desafío para su integración en la seguridad informática. En este contexto, este estudio busca analizar el impacto de Blockchain en la resiliencia cibernética de las PYME y proponer un modelo de implementación que les permita fortalecer sus mecanismos de protección sin comprometer su capacidad operativa, contribuyendo así a la construcción de un entorno empresarial más seguro y confiable.(Lucía Ramirez Blanco et al., 2020)

Otro factor importante es la aplicación de normativas SARLAFT y SAGRILAFT, que obligan a las empresas a implementar mecanismos de control para prevenir el lavado de activos y la financiación del terrorismo. Blockchain puede ser una herramienta clave para mejorar la trazabilidad de las transacciones y el cumplimiento normativo, pero a su vez, la falta de regulación específica sobre su uso en sectores como el financiero y el comercio puede generar

incertidumbre en las Pymes. Por lo tanto, es fundamental que las empresas que adopten esta tecnología alineen sus procesos con los requisitos exigidos por la Superintendencia de Industria y Comercio (SIC) y la Superintendencia Financiera.

En conclusión, aunque las regulaciones en Colombia ofrecen un marco normativo que facilita la transformación digital y el comercio electrónico, aún existen barreras legales y desafíos que pueden dificultar la adopción de Blockchain en las Pymes. Para que esta tecnología sea viable, las empresas deben garantizar el cumplimiento de las leyes de protección de datos, adaptar sus procesos a la normativa vigente y trabajar en la creación de modelos de Blockchain que permitan un equilibrio entre seguridad, transparencia y privacidad.(Superintendencia de vigilanci y seguridad Privada, 2025)

Diseño Metodológico

La presente investigación adopta un enfoque cualitativo y documental, sustentado en la revisión crítica y sistemática de literatura académica, estudios de caso, publicaciones especializadas, informes técnicos y normativas vigentes relacionadas con ciberseguridad, Blockchain y comercio electrónico en Pymes. Esta metodología es pertinente, dado el objetivo exploratorio y propositivo del trabajo, orientado a identificar estrategias tecnológicas emergentes aplicables a un sector específico.

El desarrollo del estudio se estructura en tres capítulos: el primero aborda el contexto actual de ciberseguridad en las Pymes del comercio electrónico, identificando amenazas frecuentes, vulnerabilidades más comunes y limitaciones estructurales. El segundo capítulo explora las características técnicas y funcionales de la tecnología Blockchain, diferenciándola de las soluciones centralizadas tradicionales y analizando su aplicabilidad en entornos de protección de datos y autenticación. Finalmente, el tercer capítulo propone una estrategia fundamentada en los hallazgos previos, que integra herramientas, buenas prácticas y mecanismos tecnológicos adecuados para su adopción por parte de pequeñas empresas del sector, y evalúa su viabilidad y proyección futura.

La validación de los planteamientos propuestos se sustenta en la coherencia argumentativa, la triangulación de fuentes reconocidas a nivel internacional y la alineación con marcos conceptuales vigentes en seguridad informática. Asimismo, se tuvo en cuenta el contexto nacional colombiano, considerando tanto los marcos regulatorios como las capacidades tecnológicas típicas de las PYMEs locales.

Identificación de Amenazas y Vulnerabilidades en su Entorno Digital de las Pymes de Retail y Comercio Electrónico

La tendencia digital actual, el sector retail y comercio electrónico es una pieza clave del desarrollo económico global, y que cada día, millones de pequeñas y medianas empresas pymes dependen de plataformas en línea para vender sus productos y servicios, gestionar sus inventarios y atender a sus clientes finales. Sin embargo, este crecimiento también ha traído consigo una alarmante exposición a ciberamenazas, que pueden comprometer no solo la seguridad de la información de las empresas, sino también la credibilidad de los clientes.

Las pymes del sector retail son especialmente vulnerables a ataques como el robo de credenciales, el fraude en pagos electrónicos y el ransomware, debido a que muchas de ellas no cuentan con estrategias robustas de ciberseguridad ni con recursos suficientes para implementar soluciones avanzadas de protección. Según el informe Data Breach Investigations Report 2023 de Verizon, más del 43 % de los ciberataques a nivel mundial están dirigidos a pequeñas empresas, y una filtración de datos puede significar una pérdida financiera millonaria(Rowntree, 2023)

Este capítulo tiene como objetivo establecer un panorama claro sobre las prácticas actuales de ciberseguridad en las Pymes de retail y comercio electrónico, identificando las amenazas y vulnerabilidades más comunes en su entorno digital. A través de un análisis detallado, se busca comprender los principales desafíos a los que se enfrentan estas empresas y qué medidas están adoptando o dejando de adoptar para protegerse en un ecosistema donde la seguridad digital es tan importante como la calidad del servicio que ofrecen.

Estado de la Ciberseguridad en el Comercio Electrónico y Retail

EL comercio digital ha crecido de manera acelerada transformando la manera en que las empresas operan y los consumidores acceden a bienes y servicios, este crecimiento no ha sido fortuito, sino el resultado de una combinación de factores que han creado un entorno favorable para la digitalización del comercio. Desde la accesibilidad tecnológica hasta la evolución de los métodos de pago, las Pymes del sector retail y comercio electrónico han encontrado en la digitalización una oportunidad única para expandirse, llegar a nuevos mercados y mejorar su competitividad. Sin embargo, este mismo crecimiento también ha traído consigo desafíos en materia de seguridad, exigiendo una modernización constante de las estrategias de protección digital.

El acceso a internet y el uso de dispositivos móviles han cambiado radicalmente la forma en que las personas interactúan con las empresas. Hoy en día, más del 65 % de las compras en línea se realizan desde teléfonos inteligentes, según (Holanda Dias Kershaw, 2023), lo que refleja la importancia de optimizar las plataformas digitales para estos dispositivos. La conectividad global ha permitido que las Pymes del sector retail y comercio electrónico no solo vendan localmente, sino que también accedan a mercados internacionales con relativa facilidad. Con una tienda en línea bien estructurada, una empresa puede vender productos a clientes en diferentes partes del mundo sin necesidad de establecer sucursales físicas, lo que reduce costos operativos y amplía las oportunidades de crecimiento.

Sin embargo, esta interconexión también ha generado nuevas amenazas en términos de ciberseguridad. El creciente número de dispositivos conectados a la red amplía la superficie de ataque de los ciberdelincuentes, quienes aprovechan vulnerabilidades en sistemas mal protegidos para acceder a información confidencial o interrumpir operaciones comerciales. Por ello, las

empresas que operan en el entorno digital deben adoptar estrategias de protección adecuadas, asegurando que sus plataformas sean seguras, confiables y resistentes a ataques cibernéticos.

Por otro lado, se presenta la expansión y diversificación de los métodos de pago, que han permitido que más personas puedan comprar en línea de manera rápida y segura. En el pasado, el comercio electrónico estaba limitado a pagos con tarjeta de crédito o transferencias bancarias, lo que restringía el acceso de muchos consumidores. Hoy en día, existen diversas opciones de pago, como billeteras digitales PayPal, Apple Pay, Google Pay,(SEON, 2025) criptomonedas y plataformas de financiamiento como "compre ahora, pague después" (BNPL, por sus siglas en inglés).

Para las Pymes del sector retail y comercio electrónico, ofrece múltiples métodos de pago se traduce en mayor confianza y comodidad para los clientes, lo que incrementa las tasas de conversión y fidelización. Sin embargo, esta diversificación también ha traído consigo nuevas amenazas cibernéticas, como el fraude en transacciones electrónicas, el robo de credenciales y la clonación de tarjetas y que, para mitigar estos riesgos, cada vez más empresas están recurriendo a tecnologías como Blockchain, que permite la autenticación segura de transacciones y la reducción del fraude financiero a través de contratos inteligentes y registros inmutables.

También el crecimiento de los marcketplaces y el comercio social como Amazon, MercadoLibre, Shopify y Facebook Marketplace ha democratizado el acceso al comercio electrónico, permitiendo que pequeñas y medianas empresas vendan productos sin la necesidad de desarrollar su propio sitio web desde cero. Estas plataformas proporcionan infraestructura tecnológica, servicios de pago seguros y soluciones logísticas, lo que facilita la entrada de nuevos actores al mercado digital.

Además, las redes sociales han desempeñado un papel crucial en la expansión del comercio digital. El comercio social (social commerce) ha permitido que empresas comercialicen sus productos directamente en plataformas como Instagram, TikTok y Facebook, donde los consumidores pueden descubrir, comparar y comprar productos sin salir de la aplicación. Este fenómeno ha hecho que el comercio digital sea más accesible y atractivo, especialmente para el público joven, que prioriza la experiencia de compra a través de contenidos visuales y reseñas de otros consumidores.(Ardila, n.d.)

A pesar de estas ventajas, las Pymes que operan en marketplaces o redes sociales enfrentan nuevos riesgos de ciberseguridad, como la suplantación de identidad, el robo de cuentas y la proliferación de tiendas fraudulentas. La falta de regulación en algunos mercados ha permitido que ciberdelincuentes creen tiendas falsas para estafar a consumidores desprevenidos. Ante este escenario, la implementación de tecnologías de verificación y autenticación basadas en Blockchain podría representar una solución efectiva para proteger tanto a las empresas como a los compradores en el entorno digital.

la integración de inteligencia artificial (IA) y automatización en los procesos de venta, marketing y atención al cliente. Actualmente, muchas empresas utilizan algoritmos de recomendación que analizan el comportamiento del consumidor para ofrecer productos personalizados, lo que mejora la experiencia de compra y aumenta la conversión de ventas. Asimismo, los chatbots y asistentes virtuales han optimizado la atención al cliente, proporcionando respuestas inmediatas a consultas y resolviendo dudas sin intervención humana.

En el ámbito logístico, el comercio digital ha evolucionado con el desarrollo de sistemas de entrega rápida, almacenamiento automatizado y rastreo en tiempo real. Empresas como Amazon y Alibaba han implementado centros de distribución inteligentes que utilizan robots y

análisis de datos en tiempo real para optimizar el procesamiento de pedidos. Las Pymes que logran integrar estas tecnologías pueden mejorar significativamente su competitividad, ofreciendo tiempos de entrega más rápidos y un mejor servicio al cliente.

No obstante, el uso de inteligencia artificial y automatización en el comercio digital también ha traído nuevos riesgos, especialmente en términos de seguridad de datos y ataques dirigidos a los sistemas automatizados. Los ataques a infraestructuras críticas, la manipulación de algoritmos de IA y el robo de datos personales son algunas de las amenazas emergentes que las empresas deben enfrentar. Para ello, se están explorando modelos de ciberseguridad basados en Blockchain, que permiten proteger la integridad de los datos, asegurar la trazabilidad de transacciones y evitar la manipulación de sistemas automatizados.

Amenazas cibernéticas más frecuentes en PYME del sector

A continuación, se sintetizan las amenazas cibernéticas más frecuentes que enfrentan las PYMEs del sector comercio electrónico, agrupando su descripción, impacto y datos relevantes, con el fin de proporcionar un panorama más claro y contextualizado sobre el nivel de exposición de las empresas ante los riesgos digitales actuales.

Tabla 1

Amenazas Comunes en el Comercio Electrónico para PYMEs

Tipo de Amenaza	Descripción	Impacto en PYMEs	Ejemplo o Estadística Relevante
Ransomware	Software malicioso que encripta datos del sistema y exige un rescate para su liberación.	Pérdida de datos críticos, interrupción de operaciones, altos costos de recuperación.	En 2023, el 37% de las PYMEs latinoamericanas afectadas por ransomware no lograron recuperar sus datos (ESET, 2024).

Phishing	Técnica de ingeniería social que suplanta identidades para obtener credenciales o datos sensibles.	Robo de cuentas de acceso, fraudes financieros, daño a la reputación.	Según CISCO (2023), el 86% de las brechas en PYMEs comenzaron con correos de phishing.
Ataques DDoS	Sobrecarga deliberada de servidores mediante múltiples solicitudes falsas para interrumpir servicios.	Pérdida de disponibilidad de plataformas, caídas de ventas, pérdida de confianza del cliente.	Cloudflare (2023) reportó que los sectores e-commerce y retail son los más afectados por ataques DDoS durante eventos de alto tráfico como Black Friday.
Robo de credenciales	Acceso no autorizado a través de la obtención ilícita de usuarios y contraseñas.	Acceso a cuentas internas o de clientes, modificación de pedidos, exposición de información privada.	Verizon (2023) encontró que el 61% de los incidentes en comercio electrónico involucran credenciales comprometidas.
Fraude en pagos electrónicos	Manipulación o interceptación de transacciones digitales con fines de lucro ilícito.	Reembolsos falsos, pérdida financiera, disputas legales con clientes.	Statista (2023) indica que los fraudes en pagos electrónicos representaron pérdidas de más de $41.000 millones globalmente.
Errores de configuración	Fallos humanos o técnicos en la configuración de plataformas y sistemas de seguridad.	Accesos no autorizados, exposición pública de información sensible.	Un informe de IBM (2023) indica que el 14% de las brechas se deben a errores de configuración.
Sistemas obsoletos/no actualizados	Infraestructuras con software desactualizado, sin parches de seguridad recientes.	Vulnerabilidades expuestas a exploits conocidos, infección por malware, pérdida de soporte técnico.	CISA (2022) reportó que el 60% de los ataques exitosos a PYMEs se realizaron contra sistemas con más de 3 meses sin actualizaciones.

Nota. La tabla presenta las amenazas cibernéticas más frecuentes que afectan a las pequeñas y medianas empresas en el sector del comercio electrónico, incluyendo su descripción y el impacto potencial en la seguridad.

Análisis Detallado de las Principales Amenazas

El Ransomware

Es un tipo de software malicioso que cifra los archivos del usuario, impidiendo su acceso hasta que se pague un rescate. Este, continúa siendo una de las amenazas más devastadoras para el comercio electrónico, según el informe de (Sophos, 2024), el 66 % de las PYMEs atacadas por ransomware terminaron pagando el rescate, afectando gravemente su estabilidad financiera. En América Latina, los incidentes por ransomware aumentaron un 25 % en el último año(eset, 2024). Estos ataques no solo secuestran la información de los sistemas de venta en línea, sino que paralizan operaciones completas, afectando tanto ingresos como la credibilidad de los usuarios finales. La falta de Backup seguros y planes de respuesta rápida sigue siendo un problema crítico en las PYMEs del sector.

Este tipo de amenaza encuentra terreno fértil en las múltiples vulnerabilidades comunes en las PYMEs, tales como la ausencia de copias de seguridad aisladas y actualizadas, que impide una recuperación efectiva tras un incidente. Además, muchas organizaciones operan con software desactualizado y sin aplicar parches de seguridad, lo que deja abiertas brechas fácilmente explotables por los ciberdelincuentes. Otro factor crítico es la existencia de permisos excesivos para usuarios comunes, que facilitan la propagación del malware una vez que infecta un equipo. A esto se suma la falta de segmentación de red, lo que permite que el ransomware se extienda rápidamente por toda la infraestructura. Finalmente, la baja concienciación del personal frente a correos sospechosos y la carencia de herramientas avanzadas de detección y respuesta ante amenazas aumentan considerablemente el riesgo de infección. Estas debilidades, si no se abordan de forma integral, comprometen seriamente la resiliencia cibernética de las pequeñas empresas frente a este tipo de ataques.

Phishing

El phishing es una técnica de ingeniería social en la que los atacantes se hacen pasar por entidades de confianza para engañar a las víctimas y obtener información confidencial, como credenciales de acceso o datos financieros; generalmente, se realiza a través de correos electrónicos fraudulentos que contienen enlaces a sitios web falsos diseñados para recopilar información sensible.

El phishing representa el vector de ataque inicial en más del 80 % de los incidentes de seguridad en plataformas de comercio electrónico, según el Data Breach Investigations Report de (verizon, 2023). A través de correos electrónicos fraudulentos, los atacantes logran obtener credenciales de administradores o datos de clientes. Esto facilita accesos ilegítimos a sistemas de pago y bases de datos sensibles. En América Latina, las campañas de phishing han crecido un 30 % en los últimos dos años (eset, 2024), afectando principalmente a pequeñas tiendas digitales sin políticas estrictas de verificación de identidad

En el entorno de las PYMEs del sector retail y comercio electrónico, este tipo de amenaza se ve facilitado por una serie de vulnerabilidades recurrentes. Entre ellas se destaca la falta de formación y sensibilización del personal sobre técnicas de suplantación, lo que hace que muchos empleados no logren identificar correos fraudulentos o enlaces sospechosos. También influye la carencia de herramientas de filtrado antiphishing y la inexistencia de mecanismos de autenticación robusta, como la autenticación multifactor (MFA), que podría prevenir el uso indebido de credenciales incluso si estas son comprometidas. Asimismo, es común que los sistemas no cuenten con políticas de acceso mínimamente privilegiadas, permitiendo que un atacante, al obtener una sola cuenta, tenga acceso a múltiples servicios o datos sensibles. Estas condiciones convierten al phishing en una amenaza altamente efectiva, especialmente en

entornos donde la cultura de seguridad aún no está plenamente desarrollada y la infraestructura tecnológica carece de medidas de control proactivas.(Gonzales Llorente, 2023)

Ataques DDoS

Los ataques de denegación de servicio (DDoS) se han incrementado en un 200 % durante eventos de alto tráfico como Black Friday y Cyber Monday, según el Global Ecommerce Security Report de (webscale, 2022). Estos ataques buscan saturar los servidores de las plataformas de e-commerce, provocando caídas y pérdidas de ventas significativas. Para las PYMEs, un ataque DDoS puede significar no solo la interrupción temporal de sus servicios, sino también el daño a la percepción de confiabilidad ante sus clientes, muchos de estos ataques provienen de redes de bots automatizados, difíciles de detectar con protecciones tradicionales; además estos ataques pueden ser utilizados como distracción mientras se llevan a cabo otras actividades maliciosas, como el robo de datos.(Babu, 2024)

Este tipo de amenaza es particularmente eficaz en PYMEs debido a una serie de vulnerabilidades estructurales. En primer lugar, muchas organizaciones carecen de infraestructura escalable o de servicios de mitigación específicos contra DDoS, como firewalls avanzados con detección de tráfico anómalo o soluciones de red distribuidas que absorban la carga maliciosa. Además, es común que los servidores y servicios estén directamente expuestos a Internet sin la implementación de mecanismos de balanceo de carga o segmentación lógica que limite la superficie de ataque. La ausencia de monitoreo en tiempo real y alertas tempranas también dificulta una respuesta oportuna, lo que permite que el ataque cause mayor daño antes de ser detectado. Estas debilidades convierten a las plataformas digitales de las PYMEs en blancos fáciles para atacantes que buscan interrumpir sus operaciones, afectar la experiencia del

cliente y, en muchos casos, extorsionar a los propietarios a cambio del restablecimiento del servicio.

Robo de Credenciales

El hurto de credenciales se refiere a la adquisición ilegal de nombres de usuario y claves. esto posibilita que los atacantes ingresen a cuentas personales y lleven a cabo acciones fraudulentas. Estos actos constituyen el 61% de las vulnerabilidades de seguridad en el comercio electrónico, según (verizon, 2023). Las malas contraseñas, el almacenamiento inseguro de información y la ausencia de autenticación multifactor promueven el ingreso no permitido a sistemas esenciales. Una vez infiltrados, los intrusos tienen la capacidad de ejecutar estafas, sustraer datos de los clientes o alterar los registros financieros. En América Latina, los hurtos de claves se incrementaron particularmente en pequeñas y medianas empresas que no implementan sistemas de cifrado sólidos ni protocolos de acceso seguros a plataformas de pago y gestión.

Las vulnerabilidades que posibilitan el robo de credenciales en las PYMEs son diversas y, en muchos casos, evitables. Una de las principales es el uso de contraseñas débiles o repetidas en múltiples plataformas, lo que facilita su descifrado mediante ataques de fuerza bruta o su reutilización en accesos no autorizados. A esto se suma la ausencia de políticas sólidas de gestión de contraseñas, como la caducidad periódica, el almacenamiento seguro o la autenticación multifactor (MFA), que podría actuar como una segunda barrera de protección. Otro aspecto crítico es la falta de visibilidad sobre los accesos privilegiados, permitiendo que una sola cuenta comprometida tenga control sobre varios sistemas o funciones sensibles. Además, muchas organizaciones no cuentan con mecanismos de monitoreo o alertas sobre accesos inusuales, lo que impide una detección temprana del uso fraudulento de credenciales. Esta combinación de

debilidades facilita que un atacante, una vez dentro, actúe con relativa libertad y sin ser detectado, comprometiendo la integridad de los datos y la confianza de los clientes.

Fraude en Pagos Electrónicos

El fraude en los pagos digitales incluye varias estrategias empleadas por los ciberdelincuentes para llevar a cabo operaciones no permitidas. Según (Cybersecurity Ventures, 2020), se calcularon las pérdidas mundiales debido a fraudes en transacciones digitales en 6 billones de dólares en 2021 y se prevén en 10,5 billones para 2025. Los fraudes abarcan el empleo de tarjetas hurtadas, alteración de plataformas de pago y operaciones falsas. La ausencia de autenticación sofisticada y análisis en tiempo real del comportamiento de compra son elementos que añaden a esta vulnerabilidad en pequeños comercios en línea.

Este tipo de estafa no solo provoca daños financieros directos, sino que también puede perjudicar la reputación de las compañías perjudicadas y reducir la confianza de los usuarios en las adquisiciones en línea. (Babu, 2024)

Las vulnerabilidades asociadas a esta amenaza son múltiples. En primer lugar, muchas plataformas no implementan métodos robustos de verificación de pagos, como la autenticación 3D Secure o el análisis de patrones de comportamiento de compra. También es común que las conexiones entre la tienda en línea y las pasarelas de pago no cuenten con cifrado fuerte o certificación SSL/TLS adecuada, exponiendo los datos financieros a posibles interceptaciones. Otra debilidad frecuente es la falta de mecanismos para detectar y bloquear transacciones sospechosas en tiempo real, como múltiples intentos de pago fallidos desde una misma dirección IP o el uso de tarjetas emitidas en países de alto riesgo. Además, algunas PYMEs almacenan datos de tarjetas de forma inadecuada, sin cumplir con los estándares PCI-DSS, lo que las convierte en objetivos atractivos para el robo masivo de información financiera. Estas

vulnerabilidades, sumadas a la escasa supervisión de los procesos de pago y conciliación contable, aumentan significativamente la probabilidad de sufrir fraudes electrónicos con impacto directo en los ingresos y la reputación de la empresa.

Errores de Configuración y Accesos no Autorizados

Errores de configuración, especialmente en servicios cloud y bases de datos de comercio electrónico, son responsables de una gran parte de las brechas de seguridad en PYMEs. Según (Checkpoint, 2025), aproximadamente el 45 % de las filtraciones de datos se debe a configuraciones incorrectas o falta de restricciones adecuadas en los sistemas. Esto incluye servidores expuestos, permisos excesivos y falta de actualizaciones de seguridad en infraestructuras web. Estos errores son aprovechados por atacantes para acceder a información sensible sin necesidad de explotar vulnerabilidades técnicas complejas.

Además, la falta de autenticación multifactor y controles de acceso estrictos facilita que personas no autorizadas accedan a sistemas críticos, poniendo en riesgo la integridad y confidencialidad de los datos. Implementar medidas como firewalls y seguridad de red es esencial para monitorear y bloquear intentos de intrusión, protegiendo así los activos digitales de la empresa.(Roch Moraguez, 2025)

Este tipo de amenazas se ve facilitado por la inexistencia de políticas claras de gestión de accesos y permisos, lo que permite que usuarios con roles administrativos mantengan privilegios innecesarios o compartan cuentas entre áreas. También es común la falta de auditoría y monitoreo de accesos, lo que impide detectar intrusiones o movimientos laterales dentro de la red. Además, en entornos donde no se aplican controles de seguridad como firewalls internos, listas blancas o segmentación de servicios, cualquier error de configuración puede convertirse en una puerta abierta para atacantes. Estas debilidades evidencian la necesidad urgente de aplicar

principios de seguridad por defecto y de mínimo privilegio, así como el uso de herramientas automatizadas para validar la correcta configuración de los activos tecnológicos.

Falta de Actualizaciones y Sistemas Obsoletos

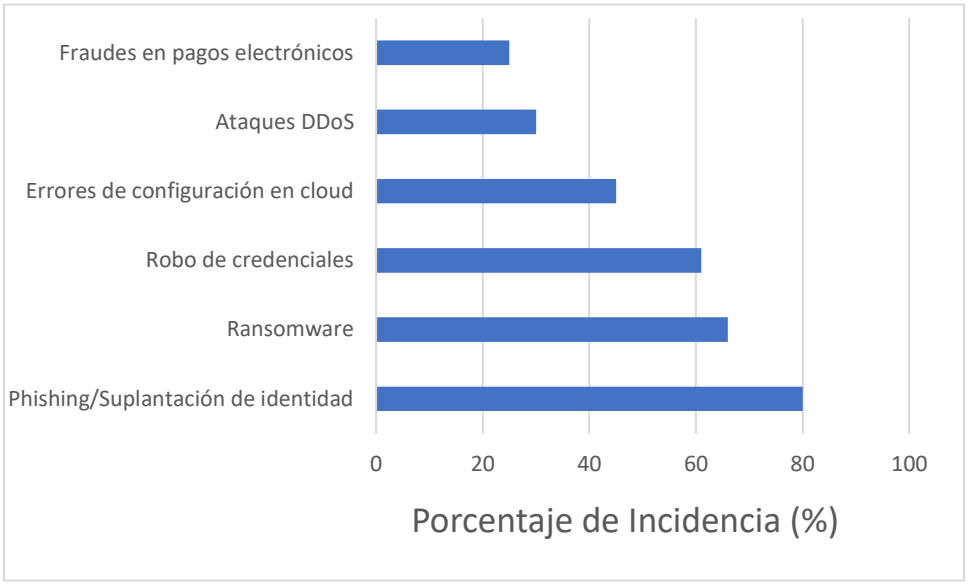
La utilización de programas y sistemas anticuados continúa siendo una de las principales falencias de las PYMEs en el comercio electrónico. Según (ENISA, 2025), el 35% de los incidentes de seguridad en pequeñas empresas son resultado de la explotación de debilidades detectadas, pero no corregidas. Las aplicaciones de comercio electrónico, pasarelas de pago y sistemas de stock antiguos poseen vulnerabilidades esenciales que los ciberdelincuentes pueden aprovechar de manera sencilla.

Las vulnerabilidades asociadas a esta amenaza tienen su origen en la falta de una política estructurada de gestión de actualizaciones. Muchas empresas no disponen de herramientas para el control de versiones ni de inventarios actualizados de sus activos tecnológicos, lo que dificulta la identificación de software obsoleto o vulnerable. A esto se suma el temor al impacto de las actualizaciones sobre la operatividad de los sistemas, lo cual lleva a aplazar indefinidamente los parches de seguridad. También es frecuente encontrar aplicaciones heredadas que siguen activas por dependencia operativa, pero que ya no reciben soporte técnico ni actualizaciones. Estas condiciones hacen que las PYMEs operen con un nivel de exposición alto ante amenazas automatizadas que escanean permanentemente la red en busca de estos puntos débiles. Adoptar un enfoque de actualización continua, junto con mecanismos de virtualización y pruebas en entornos controlados, se vuelve fundamental para reducir este tipo de riesgo.

Además, sistemas heredados basados en infraestructuras envejecidas y software obsoleto luchan por mantenerse al día con las demandas de la lógica comercial moderna, convirtiéndose en un obstáculo para el crecimiento y la innovación del negocio(Rasectech, 2023)

Figura 3

¿Qué Tan Vulnerables Somos? Ranking de Ciberamenazas más Frecuentes



Nota. La figura presenta un ranking de las ciberamenazas más frecuentes que afectan a las PYMEs del sector retail y comercio electrónico, destacando la prevalencia de ataques como ransomware, phishing y robo de credenciales. El gráfico permite visualizar el nivel de riesgo asociado a cada amenaza, facilitando la priorización de medidas de seguridad y estrategias de mitigación. Elaboración propia en Excel

Estrategias de Seguridad Tradicionales en Pymes del Comercio Electrónico

Las pequeñas y medianas empresas que operan en el comercio electrónico se enfrentan a una creciente presión para fortalecer su ciberseguridad. Aunque muchas de estas organizaciones inician con herramientas básicas como firewalls y antivirus, cada vez es más común que integren soluciones más sofisticadas para proteger sus activos digitales y garantizar la confianza y fidelización de sus clientes, por ejemplo, herramientas como Bitdefender, Sophos o Kaspersky

Small Office Security ofrecen protección avanzada contra malware, ransomware y amenazas web, diseñadas específicamente para entornos de pequeña empresa. Estas soluciones brindan un equilibrio entre eficacia y facilidad de uso, algo importante para las PYMEs que no siempre cuentan con personal técnico especializado.(Docusign, 2022)

Además, muchas empresas han comenzado a incorporar plataformas EDR (Endpoint Detection and Response)(Aarness, 2024), como CrowdStrike Falcon, SentinelOne o Microsoft Defender for Business, que permiten una detección más proactiva de comportamientos anómalos en los dispositivos. Estas herramientas no solo detectan amenazas, sino que también permiten contenerlas y remediarlas rápidamente. De forma complementaria, algunas Pymes están utilizando SIEM (Security Information and Event Management) como Splunk, QRadar o soluciones open source como Wazuh, que integran y analizan registros de actividad en la red para identificar patrones sospechosos o violaciones a políticas de seguridad.

En el ámbito del control de accesos, es cada vez más común que las Pymes implementen autenticación multifactor (MFA) en sus plataformas de comercio electrónico, sistemas administrativos y correos corporativos. Herramientas como Google Authenticator, Microsoft Authenticator o soluciones integradas en servicios como AWS, Google Cloud o Azure, facilitan esta medida sin representar un costo elevado. También se están adoptando con mayor frecuencia las soluciones IAM (Identity and Access Management), que permiten asignar permisos basados en roles, automatizar procesos de alta y baja de usuarios, y auditar el acceso a sistemas críticos, asegurando una trazabilidad completa.

Respecto a las políticas internas, cada vez más PYMEs están estructurando y documentando protocolos de seguridad que incluyen desde el uso obligatorio de contraseñas robustas, hasta normas para el teletrabajo seguro y el manejo de la información sensible. Estas

políticas no solo buscan proteger la información, sino también fomentar una cultura de seguridad organizacional, donde todos los colaboradores comprendan su rol frente a las amenazas digitales. De hecho, muchas empresas han comenzado a capacitar a sus equipos mediante plataformas como KnowBe4 o cursos de concienciación en ciberseguridad ofrecidos por entidades gubernamentales y privadas.

Otra práctica en aumento es la implementación de copias de seguridad automáticas en la nube, con soluciones como Acronis, Veeam, Google Workspace Backup o Microsoft OneDrive for Business, que permiten restaurar operaciones rápidamente ante incidentes como ransomware o pérdida de datos. Además, en el frente de las comunicaciones, se están adoptando herramientas que aseguran el cifrado de extremo a extremo, tanto para correos electrónicos como para chats internos, usando soluciones como ProtonMail, Tutanota, Signal o Slack con cifrado habilitado.

Sin embargo, un reto persistente es la actualización tecnológica. Muchas PYMEs aún utilizan sistemas obsoletos o no parchean sus aplicaciones a tiempo, lo que deja puertas abiertas a ataques comunes. Para mitigar este riesgo, se han comenzado a usar herramientas de gestión de vulnerabilidades como Nessus Essentials o OpenVAS, que escanean la infraestructura en busca de configuraciones débiles o software desactualizado. Aunque su adopción aún es baja, representan un paso significativo hacia una postura de seguridad más madura.

A pesar de la implementación de estas medidas tradicionales, las Pymes enfrentan desafíos significativos ante amenazas cibernéticas cada vez más sofisticadas. Los firewalls y antivirus convencionales pueden ser insuficientes para detectar y mitigar ataques avanzados, como el ransomware o las amenazas persistentes avanzadas (APT), que emplean técnicas evasivas para infiltrarse en los sistemas. Además, los IDS pueden generar falsos positivos o no identificar nuevas formas de ataque si no se actualizan constantemente. La dependencia

exclusiva en estas herramientas puede generar una falsa sensación de seguridad, dejando a las empresas vulnerables a brechas que podrían tener consecuencias devastadoras. Es esencial que las PYMEs complementen estas estrategias con soluciones más avanzadas, como sistemas de detección y respuesta en endpoints (EDR) y plataformas de gestión de eventos e información de seguridad (SIEM), para enfrentar eficazmente el panorama actual de amenazas.

Finalmente, cabe resaltar que las PYMEs, motivadas por la necesidad de cumplir con normativas como la Ley 1581 de 2012 de Protección de Datos Personales en Colombia o estándares como PCI DSS para manejo de datos financieros, han empezado a documentar e implementar políticas de cumplimiento. Esto incluye definir responsables de seguridad de la información, registrar bases de datos ante la SIC (Superintendencia de Industria y Comercio), y establecer protocolos de respuesta ante incidentes**.**

Blockchain como Tecnología Emergente en el Fortalecimiento de la Resiliencia Cibernética en Pymes del Sector Retail y Comercio Electrónico

La resiliencia cibernética se define como la capacidad de una organización para anticipar, resistir, recuperarse y adaptarse ante condiciones adversas del entorno digital, incluyendo ciberataques, fallas tecnológicas y errores humanos. En el contexto de las pequeñas y medianas empresas Pyme del sector retail y comercio electrónico, esta resiliencia se convierte en un factor importante para garantizar la continuidad del negocio, proteger los datos sensibles de clientes y mantener la seguridad de los usuarios finales.

Frente a esta necesidad, la tecnología Blockchain ofrece un enfoque disruptivo para reforzar la resiliencia digital desde tres dimensiones clave: prevención, resistencia y recuperación.

Prevención: minimizar vectores de ataque mediante descentralización y autenticación segura

La arquitectura descentralizada de Blockchain elimina los puntos únicos de falla que caracterizan a los sistemas tradicionales basados en servidores centrales. Al distribuir la información entre múltiples nodos, se dificulta la manipulación maliciosa de datos y se reduce la superficie de ataque para técnicas como el ransomware o el secuestro de bases de datos.

Además, la autenticación basada en claves criptográficas elimina la dependencia de contraseñas vulnerables, permitiendo esquemas de identidad digital donde el usuario conserva el control sobre su información personal. Esto refuerza la confidencialidad y dificulta ataques de suplantación de identidad, especialmente frecuentes en el comercio electrónico.

Resistencia: mantener la integridad y disponibilidad frente a incidentes

Uno de los pilares de Blockchain es su inmutabilidad: una vez que los datos son registrados en la cadena, no pueden ser modificados sin consenso de la red. Esto asegura la integridad de los registros, incluso si uno o varios nodos han sido comprometidos. En términos operativos, esto permite a las PYME registrar logs de auditoría, movimientos financieros o trazabilidad de productos sin riesgo de alteración maliciosa o accidental.

La disponibilidad también se ve fortalecida gracias a la redundancia distribuida. Incluso si un nodo es atacado o sufre una interrupción, el resto de la red mantiene el acceso a la información. Esto permite continuar operaciones con mínima interrupción, lo que es esencial para negocios digitales que operan 24/7.

Recuperación: facilitar análisis forense, trazabilidad y continuidad

Ante un incidente de seguridad, la trazabilidad que ofrece Blockchain facilita el análisis forense posterior. Cada transacción queda registrada cronológicamente, con referencias criptográficas que permiten rastrear su origen, destino y momento exacto de ejecución. Esta capacidad permite no solo investigar lo ocurrido, sino también detectar vulnerabilidades estructurales y mejorar las estrategias de respuesta futuras.

Además, Blockchain permite construir sistemas de respaldo descentralizado que, combinados con contratos inteligentes, activan automáticamente procedimientos de contingencia en caso de detección de incidentes. Por ejemplo, ante una alteración sospechosa en el sistema de pedidos, podría ejecutarse una alerta automática o activar un mecanismo de validación externo para bloquear transacciones maliciosas.

Adaptabilidad a Pymes: escalabilidad y modelos accesibles

Un argumento recurrente contra la adopción de Blockchain en PYMEs es su supuesta complejidad técnica y alto costo. Sin embargo, el surgimiento de modelos Blockchain-as-a-

Service (BaaS) como los ofrecidos por IBM, Amazon Web Services o Microsoft Azure ha democratizado el acceso a esta tecnología. Estos servicios permiten a las Pymes implementar soluciones escalables, seguras y personalizables sin necesidad de mantener infraestructura propia ni equipos técnicos especializados.

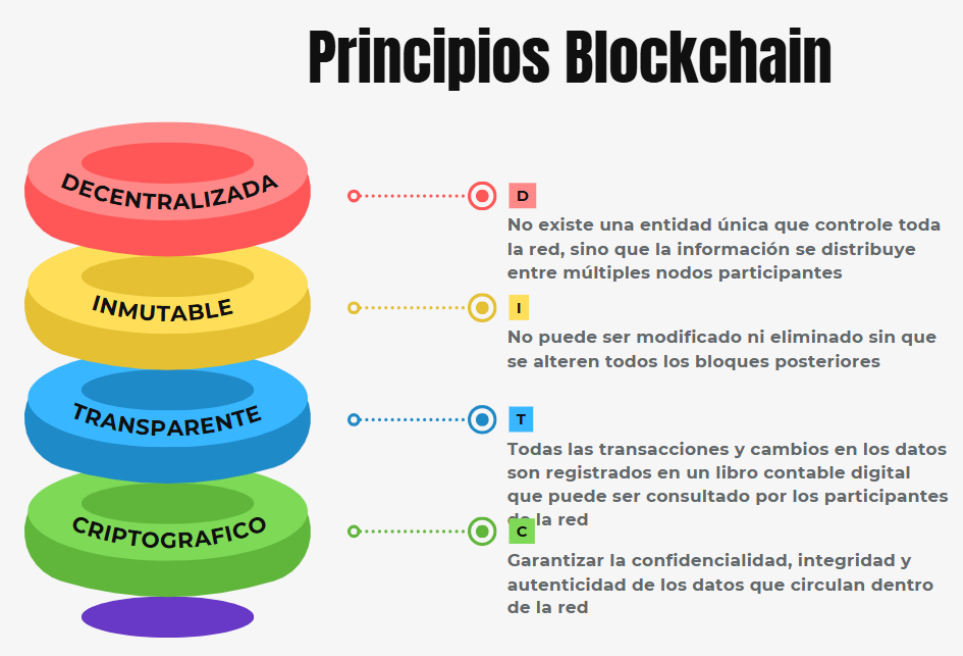
En este sentido, Blockchain no solo fortalece la seguridad, sino que también se convierte en una palanca de transformación digital, alineando la protección de activos con los objetivos estratégicos del negocio.

Principios Fundamentales de Blockchain

La Figura 4 ilustra los principios fundamentales que sustentan la tecnología Blockchain, destacando los elementos que garantizan su seguridad, transparencia y confiabilidad. Estos principios son la base de su aplicabilidad en entornos empresariales, especialmente en el comercio electrónico y el sector retail.

Figura 4

Principios de Blockchain



Nota. La figura representa los principios clave de la tecnología Blockchain, incluyendo descentralización, inmutabilidad, transparencia, consenso y seguridad criptográfica. Estos elementos permiten el almacenamiento y transmisión de información de manera confiable, sin necesidad de intermediarios y con resistencia frente a alteraciones no autorizadas. Elaboración propia en Canva.com

Descentralización y Eliminación de Intermediarios en Procesos de Seguridad

Uno de los pilares fundamentales de la tecnología Blockchain es su naturaleza descentralizada, lo cual significa que no existe una entidad única que controle toda la red, sino que la información se distribuye entre múltiples nodos participantes. Esta arquitectura representa una ruptura con los modelos tradicionales centralizados, en los que la seguridad y la gestión de la información dependen de servidores únicos o autoridades centralizadas que, al verse comprometidas, pueden poner en riesgo la integridad del sistema completo

La descentralización de Blockchain contribuye directamente a la mejora de los procesos de seguridad al eliminar los puntos únicos de falla. En lugar de confiar en intermediarios o terceros de confianza para validar transacciones o proteger la información, Blockchain permite que estos procesos se realicen de forma automatizada mediante consensos criptográficos distribuidos. Esto no solo reduce la posibilidad de ataques dirigidos a entidades centrales, sino que también limita la manipulación de datos por actores maliciosos internos o externos.(Antoniucci et al., 2024)

La eliminación de intermediarios en los procesos de verificación y validación también implica una reducción en los costos operativos y una mejora en la eficiencia, ya que las transacciones pueden ejecutarse directamente entre las partes involucradas. Además, la veracidad

de las operaciones es garantizada por la red de nodos mediante mecanismos como Proof of Work (PoW), Proof of Stake (PoS) u otros algoritmos de consenso, lo que asegura que solo los registros legítimos y verificables sean añadidos al libro mayor

Desde el punto de vista de la ciberseguridad, esta propiedad descentralizada impide que actores maliciosos alteren los registros sin el consenso de la mayoría de los nodos, elevando considerablemente la resistencia ante ataques como el spoofing, la alteración de registros y las intrusiones. En sectores como el comercio electrónico y el retail, donde el volumen de transacciones digitales es elevado, esta arquitectura ofrece una robustez significativamente mayor frente a los sistemas tradicionales.

Inmutabilidad y su Impacto en la Integridad de Datos y Transacciones

La inmutabilidad es una de las características técnicas más distintivas de la tecnología Blockchain y desempeña un papel esencial en la protección de la integridad de los datos. En términos simples, una vez que una transacción es registrada en un bloque y este bloque es añadido a la cadena, no puede ser modificado ni eliminado sin que se alteren todos los bloques posteriores, lo que requeriría la aprobación de la mayoría de los nodos de la red. Esta característica confiere a Blockchain un alto nivel de resistencia frente a la manipulación de información (García Munguía et al., 2022)

Este atributo es especialmente importante en contextos empresariales donde la veracidad de la información y el cumplimiento normativo son críticos. En el sector del comercio electrónico, por ejemplo, la inmutabilidad garantiza que los registros de transacciones no puedan ser alterados por terceros con fines fraudulentos, lo cual es crucial para proteger tanto a los consumidores como a los comerciantes. Además, proporciona una trazabilidad confiable que puede ser auditada fácilmente, mejorando la transparencia en las operaciones comerciales.

Desde una perspectiva de ciberseguridad, la inmutabilidad fortalece la integridad de los datos, uno de los pilares fundamentales de la seguridad de la información, junto con la confidencialidad y la disponibilidad. Los sistemas tradicionales son vulnerables a modificaciones no autorizadas, ya sea por errores humanos, ataques de malware o accesos indebidos. En contraste, Blockchain impide técnicamente estas alteraciones al asegurar criptográficamente cada bloque con una función hash única que está enlazada al bloque anterior.

Asimismo, esta propiedad facilita la detección de intentos de modificación. Cualquier cambio en los datos originales altera el hash del bloque afectado, rompiendo la cadena de validación y alertando a la red. Este nivel de control no solo impide el fraude, sino que también proporciona evidencia digital sólida para investigaciones de incidentes, fortaleciendo las capacidades forenses en caso de ciberataques o disputas contractuales.(García Munguía et al., 2022)

Transparencia y Trazabilidad en la Gestión de Información en E-commerce

La transparencia y la trazabilidad son dos principios clave que la tecnología Blockchain aporta a los entornos digitales, especialmente en el comercio electrónico, donde la confianza del consumidor y la integridad de la cadena de suministro son fundamentales. En un sistema basado en Blockchain, todas las transacciones y cambios en los datos son registrados en un libro contable digital que puede ser consultado por los participantes de la red, lo que promueve una gestión de información más abierta y verificable

En el ámbito del e-commerce, la transparencia mejora la relación entre consumidores y vendedores al ofrecer visibilidad total sobre el ciclo de vida de un producto o servicio. Por ejemplo, los clientes pueden rastrear el origen de un artículo, sus etapas de fabricación, almacenamiento y distribución, simplemente accediendo al historial registrado en Blockchain.

Esto no solo refuerza la credibilidad del vendedor, sino que también permite al consumidor tomar decisiones informadas basadas en evidencia objetiva.

La trazabilidad, por su parte, permite seguir el rastro de cada operación o evento dentro de una cadena logística o transaccional, registrando de manera inmutable quién hizo qué, cuándo y cómo. En el caso de las plataformas de comercio digital, esto es particularmente útil para detectar irregularidades en pagos, envíos, devoluciones o quejas. De este modo, se pueden evitar disputas o resolverlas de manera eficiente, gracias a los registros auditables que provee Blockchain.

Estas capacidades también fortalecen la ciberseguridad. Al permitir la auditoría completa de las operaciones y la detección temprana de anomalías, Blockchain ayuda a prevenir fraudes internos y externos. Además, al no depender de un ente centralizado para validar las transacciones, se reduce el riesgo de manipulación o corrupción de los datos por actores malintencionados.

En resumen, la transparencia y la trazabilidad basadas en Blockchain no solo generan un entorno comercial más confiable, sino que también potencian la seguridad de los datos y procesos en el comercio electrónico, lo cual representa una ventaja competitiva clave, especialmente para las PYMEs que necesitan fortalecer su reputación digital.(Alzate et al., 2023)

Uso de Criptografía y Contratos Inteligentes para Mejorar la Seguridad

La criptografía es uno de los pilares esenciales que sustenta la seguridad de Blockchain. En este contexto, se utiliza para garantizar la confidencialidad, integridad y autenticidad de los datos que circulan dentro de la red. Cada transacción realizada en una cadena de bloques es cifrada utilizando algoritmos criptográficos avanzados, como SHA-256 o firmas digitales, los cuales impiden que los datos sean manipulados sin ser detectados

En plataformas de comercio electrónico, esto significa que la información financiera, las credenciales de acceso y los registros de compra están protegidos contra accesos no autorizados, suplantaciones de identidad o alteraciones maliciosas. La criptografía asimétrica basada en claves públicas y privadas permite que solo los usuarios autorizados puedan firmar o descifrar transacciones, fortaleciendo el control de acceso y autenticación en los sistemas digitales.

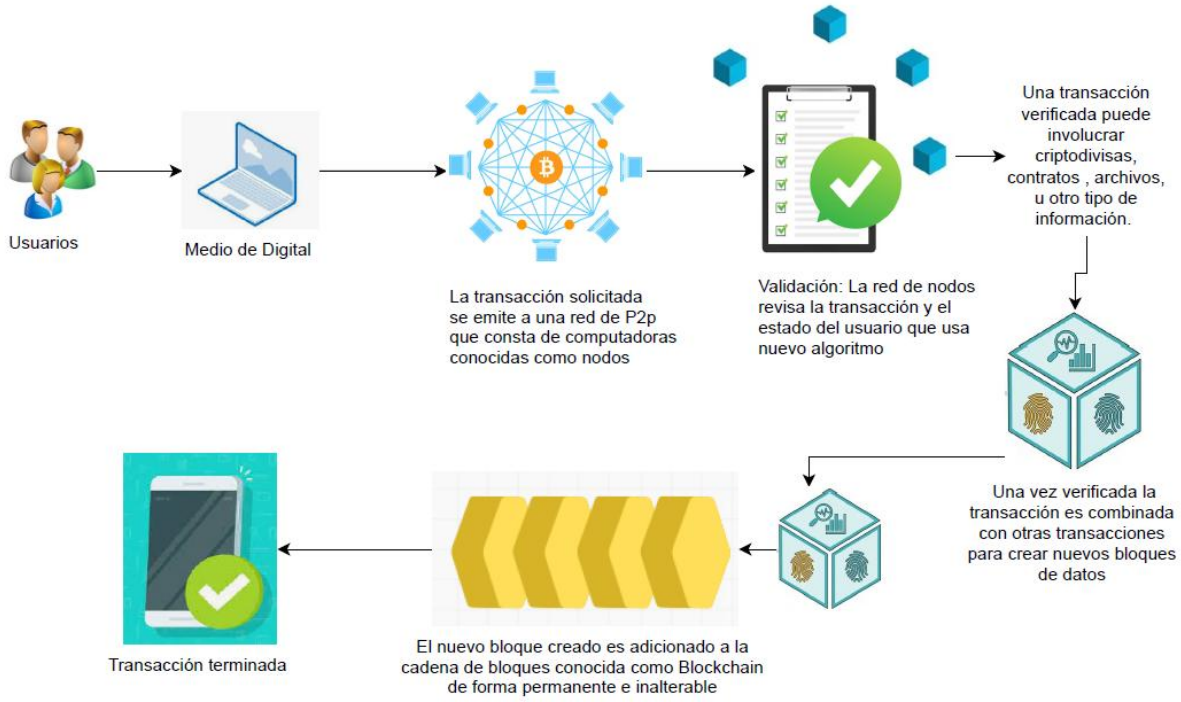
Por otro lado, los contratos inteligentes representan una innovación que amplifica la seguridad y automatización en los entornos digitales. Estos son fragmentos de código que se ejecutan automáticamente en Blockchain cuando se cumplen ciertas condiciones predefinidas. Al estar programados para operar sin intervención humana, eliminan el riesgo de errores o manipulaciones por parte de terceros y permiten realizar acuerdos digitales de forma segura, transparente y verificable.

En el comercio electrónico, los contratos inteligentes pueden usarse para validar pagos, controlar entregas, gestionar devoluciones y aplicar penalidades automáticamente si alguna parte incumple el acuerdo. Esta automatización no solo reduce los costos operativos y burocráticos, sino que también minimiza los riesgos de fraude y conflictos legales, ya que todo queda registrado de forma inmutable y consensuada por la red.(Rosales Álvarez et al., 2023)

A continuación, ilustra el proceso general de una transacción digital en Blockchain, destacando su validación descentralizada, agrupación en bloques y registro inmutable. Esta arquitectura refuerza la integridad, trazabilidad y seguridad de las operaciones en plataformas de e-commerce.

Figura 5

Arquitectura Blockchain Aplicada al Comercio Electrónico en PYMEs



Nota. La figura describe la arquitectura de una solución Blockchain aplicada al comercio electrónico en PYMEs, en la que se incluyen componentes como la capa de red, los nodos validadores, los contratos inteligentes y la interfaz de usuario. Esta estructura permite mejorar la trazabilidad, optimizar la gestión de pagos y reforzar la protección contra fraudes en entornos digitales. Elaboración propia en Canva.com

Evolución de Blockchain en Entornos Empresariales

Desde su creación en 2008 como la tecnología subyacente de Bitcoin, Blockchain ha pasado de ser un sistema experimental de criptomonedas a una infraestructura tecnológica con un amplio espectro de aplicaciones empresariales. En sus inicios, el uso de Blockchain se limitaba a la transferencia de valor sin intermediarios. Sin embargo, a medida que las organizaciones

identificaron su potencial para garantizar transparencia, trazabilidad y seguridad, comenzaron a surgir soluciones enfocadas en otros sectores económicos (Lansiti & Lakhani, 2020)

A partir de 2015, con la aparición de plataformas como Ethereum, que introdujeron los contratos inteligentes, Blockchain adquirió una mayor capacidad de personalización y automatización de procesos empresariales. Esto marcó un hito en su evolución, ya que permitió la implementación de reglas de negocio codificadas que se ejecutan de forma automática y segura, sin intervención humana (Taylor et al., 2020)Desde entonces, las empresas han comenzado a explorar su utilidad en áreas como la gestión de la cadena de suministro, la identidad digital, la auditoría, la ciberseguridad y el cumplimiento normativo.

Actualmente, grandes corporaciones como IBM, Microsoft, Amazon y Oracle ofrecen servicios de Blockchain-as-a-Service (BaaS), permitiendo a pequeñas y medianas empresas acceder a esta tecnología sin necesidad de invertir en infraestructura compleja (Zheng et al., 2018). Además, organismos internacionales como la OCDE y el Foro Económico Mundial han reconocido el valor estratégico de Blockchain para la transformación digital de las empresas y la mejora de sus prácticas de gobernanza y seguridad.

Uno de los principales impulsores de su adopción ha sido la necesidad de reforzar la confianza en entornos empresariales cada vez más digitalizados. En sectores como el comercio electrónico y retail, Blockchain se utiliza para certificar el origen de productos, validar la autenticidad de transacciones, y proteger la información del cliente frente a fraudes y ciberataques. Así, la evolución de esta tecnología ha estado marcada por su transición de un modelo abierto y descentralizado (como Bitcoin) hacia modelos híbridos y privados que responden a las necesidades de control, escalabilidad y confidencialidad de las organizaciones.(Burgos, 2024)

A medida que los marcos regulatorios y las normativas de seguridad digital se consolidan, se espera que Blockchain continúe su integración en entornos empresariales como un componente clave de las estrategias de ciberseguridad, resiliencia operativa y transformación digital.

Importancia en el Sector Retail y Comercio Electrónico

El sector retail y el comercio electrónico enfrentan desafíos significativos en materia de ciberseguridad, trazabilidad de productos, protección de datos personales y prevención del fraude. En este contexto, Blockchain ha emergido como una tecnología estratégica que puede transformar la forma en que las empresas gestionan sus operaciones digitales y la confianza con sus clientes. Su capacidad para garantizar la integridad y transparencia de la información resulta particularmente valiosa en sectores donde la interacción en línea y las transacciones digitales son constantes.

Una de las aplicaciones más destacadas de Blockchain en el comercio electrónico es la trazabilidad de productos. Gracias a su estructura descentralizada e inmutable, las empresas pueden registrar cada etapa del ciclo de vida de un producto desde la fabricación hasta la entrega lo cual garantiza autenticidad y permite a los consumidores verificar el origen de lo que adquieren (Kim & Laskowski, 2018) . Esto es especialmente importante para productos de alto valor, perecederos o con certificaciones de sostenibilidad.

En cuanto a la ciberseguridad, Blockchain ofrece mecanismos que reducen la vulnerabilidad ante ataques y fraudes. La protección de los datos del cliente, incluyendo métodos de pago, credenciales de acceso y registros de compras, puede fortalecerse mediante sistemas de identidad digital descentralizada, donde el usuario mantiene el control sobre su información y reduce la exposición a brechas de seguridad (Grigera del Campillo, 2022)

Además, la implementación de contratos inteligentes permite automatizar procesos clave en plataformas e-commerce, como la verificación de pagos, condiciones de entrega o gestión de reclamos, eliminando la necesidad de intermediarios y reduciendo los tiempos y errores operativos. Esto no solo mejora la experiencia del usuario, sino que también optimiza la eficiencia de la empresa.

Empresas líderes en el sector retail, como Walmart, Carrefour o Alibaba, han comenzado a utilizar soluciones basadas en Blockchain para la trazabilidad de alimentos, la gestión de inventarios y la validación de la cadena de suministro. Estos casos de éxito demuestran que la adopción de esta tecnología no solo responde a una necesidad de seguridad, sino también a una estrategia competitiva orientada a la transparencia, sostenibilidad y confianza del cliente

En definitiva, la importancia de Blockchain en el retail y el comercio electrónico radica en su capacidad para fortalecer la seguridad de las operaciones digitales, mejorar la eficiencia logística y generar un entorno de confianza en el ecosistema digital. Estas ventajas son especialmente relevantes para las pequeñas y medianas empresas (PYMEs), que buscan soluciones innovadoras y asequibles para competir en un mercado cada vez más digitalizado.(Hancco Quispe et al., 2023)

Comparación entre Blockchain y Soluciones Tradicionales de Seguridad

A diferencia de las bases de datos tradicionales, que operan bajo un modelo centralizado donde un único servidor o autoridad controla el acceso y la modificación de los datos, Blockchain distribuye la información entre múltiples nodos interconectados. Esta arquitectura descentralizada reduce significativamente los puntos únicos de fallo y dificulta los ataques dirigidos, ya que para comprometer la red es necesario alterar simultáneamente la mayoría de los nodos

Mientras que en una base de datos centralizada una intrusión puede alterar o eliminar registros sin dejar rastro inmediato, Blockchain garantiza la inmutabilidad de los datos. Cada transacción registrada es verificada por consenso y enlazada criptográficamente a bloques anteriores, lo que impide su modificación sin alertar a toda la red. Esto lo convierte en un sistema ideal para proteger registros sensibles en el comercio digital, como historiales de compra, detalles de pagos y trazabilidad de productos.(Tort, 2023)

A continuación, se presenta una comparación entre ambos enfoques, resaltando sus diferencias clave en el manejo de la ciberseguridad.

Tabla 2

Comparación Blockchain y Soluciones Tradicionales en Ciberseguridad del Comercio Electrónico

Aspecto	Soluciones Tradicionales	Blockchain
Modelo de Seguridad	Seguridad perimetral, protección basada en firmas (firewalls, antivirus, IDS/IPS).	Seguridad basada en consenso distribuido, criptografía y registros inmutables.
Prácticas comunes	Autenticación por usuario/contraseña, MFA, backups, control de acceso, políticas de seguridad.	Contratos inteligentes, identidades descentralizadas (DID), trazabilidad en cadena de bloques, BaaS.
Protección de pagos	Procesadores externos (PayU, Stripe), cifrado TLS, tokenización.	Transacciones verificables P2P sin intermediarios, validación criptográfica, reducción de fraudes.
Gestión de identidades	Autenticación centralizada, bases de datos vulnerables.	Identidad soberana, sin almacenamiento de credenciales centralizado.
Trazabilidad	Depende de ERP, registros internos (modificables).	Registro inmutable de cada transacción (pedido, entrega, devolución). Ideal para productos de alto valor o regulados.

Aspecto	Soluciones Tradicionales	Blockchain
Ventajas para e-commerce	Facilidad de uso, soluciones maduras, bajo costo inicial.	Confianza del cliente, transparencia en productos y pagos, resiliencia ante ataques y fraudes.
Desventajas para e-commerce	Dependencia de terceros (bancos, pasarelas), mayor riesgo de ataques internos o phishing.	Costos iniciales más altos, curva de aprendizaje técnica, problemas de escalabilidad si no se diseña bien.
Casos de uso reales	Plataformas con PayPal, Shopify con autenticación y cifrado TLS.	Walmart y VeChain para trazabilidad de alimentos; IBM Blockchain Payments para e-commerce global.
Aplicabilidad al retail	Protección básica de pasarelas de pago, cifrado de datos	Protección de identidad, trazabilidad de productos, pagos seguros descentralizados
Debilidades	Vulnerabilidad a ataques internos, errores humanos, dependencia de terceros	Complejidad técnica, costos iniciales, problemas de escalabilidad en blockchains públicas
Puntos de fallo	Alto riesgo de fallo único (servidor comprometido = red comprometida)	Bajo; requiere comprometer múltiples nodos simultáneamente
Escalabilidad	Limitada por infraestructura física	Escalable según modelo (blockchains privadas o híbridas)
Actualización	Necesidad constante de parches y mantenimiento manual	Actualizaciones menos frecuentes, mejoras mediante bifurcaciones (forks)
Costo de implementación	Bajo a moderado (dependiendo del tamaño de la empresa)	Inicialmente alto, pero con opciones BaaS es más accesible

Nota. La tabla compara las características clave de Blockchain frente a los métodos tradicionales de ciberseguridad utilizados en el comercio electrónico, evaluando aspectos como la integridad

de los datos, la resistencia a ciberataques, la gestión de identidades, los costos de implementación y la escalabilidad para PYMEs.

Ventajas sobre sistemas tradicionales de autenticación y gestión de identidades

En los sistemas tradicionales de autenticación, los usuarios dependen de proveedores centralizados que almacenan sus credenciales (como nombres de usuario y contraseñas), lo cual representa un riesgo considerable si esas bases de datos son comprometidas. Blockchain ofrece una alternativa a través de identidades digitales descentralizadas (DIDs), donde los usuarios controlan sus credenciales mediante claves criptográficas, sin necesidad de confiar en un único proveedor o servidor.

Además, gracias al uso de contratos inteligentes y firmas digitales, Blockchain permite establecer mecanismos de autenticación multifactor y validación automática de permisos, lo que mejora la eficiencia y seguridad en comparación con los métodos tradicionales basados en contraseñas, tokens o certificados físicos. Esto resulta especialmente útil en el comercio electrónico, donde la validación segura y rápida de la identidad del comprador o del proveedor es fundamental.(ISO, 2023)

Costos y Viabilidad de Implementación en Pymes Frente a otros Métodos de Ciberseguridad

Históricamente, uno de los principales obstáculos para la adopción de blockchain ha sido su complejidad técnica y los costos de implementación, que solían estar fuera del alcance de muchas pequeñas y medianas empresas (pymes). Sin embargo, esta barrera ha disminuido significativamente con la aparición de soluciones como blockchain como servicio (BaaS), ofrecidas por proveedores como IBM, Microsoft Azure y Amazon Web Services.

Estas plataformas permiten a las pymes acceder a infraestructuras Blockchain escalables sin necesidad de grandes inversiones iniciales en hardware, desarrollo ni mantenimiento. Además, las ventajas de seguridad, integridad de datos y automatización de procesos que ofrece Blockchain pueden traducirse en ahorros a medio plazo al reducir el riesgo de ciberataques, fraude y pérdida de datos críticos. (Augusto Coca, 2024)

Aplicaciones Potenciales de Blockchain en la Ciberseguridad del Retail y el Comercio Electrónico

A continuación, se describen algunos casos de uso concretos que demuestran el potencial de Blockchain en la ciberseguridad del sector:

Gestión Descentralizada de Identidades de Clientes y Empleados

En plataformas de comercio electrónico, la gestión segura de credenciales es crucial. Mediante identidades descentralizadas (DID), las PYME pueden evitar almacenar contraseñas en bases de datos vulnerables. En su lugar, cada usuario posee una clave criptográfica única, lo que reduce el riesgo de robo de identidad, ataques de phishing o fugas de información. Esto es especialmente útil para autenticar compras, accesos administrativos o integraciones con pasarelas de pago. (Shoemaker, 2025)

Automatización Segura de Procesos con Contratos Inteligentes

Los smart contracts permiten ejecutar de forma automática condiciones comerciales, como pagos, entregas o devoluciones, sin necesidad de intervención manual ni terceros. Por ejemplo, un contrato inteligente puede liberar el pago de un producto solo cuando el sistema detecta que ha sido entregado. Esto no solo reduce los fraudes y disputas, sino que mejora la eficiencia operativa, registrando cada acción en Blockchain con plena auditabilidad.

Auditoría y Trazabilidad de Transacciones y Logística

Blockchain permite registrar cada transacción o evento logístico (compra, envío, devolución, reclamo) de manera inmutable. Esto genera un historial confiable, accesible tanto para la empresa como para el cliente, reforzando la confianza en las operaciones. En caso de incidentes, la trazabilidad facilita la investigación forense y la rendición de cuentas.

Respaldo Seguro Contra Ransomware y Pérdida de Información

Mediante el almacenamiento distribuido (por ejemplo, combinando Blockchain con IPFS), las PYME pueden guardar copias cifradas de documentos críticos (facturas, bases de datos, configuraciones) de forma inalterable. En caso de un ataque de ransomware, la empresa puede restaurar versiones válidas sin ceder ante chantajes, mejorando su resiliencia operativa y reputacional.

Control de Acceso Distribuido a Sistemas y Servicios

Blockchain permite implementar esquemas de control de acceso basados en roles o atributos, sin necesidad de un servidor central. Esto resulta útil en entornos de trabajo remoto, permitiendo validar permisos en tiempo real y evitando escaladas no autorizadas de privilegios. Cada intento de acceso queda registrado, reforzando la trazabilidad y detección de anomalías.

Aplicación en el Almacenamiento Seguro de Registros Digitales

Blockchain se ha convertido en una herramienta clave para garantizar el almacenamiento seguro de registros digitales en el sector del retail, todo esto gracias a su estructura descentralizada e inmutable, los datos almacenados en una cadena de bloques no pueden ser alterados ni eliminados sin consenso, lo que lo convierte en una solución efectiva para prevenir fraudes, manipulaciones o pérdidas de información. Esta característica resulta

especialmente útil en el comercio electrónico, donde los registros de pedidos, pagos y entregas requieren altos niveles de integridad y disponibilidad.

Empresas de e-commerce han comenzado a utilizar Blockchain para almacenar historiales de compra, comprobantes de pago, inventarios y auditorías, mejorando la trazabilidad de los productos y asegurando que la información no sea falsificada o vulnerada durante el proceso comercial.(Peña Valenzuela et al., 2021)

Monitoreo de Transacciones en Tiempo Real y Prevención de Fraudes

La naturaleza distribuida de Blockchain permite la supervisión continua de transacciones en tiempo real. Cada operación registrada puede ser auditada por múltiples nodos, lo que facilita la detección inmediata de comportamientos anómalos o patrones sospechosos que podrían indicar fraude financiero o actividades maliciosas.

Este tipo de monitoreo activo es especialmente valioso en entornos de pagos electrónicos y plataformas P2P, donde la confianza entre las partes puede no estar garantizada. Blockchain permite a los comercios verificar automáticamente la validez de las operaciones, aplicar políticas de seguridad en tiempo real y prevenir el uso indebido de tarjetas de crédito o cuentas bancarias.(Seon, 2025)

Empresas y Plataformas que han Implementado Soluciones Blockchain

La implementación de tecnologías Blockchain en el ámbito del comercio electrónico ha sido una estrategia adoptada por diversas empresas para afrontar problemáticas como la falsificación de productos, el fraude en pagos, la trazabilidad de mercancías y la optimización logística. Esta tecnología ha demostrado ser clave en la generación de confianza, eficiencia y seguridad en las transacciones digitales, aspectos que resultan fundamentales en un entorno altamente competitivo y globalizado.

Tabla 3

Implementación de Blockchain y su Impacto en el Comercio Electrónico

Empresa / Plataforma	Motivo de Implementación	Aplicación Blockchain	Contribución al Comercio Electrónico
Walmart	Garantizar la trazabilidad de productos alimentarios para evitar fraudes y mejorar la seguridad.	Uso de Hyperledger Fabric para rastrear productos desde su origen hasta el punto de venta.	Permite a los consumidores verificar la procedencia y frescura de los productos; fortalece la transparencia en el marketplace, lo que reduce devoluciones y mejora la confianza en las compras online.
Alibaba (Tmall)	Combatir la falsificación de productos de lujo y ofrecer garantías a los compradores.	Sistema de trazabilidad que registra cada paso del producto en la cadena de suministro mediante blockchain.	Refuerza la autenticidad de los artículos vendidos online, reduciendo reclamos, disputas y fraudes. Incentiva las ventas de productos premium en canales digitales.
Amazon Web Services (AWS)	Ofrecer infraestructura blockchain como servicio para clientes e-commerce.	Amazon Managed Blockchain permite construir redes blockchain privadas.	Proporciona a empresas de e-commerce una forma segura de compartir datos con socios logísticos, bancos y proveedores sin comprometer la integridad. Facilita la trazabilidad y la automatización de contratos inteligentes.
Shopify	Aumentar las opciones de pago seguras y reducir el fraude financiero.	Integración de pagos en criptomonedas (Bitcoin, Ethereum, etc.) mediante pasarelas como Coinbase Commerce y BitPay.	Amplía el acceso a mercados globales y descentralizados, permite transacciones sin terceros, reduce costos de procesamiento y mejora la seguridad de pagos digitales.
Maersk (TradeLens)	Optimizar la logística internacional mediante el intercambio seguro de documentos.	Plataforma blockchain (en colaboración con IBM) que registra datos logísticos y aduaneros.	Mejora el cumplimiento y la entrega eficiente en operaciones e-commerce internacionales. Reduce costos de envío, tiempos de entrega y pérdidas por errores logísticos.

Empresa / Plataforma	Motivo de Implementación	Aplicación Blockchain	Contribución al Comercio Electrónico
VeChain	Validar la autenticidad de productos físicos (ropa, lujo, vino, etc.).	Asignación de identificadores únicos (NFC, QR, RFID) conectados a registros en blockchain.	Aumenta la transparencia en los catálogos digitales, protege al consumidor contra falsificaciones y fortalece el branding en tiendas en línea. Ideal para modelos D2C (Direct to Consumer).
Nike (CryptoKicks)	Prevenir falsificaciones y rastrear la propiedad digital de productos exclusivos.	Asociación de zapatillas físicas con tokens digitales (NFTs) registrados en blockchain.	Revaloriza el comercio de productos limitados en línea, habilita mercados secundarios digitales seguros, y permite a los usuarios verificar originalidad antes de comprar.
IBM Blockchain Payments	Solucionar ineficiencias y riesgos en pagos internacionales.	Plataforma blockchain que permite pagos transfronterizos seguros y rápidos.	Mejora la experiencia del cliente en compras internacionales al reducir comisiones bancarias, retrasos en transferencias y fraudes en conversiones monetarias.
Provenance	Garantizar la sostenibilidad y trazabilidad en la cadena de valor de productos éticos.	Blockchain pública para registrar información verificable sobre cada etapa del producto.	Atrae consumidores responsables, ofrece una ventaja competitiva en mercados verdes o éticos, y mejora la credibilidad de productos en canales e-commerce orientados al consumo consciente.
OpenBazaar	Crear un ecosistema de comercio electrónico verdaderamente descentralizado.	Plataforma peer-to-peer que utiliza blockchain para registrar transacciones sin servidores centrales.	Elimina intermediarios, comisiones y censura en el e-commerce. Otorga a compradores y vendedores total autonomía, seguridad en transacciones y control sobre los datos personales.

Nota. La tabla presenta los principales ámbitos de aplicación de Blockchain en el comercio electrónico y su influencia en la seguridad, transparencia y eficiencia de las transacciones. Resume beneficios como la reducción del fraude, la mejora en la trazabilidad y el fortalecimiento de la confianza del cliente. Asimismo, muestra cómo estas mejoras incrementan la resiliencia cibernética de las PYMEs del sector retail.

Empresas como Walmart han integrado Blockchain (Hyperledger Fabric) para la trazabilidad de productos alimentarios, reduciendo el tiempo de rastreo de lotes contaminados de días a segundos(Lfdecentralizedtrust, 2024). Alibaba, a través de su plataforma Tmall, ha incorporado soluciones Blockchain para certificar la autenticidad de productos de lujo, mejorando la transparencia de los procesos de compra[2]. En el ámbito de servicios, Amazon Web Services (AWS) ofrece infraestructura Blockchain como servicio (BaaS), permitiendo a empresas de e-commerce integrar esta tecnología sin necesidad de desarrollar sistemas complejos.

En cuanto a medios de pago, Shopify ha facilitado la aceptación de criptomonedas mediante la integración de pasarelas seguras como Coinbase Commerce, ampliando así las alternativas para usuarios internacionales y reduciendo costos por intermediarios. En el sector logístico, Maersk, en colaboración con IBM, ha desarrollado TradeLens, una plataforma Blockchain que digitaliza y asegura el intercambio de documentos entre actores del comercio internacional[5]. Esta herramienta ha sido clave para optimizar tiempos de entrega en operaciones de comercio electrónico transfronterizo.

Por su parte, VeChain emplea identificadores únicos y Blockchain para garantizar la autenticidad de productos, especialmente en sectores como la moda y el vino, aportando confianza y trazabilidad en el comercio online[6]. Nike también ha incursionado con su proyecto CryptoKicks, un sistema que enlaza productos físicos con tokens no fungibles (NFTs), permitiendo validar propiedad y originalidad en ventas digitales. Para resolver el problema de las transferencias internacionales lentas y propensas a errores, IBM Blockchain Payments ha propuesto una alternativa rápida y segura que beneficia a tiendas en línea que operan

globalmente[8]. Además, plataformas como Provenance permiten verificar el origen sostenible de productos, fortaleciendo marcas con principios éticos y transparencia en marketplaces.

Finalmente, OpenBazaar representa un enfoque disruptivo al ofrecer un mercado descentralizado sin intermediarios, donde compradores y vendedores se conectan directamente usando Blockchain. Esta solución maximiza la privacidad, reduce comisiones y evita censura, constituyéndose como una alternativa viable para un comercio electrónico autónomo

Diversas compañías han comenzado a implementar soluciones Blockchain orientadas a la ciberseguridad y la confianza digital en el comercio electrónico. Algunos ejemplos destacados incluyen:

Evaluación de su Aplicabilidad en Pyme del Comercio Electrónico

La adopción de tecnologías emergentes como Blockchain en pequeñas y medianas empresas (PYMEs) del sector de comercio electrónico representa una oportunidad estratégica para reforzar sus capacidades de ciberseguridad. Sin embargo, su implementación no está exenta de desafíos técnicos, económicos y organizacionales que deben ser cuidadosamente evaluados antes de su integración.

En primer lugar, la infraestructura tecnológica de muchas PYMEs aún no está preparada para soportar sistemas distribuidos o algoritmos de consenso complejos. A diferencia de las grandes corporaciones, estas empresas suelen operar con recursos limitados en términos de hardware, personal especializado y conectividad, lo que puede dificultar la integración directa de una red Blockchain propia. No obstante, soluciones como Blockchain-as-a-Service (BaaS) ofrecidas por proveedores en la nube permiten reducir esta barrera, brindando acceso a plataformas ya configuradas bajo esquemas de pago por uso.

Desde el punto de vista de la seguridad informática, Blockchain ofrece ventajas significativas como la inmutabilidad de los registros, la descentralización de la autenticación y la trazabilidad transparente de operaciones, elementos particularmente valiosos para el comercio electrónico, donde la protección de datos personales, la validación de transacciones y la resistencia al fraude son prioritarias. Por ejemplo, la implementación de identidades digitales descentralizadas (DID) podría reducir significativamente los riesgos de suplantación y accesos no autorizados en tiendas virtuales.

Sin embargo, la aplicabilidad práctica depende también del grado de madurez digital de la empresa y del contexto regulatorio en el que opere. En países donde la normatividad en protección de datos y tecnologías emergentes es aún incipiente o poco clara, la adopción de Blockchain debe hacerse con especial cuidado para asegurar la conformidad legal, por ejemplo, con leyes como la Ley 1581 de 2012 en Colombia o el GDPR en Europa.

Otro factor relevante es la viabilidad económica. Aunque las plataformas BaaS hacen más accesible la tecnología, aún existen costos asociados con la capacitación del personal, la adaptación de procesos y la integración con sistemas existentes (ERP, CMS, pasarelas de pago, etc.). No obstante, este tipo de inversión puede traducirse en beneficios sostenibles a mediano plazo, como la reducción de fraudes, la automatización de procesos con contratos inteligentes y el fortalecimiento de la confianza del consumidor.

En síntesis, Blockchain es aplicable a las PYMEs del comercio electrónico, siempre que se realice un análisis integral que considere su capacidad tecnológica, la alineación con normativas vigentes, el retorno esperado de la inversión y el impacto positivo en la seguridad de la información. Su implementación progresiva y acompañada de asesoría especializada puede ser

un camino viable hacia una transformación digital más resiliente y segura. (Atiencia García & Jaramillo Villafuerte, 2024)

Ventajas y Desafíos de Implementación en Pymes

La tabla contrasta las principales ventajas de implementar Blockchain en PYMEs, como la integridad de datos y la reducción de fraudes, frente a desafíos comunes como la falta de conocimiento técnico o la resistencia al cambio. Presenta de forma resumida factores clave para evaluar su adopción en el sector retail y comercio electrónico.

Tabla 4

Ventajas y Desafíos en Pymes

Ventajas Principales	Desafíos Comunes
Integridad de datos garantizada	Falta de conocimiento técnico
Reducción de fraudes y errores	Costos iniciales percibidos como altos
Mejora en la confianza del cliente	Ausencia de marcos regulatorios claros
Seguridad sin intermediarios	Dificultades en la integración con sistemas existentes
Escalabilidad mediante BaaS	Resistencia al cambio organizacional

Nota. La tabla presenta de forma comparativa las ventajas principales y los desafíos comunes asociados a la implementación de Blockchain en PYMEs del sector retail y comercio electrónico. Entre las ventajas destacan la integridad de datos, la reducción de fraudes y la escalabilidad mediante BaaS; mientras que los desafíos incluyen la falta de conocimiento técnico, los costos iniciales percibidos como altos y la resistencia al cambio organizacional.

Estrategias de Implementación de Blockchain para la Seguridad de Pymes de Comercio Electrónico

El comercio electrónico cada vez es más dependiente de plataformas de comercio, haciendo que las empresas, especialmente las pequeñas y medianas Pyme, enfrenten crecientes riesgos de ciberseguridad. Dentro de estas organizaciones suelen carecer de recursos técnicos y financieros para implementar soluciones robustas que las protejan contra amenazas como el robo de identidad, la falsificación de datos o los ataques de denegación de servicio (DoS), situaciones que pueden comprometer seriamente su sostenibilidad operativa.

Blockchain surge como una solución innovadora que responde a esta necesidad, al ofrecer una infraestructura tecnológica descentralizada, segura y transparente, además de su capacidad para registrar datos de forma inmutable permite fortalecer la integridad de las transacciones digitales y reducir significativamente la exposición a fraudes. A diferencia de los sistemas tradicionales basados en servidores centralizados, Blockchain distribuye la información en múltiples nodos, dificultando los ataques dirigidos y aumentando la resiliencia del sistema.

En el contexto del comercio digital, donde la trazabilidad, la confianza del cliente y la autenticidad de la información son fundamentales, Blockchain representa un cambio de paradigma, su implementación posibilita el uso de contratos inteligentes para automatizar procesos clave como la verificación de pagos, la gestión de inventarios o la validación de identidad, disminuyendo los errores humanos y mejorando la eficiencia operativa.

Asimismo, la adopción de identidades digitales basadas en Blockchain brinda a los usuarios mayor control sobre su información personal y garantiza procesos de autenticación más seguros. Esto no solo refuerza la protección de datos sensibles, sino que también mejora la

experiencia del cliente y fortalece la reputación de las empresas en un entorno donde la confianza es un activo estratégico.

Por tanto, implementar Blockchain en el comercio digital no es solo una medida tecnológica, sino una estrategia de ciberseguridad proactiva que responde a los desafíos actuales del entorno digital. En particular, para las PYMES del sector retail, representa una oportunidad de adoptar soluciones escalables, accesibles y adaptadas a sus necesidades específicas, mejorando su competitividad, mitigando riesgos críticos y asegurando la continuidad de sus operaciones.

Estrategias para la Autenticación Segura de Usuarios y Eliminación del Fraude en Credenciales

El robo de credenciales son las amenazas más recurrentes en los entornos digitales, que puede desencadenar accesos no autorizados, fuga de información y fraudes financieros. En este escenario, Blockchain ofrece un marco eficaz para redefinir los procesos de autenticación mediante la implementación de identidades digitales descentralizadas (DID, por sus siglas en inglés), en las que los usuarios controlan sus propios datos y las empresas no necesitan almacenarlos en servidores vulnerables.

Estas identidades están respaldadas por claves criptográficas únicas y pueden integrarse con sistemas de verificación biométrica o autenticación multifactor (MFA), lo que refuerza los mecanismos de acceso y dificulta la suplantación de identidad. A través de contratos inteligentes, es posible automatizar la validación de usuarios y limitar el acceso a recursos según los niveles de permisos predefinidos, reduciendo errores humanos y puntos de fallo centralizados.

Además, las estrategias basadas en Blockchain permiten registrar cada intento de acceso en una cadena de bloques inmutable, lo que garantiza trazabilidad completa y simplifica las

auditorías de seguridad. Esto permite a las organizaciones detectar patrones de comportamiento sospechosos, identificar ataques en tiempo real y actuar con rapidez ante incidentes.

Otra táctica clave es la tokenización de credenciales, donde la información de acceso es representada por tokens digitales que no pueden reutilizarse ni interceptarse en transacciones maliciosas. Esta técnica mitiga el riesgo de ataques como phishing, replay attacks o credential stuffing, mejorando la confianza en el sistema de autenticación.

Implementación de Contratos Inteligentes en Sistemas de Pago para Eliminar Riesgos de Manipulación

La implementación de contratos inteligentes en sistemas de pago representa una solución innovadora y robusta para enfrentar los riesgos de manipulación en las transacciones financieras digitales. Los contratos inteligentes, ejecutados en plataformas blockchain, automatizan acuerdos entre partes sin necesidad de intermediarios. Esto se traduce en operaciones más seguras, ágiles y transparentes, lo cual es especialmente beneficioso para las pequeñas y medianas empresas (PYMEs) que manejan recursos limitados y requieren soluciones confiables. La naturaleza descentralizada de blockchain garantiza que estos contratos no puedan ser alterados una vez establecidos, lo que elimina vulnerabilidades asociadas a fraudes internos o externos.

Una de las principales fortalezas de los contratos inteligentes es su capacidad para ejecutar instrucciones de manera automática al cumplirse condiciones previamente definidas. Esto evita la intervención humana, reduciendo significativamente el riesgo de errores operativos y manipulaciones maliciosas. Por ejemplo, en un acuerdo comercial entre una PyME y un cliente, el contrato puede verificar la disponibilidad de fondos, confirmar la entrega del producto o servicio, y liberar el pago automáticamente. Todo este proceso ocurre de forma transparente y verificable, sin requerir intervención de terceros como bancos u operadores de pago.

Además, estos contratos refuerzan la confianza entre las partes al proporcionar trazabilidad total sobre las transacciones. Cada paso queda registrado de forma permanente e inalterable en la blockchain, permitiendo auditorías en tiempo real y previniendo disputas legales. Este nivel de visibilidad es esencial para las PYMEs, ya que minimiza conflictos con los clientes y mejora la reputación organizacional. En contextos donde la confianza es clave para la fidelización de clientes y socios comerciales, los contratos inteligentes se convierten en una herramienta estratégica.

En términos de seguridad informática, la utilización de contratos inteligentes ofrece una barrera eficaz contra ciberataques dirigidos a manipular condiciones de pago o alterar registros financieros. Al estar integrados en una red blockchain, los contratos funcionan sobre estructuras distribuidas, lo que impide puntos únicos de fallo. Esto dificulta considerablemente las intrusiones y asegura que ningún actor, interno o externo, pueda modificar el acuerdo o interferir con la ejecución del pago. Así, las PYMEs fortalecen su postura de ciberseguridad sin necesidad de invertir en infraestructura costosa.

Por otra parte, la automatización de procesos mediante contratos inteligentes también reduce considerablemente los costos operativos, al eliminar intermediarios y disminuir los tiempos de espera en las transacciones. Esto no solo mejora el flujo de caja en las organizaciones, sino que también incrementa la eficiencia operativa. Las PYMEs pueden usar esta tecnología para establecer pagos en etapas, vincular cobros a entregables o hitos, y asegurar que las obligaciones contractuales se cumplan al pie de la letra antes de liberar fondos. De esta forma, se eliminan disputas y se gana en agilidad.

La implementación de contratos inteligentes en sistemas de pago representa un avance significativo en la protección de las operaciones financieras frente a manipulaciones y fraudes.

Para las PYMEs, su adopción no solo implica una mejora en la seguridad, sino también en eficiencia, transparencia y confianza. Este tipo de soluciones basadas en tecnología blockchain son clave para promover entornos digitales seguros y resilientes, posicionando a las empresas como actores innovadores dentro de sus sectores. Integrarlos estratégicamente es un paso hacia una transformación digital sólida y sostenible.

Trazabilidad y Almacenamiento Seguro de Información Crítica en Blockchain

Integración de Blockchain con tecnologías de seguridad existentes (firewalls, IDS, autenticación multifactor).

La trazabilidad y el almacenamiento seguro de información importante son aspectos fundamentales en los sistemas de ciberseguridad modernos. Blockchain, al ser una tecnología distribuida e inmutable, permite registrar eventos, transacciones o cambios en los datos de forma cronológica y verificable. Esto garantiza que la información no pueda ser alterada sin dejar rastro, aportando transparencia y confianza. Para organizaciones como las PYMEs, que gestionan activos digitales sensibles, este tipo de trazabilidad ofrece una ventaja significativa en cuanto a auditoría y control de accesos. Cada interacción puede ser registrada como un bloque, sellado criptográficamente.

El almacenamiento de información crítica en Blockchain también permite blindar los datos frente a accesos no autorizados o manipulaciones. A diferencia de los sistemas tradicionales centralizados, donde un fallo o ataque compromete el nodo principal, en Blockchain los datos están replicados en múltiples nodos. Esto hace casi imposible que una única amenaza comprometa todo el sistema. Además, la utilización de algoritmos de cifrado robustos durante la escritura y lectura de datos refuerza su confidencialidad. Las PYMEs pueden asegurar la integridad de documentos como contratos, respaldos, historiales de clientes, y logs operativos.

Para ampliar su eficacia, Blockchain puede integrarse con tecnologías de seguridad ya implementadas como firewalls, sistemas de detección de intrusos (IDS), y autenticación multifactor (MFA). Por ejemplo, un firewall puede limitar el tráfico hacia nodos Blockchain no autorizados, mientras un IDS puede detectar patrones anómalos en las solicitudes de consulta a la cadena de bloques. A su vez, el acceso a las interfaces que permiten leer o escribir datos puede estar protegido mediante MFA, garantizando que solo usuarios verificados puedan realizar operaciones. Esta convergencia tecnológica mejora exponencialmente la postura de seguridad de cualquier organización.

Integración de Blockchain con Tecnologías de Seguridad Existentes

La integración entre Blockchain y tecnologías existentes también facilita la implementación de políticas de seguridad más coherentes y automatizadas. Por ejemplo, los logs generados por un IDS pueden almacenarse directamente en una blockchain para asegurar su autenticidad en auditorías posteriores. Asimismo, los resultados de análisis forense digital pueden documentarse de forma segura, sin el riesgo de ser alterados. Este enfoque híbrido entre tecnologías tradicionales y blockchain permite a las PYMEs cumplir con normativas de protección de datos como la ISO/IEC 27001 o la GDPR, sin incurrir en grandes inversiones.

Otro beneficio clave es la capacidad de detectar y mitigar incidentes de seguridad en tiempo real. Al combinar Blockchain con sistemas de monitoreo activos, las organizaciones pueden registrar alertas y respuestas automáticamente en la cadena de bloques, estableciendo líneas temporales de eventos sin posibilidad de manipulación posterior. Este tipo de evidencia puede ser fundamental en investigaciones digitales o procesos judiciales. La trazabilidad asegurada permite reconstruir con precisión qué ocurrió, cuándo, y quién estuvo involucrado, lo que fortalece la resiliencia organizacional.

En síntesis, Blockchain no solo revoluciona el almacenamiento seguro de información crítica, sino que también potencia otras soluciones de seguridad al integrarse con ellas. Esta tecnología ofrece a las PYMEs la posibilidad de modernizar sus esquemas de protección con una solución escalable, distribuida y resiliente. Implementarla junto a firewalls, IDS y autenticación multifactor crea un ecosistema digital cohesivo y robusto. En un entorno cada vez más amenazado por ataques sofisticados, esta integración representa un pilar estratégico para garantizar continuidad del negocio y protección de activos clave.

Propuesta de Estrategias Basadas en Blockchain para Mitigar Vulnerabilidades en PYMEs del Sector Comercio electrónico

En atención al objetivo de proponer estrategias que integren la tecnología Blockchain para mitigar vulnerabilidades críticas en las pequeñas y medianas empresas (PYMEs) del sector comercio electrónico, a continuación, se desarrolla un conjunto de soluciones que abordan las debilidades más recurrentes identificadas en estas organizaciones.

Una de las vulnerabilidades más frecuentes es la falta de respaldos inmutables y protegidos frente a ataques como el ransomware o la manipulación interna. Para ello, Blockchain permite crear registros referenciados mediante funciones hash, de forma que las copias de seguridad, aunque no se almacenen directamente en la cadena, puedan validarse en todo momento respecto a su integridad. Esta técnica garantiza que los datos respaldados no han sido alterados y ofrece una herramienta confiable para la recuperación posterior al incidente.

Otra debilidad común es el uso de contraseñas débiles o compartidas, junto con la inexistencia de mecanismos robustos de autenticación. Blockchain aborda esta vulnerabilidad mediante la implementación de sistemas de identidad digital descentralizada (DID), donde las credenciales de los usuarios no dependen de un servidor central ni pueden ser suplantadas con

facilidad. Esto contribuye a reducir significativamente los accesos no autorizados y refuerza la autenticidad de las transacciones.

Asimismo, muchas PYMEs carecen de trazabilidad en los accesos a sistemas y cambios de configuración, lo que impide realizar auditorías o investigaciones forenses tras un incidente. Con Blockchain, es posible registrar los eventos más relevantes en una cadena privada, generando un historial inalterable que permite reconstruir lo ocurrido y establecer responsabilidades. Esto no solo mejora la detección y respuesta ante incidentes, sino que eleva el nivel de transparencia en los procesos.

En cuanto a los procesos críticos expuestos a errores humanos o fraude, como la emisión de facturas, pedidos o pagos, Blockchain ofrece soluciones a través de contratos inteligentes (smart contracts). Estos permiten automatizar ciertas reglas de negocio bajo condiciones previamente definidas, reduciendo la intervención manual y evitando manipulaciones. Esta automatización contribuye a prevenir errores y fortalece la confianza entre partes involucradas.Otro aspecto delicado en las PYMEs es el almacenamiento centralizado de datos sensibles, que puede ser comprometido fácilmente si no cuenta con medidas de protección suficientes. En este caso, Blockchain permite distribuir de forma segura ciertos tipos de información o al menos sus referencias (hashes), reduciendo el riesgo de pérdida, alteración o acceso indebido, y mejorando la disponibilidad y la integridad de los datos críticos.

Finalmente, muchas pequeñas empresas no cuentan con sistemas de monitoreo continuo de sus transacciones electrónicas, lo que favorece la ejecución de fraudes sin detección oportuna. Al registrar automáticamente las transacciones en Blockchain, es posible validar en tiempo real su legitimidad, establecer umbrales de alerta y generar evidencias confiables en caso de disputas o auditorías posteriores.

Estas estrategias reflejan el potencial real de Blockchain no solo como una tecnología disruptiva, sino como una herramienta aplicable y adaptable a la realidad de las PYMEs. Al enfocarse en mitigar vulnerabilidades específicas y no solo en reaccionar ante amenazas externas, se promueve una cultura de prevención y resiliencia, elevando el estándar de ciberseguridad en el comercio digital.

Impacto en Costos y viabilidad Operativa de las Soluciones Propuestas

La implementación de soluciones basadas en Blockchain en PYMEs del comercio electrónico plantea inicialmente una inversión tecnológica considerable, especialmente si se requiere infraestructura personalizada. Sin embargo, a mediano y largo plazo, este gasto se traduce en ahorros operativos derivados de la automatización de procesos, reducción de fraudes, eliminación de intermediarios y disminución de disputas comerciales. Por tanto, se convierte en una inversión estratégica de alto retorno.

Uno de los beneficios más evidentes es la reducción de los costos asociados a intermediarios financieros. Al integrar Blockchain, las PYMEs pueden gestionar pagos mediante criptomonedas o stablecoins sin necesidad de pasar por bancos o pasarelas de pago tradicionales, lo cual minimiza comisiones. Además, los contratos inteligentes reducen la carga operativa y legal, automatizando acuerdos y condiciones sin intervención humana constante.

En términos de operatividad, Blockchain aporta eficiencia al permitir la trazabilidad automática de productos, servicios o transacciones. Esto disminuye la necesidad de auditorías manuales o registros físicos, y simplifica el cumplimiento normativo en sectores regulados. Al mismo tiempo, la transparencia de la cadena de bloques permite resolver disputas de manera más rápida y menos costosa, dado que la evidencia transaccional es pública, verificable y no editable.

La viabilidad operativa de estas soluciones ha mejorado gracias al desarrollo de plataformas Blockchain como Ethereum, Hyperledger o Polygon, que ofrecen entornos accesibles y adaptables para PYMEs. Estas tecnologías permiten escalar soluciones desde prototipos hasta entornos reales, sin necesidad de una infraestructura técnica compleja. Además, muchas de estas herramientas ofrecen integración con sistemas existentes, como ERPs, CRM o plataformas de e-commerce.

A nivel técnico, los costos de mantenimiento y soporte de soluciones Blockchain pueden mantenerse bajos si se opta por servicios en la nube o Blockchain-as-a-Service (BaaS). Esto permite a las PYMEs tercerizar la complejidad tecnológica y centrarse en su core de negocio. Incluso, existen consorcios Blockchain y redes privadas compartidas que permiten dividir costos entre varias organizaciones, facilitando la adopción sin necesidad de una infraestructura propia costosa.

Principales Aportes de las Estrategias de Implementación de Blockchain en Comercio Electrónico

Las estrategias basadas en Blockchain han demostrado aportar soluciones sustanciales a los principales desafíos que enfrenta el comercio electrónico, particularmente en el entorno de las pequeñas y medianas empresas (PYMEs). Uno de los aportes más relevantes es la garantía de integridad de la información, ya que la tecnología Blockchain, al operar sobre un sistema de registros inmutables y descentralizados, previene la alteración no autorizada de datos sensibles como transacciones financieras, historiales de compras y credenciales de autenticación. Esto representa una ventaja considerable frente a los sistemas centralizados, donde una sola brecha de seguridad puede comprometer grandes volúmenes de datos.

Otro aporte fundamental radica en el refuerzo de la confianza entre partes involucradas en las transacciones electrónicas, particularmente en entornos donde no existen relaciones comerciales previas. A través del uso de contratos inteligentes, se automatizan procesos como pagos, validación de entregas o verificación de identidad, eliminando intermediarios y reduciendo significativamente la exposición al fraude. Este mecanismo transparente y autoejecutable permite a las PYMEs operar de manera más segura en mercados digitales ampliados, reduciendo riesgos operacionales y costes relacionados con litigios o reclamos por incumplimiento.

Además, la implementación de Blockchain mejora de forma significativa la trazabilidad de las operaciones y la auditoría de los sistemas. Cada bloque almacenado incluye un registro cronológico y verificable de actividades, lo que facilita la detección oportuna de anomalías, incidentes de seguridad o inconsistencias. En sectores como logística, pagos o cumplimiento normativo (compliance), esta visibilidad y verificabilidad se convierte en una herramienta clave para prevenir el lavado de activos, rastrear el origen de productos y garantizar el cumplimiento de estándares regulatorios internacionales, lo cual también mejora la reputación corporativa.

Desde una perspectiva de sostenibilidad operativa, Blockchain contribuye a disminuir los costes asociados a las infraestructuras de ciberseguridad tradicionales. Al reemplazar soluciones centralizadas por arquitecturas distribuidas, las empresas pueden mitigar los gastos derivados de mantenimientos, renovaciones constantes de licencias o adquisición de hardware especializado. Esta descentralización también redistribuye la responsabilidad sobre los datos, haciendo menos vulnerable el sistema en caso de ataques dirigidos.

Finalmente, el uso de esta tecnología facilita la adaptación de las PYMEs a los nuevos modelos de negocio digitales, ya que permite integrar funcionalidades avanzadas como pagos

con criptomonedas, sistemas descentralizados de identidad (DID) y marketplaces seguros. Esto no solo optimiza sus capacidades de innovación, sino que además las posiciona como actores resilientes frente a amenazas cibernéticas emergentes. En suma, los aportes de Blockchain no son meramente tecnológicos, sino estratégicos, ya que brindan a las PYMEs un marco de seguridad que evoluciona al ritmo del ecosistema digital.

Implicaciones Futuras para la Seguridad Cibernética en Pymes del Sector

El panorama de la ciberseguridad para las PYMEs del sector del comercio electrónico está evolucionando rápidamente, impulsado tanto por la creciente sofisticación de las amenazas como por la transformación digital que exige nuevas formas de proteger los activos digitales. En este contexto, la incorporación de estrategias basadas en Blockchain no solo representa una solución innovadora, sino que proyecta implicaciones trascendentales para el futuro de la protección de datos, las transacciones seguras y la resiliencia organizacional.

A medida que los ataques como el ransomware, el phishing y la suplantación de identidad continúan aumentando según informes recientes, más del 60 % de los ciberataques exitosos en América Latina afectaron directamente a PYMEs, se hace evidente que las soluciones tradicionales ya no son suficientes para garantizar una defensa eficaz. Blockchain, al ofrecer un entorno distribuido, transparente y resistente a manipulaciones, plantea una nueva forma de entender y abordar la seguridad: no desde la reacción, sino desde la prevención estructural y la confianza automatizada.

Las implicaciones futuras incluyen una mayor descentralización de la seguridad, donde las decisiones sobre acceso, verificación y validación de identidades no dependerán exclusivamente de sistemas cerrados o humanos, sino de protocolos criptográficos autoejecutables. Esta transición redefine la forma en que las PYMEs gestionarán el control de

sus sistemas, al permitirles reducir su dependencia de proveedores externos de seguridad y ganar autonomía digital sin comprometer la protección de su infraestructura.

Además, se prevé una transformación en la cultura organizacional de la ciberseguridad, donde los principios de integridad, transparencia y trazabilidad de Blockchain comiencen a permear en los procesos internos, promoviendo una toma de decisiones basada en la evidencia digital y en registros confiables. Esta evolución será clave para enfrentar no solo las amenazas técnicas, sino también los desafíos normativos y reputacionales que afectan la confianza del consumidor y la sostenibilidad del negocio.

En términos de escalabilidad, Blockchain permitirá a las PYMEs integrar soluciones de ciberseguridad más robustas sin requerir grandes inversiones, democratizando así el acceso a tecnologías de protección avanzada. Esto representa un cambio paradigmático: por primera vez, empresas pequeñas tendrán la posibilidad de competir en igualdad de condiciones con grandes actores del mercado en términos de seguridad y confianza digital.

En síntesis, las implicaciones futuras apuntan a un ecosistema digital más seguro, transparente y resiliente para las PYMEs del comercio electrónico, donde Blockchain se consolida no como una herramienta aislada, sino como un habilitador estratégico de la ciberseguridad moderna. Su implementación anticipa no solo una mejora técnica, sino un salto evolutivo en la manera en que las organizaciones protegen su presente y construyen su futuro digital.

Enumeración de Estrategias Basadas en Blockchain para la Ciberseguridad en Pymes de Comercio Electrónico

La adopción de tecnologías emergentes como Blockchain se presenta no solo como una opción innovadora, sino como una necesidad estratégica. Esta tecnología descentralizada ha dado

lugar a diversas estrategias que responden a las amenazas más frecuentes en el entorno digital, especialmente aquellas relacionadas con el robo de datos, el fraude electrónico y los accesos no autorizados.

Entre las principales estrategias basadas en Blockchain que se identifican como aplicables al sector, se destaca la implementación de sistemas de autenticación y verificación de identidad descentralizados, los cuales eliminan los puntos únicos de falla al no depender de servidores centrales vulnerables. Esto contribuye a reducir drásticamente los riesgos de robo de credenciales o suplantación de identidad. Asimismo, el uso de contratos inteligentes permite establecer reglas automáticas e inviolables para ejecutar transacciones, lo que mejora la eficiencia operativa al tiempo que garantiza la integridad del proceso, reduciendo la intervención humana y las posibilidades de manipulación.

Otra estrategia esencial es el registro inmutable de eventos de seguridad, que proporciona trazabilidad completa sobre actividades críticas en la red. Esto fortalece los procesos de auditoría y análisis forense, aportando evidencias sólidas en caso de incidentes y facilitando la respuesta oportuna. Además, la transparencia transaccional propia de Blockchain refuerza la confianza del cliente al permitirle validar el historial de compras o verificar la legitimidad de los productos, elemento clave en mercados digitales sensibles a la reputación.

En materia financiera, las PYMEs también pueden beneficiarse del uso de soluciones de pago seguras mediante criptoactivos o tokens privados, disminuyendo la exposición a fraudes en pasarelas de pago tradicionales. Complementariamente, la gestión segura de certificados digitales y llaves criptográficas a través de nodos distribuidos fortalece la protección de la infraestructura tecnológica, permitiendo un control más seguro sobre los mecanismos de cifrado.

Estas estrategias, cuando se integran de forma estructurada y progresiva, representan una arquitectura de ciberseguridad sólida, adaptable a la realidad operativa de las PYMEs y alineada con las nuevas exigencias del comercio electrónico. Su valor radica no solo en la tecnología subyacente, sino en el cambio de paradigma que propone: pasar de modelos reactivos a esquemas proactivos, resilientes y centrados en la confianza.

Evaluación de Tecnologías, Prácticas y Herramientas de Implementación

El comercio electrónico de las PYMEs requiere una cuidadosa selección de tecnologías y herramientas que no solo sean efectivas, sino también compatibles con sus limitaciones operativas, presupuestarias y de infraestructura. En este contexto, tecnologías como Hyperledger Fabric y Ethereum resultan particularmente adecuadas. Hyperledger, al ser una plataforma permisionada, garantiza confidencialidad y control sobre los participantes, lo que es ideal para entornos donde la protección de datos de clientes y proveedores es prioritaria. Por otro lado, Ethereum, con su arquitectura abierta y robusta, permite la automatización segura de procesos mediante contratos inteligentes, lo cual se alinea con el objetivo de reducir intermediarios, errores humanos y fraudes.

En cuanto a prácticas recomendadas, se sugiere adoptar una implementación por fases, iniciando con proyectos piloto en áreas críticas como la gestión de pagos, validación de transacciones y verificación de identidades, donde Blockchain puede demostrar un impacto inmediato en términos de seguridad y trazabilidad. La práctica de realizar auditorías periódicas de contratos inteligentes, así como establecer políticas claras de gestión de claves privadas y uso de billeteras digitales, resulta esencial para mantener la integridad del sistema.

Respecto a herramientas específicas, Truffle y Ganache facilitan el desarrollo y prueba de contratos inteligentes antes de ser desplegados en producción, lo cual minimiza riesgos.

MetaMask es útil para la gestión segura de credenciales y transacciones desde navegadores, mientras que Infura permite a las PYMEs conectarse a la red Blockchain sin necesidad de mantener infraestructura propia. Estas herramientas son altamente efectivas en términos de facilidad de adopción, bajo costo relativo y escalabilidad progresiva.

La compatibilidad con los objetivos estratégicos del sector es evidente: las PYMEs necesitan soluciones que aumenten la confianza del cliente, reduzcan los costos de intermediación, fortalezcan la integridad de los datos y protejan la cadena de valor digital. Blockchain, aplicada con estas tecnologías y prácticas, no solo cumple con estos propósitos, sino que lo hace de manera resiliente, descentralizada y adaptable, permitiendo que incluso empresas con recursos limitados se beneficien de mecanismos de ciberseguridad robustos y sostenibles.

Beneficios y Limitaciones del uso de esta Tecnología en Ciberseguridad

Uno de los beneficios más relevantes es su descentralización, que elimina el punto único de fallo de los sistemas tradicionales y reduce las posibilidades de ataques dirigidos a servidores centrales. Esta arquitectura distribuida garantiza mayor resiliencia operativa frente a amenazas como ataques DDoS o caídas de servicio.

Otro beneficio clave es la inmutabilidad de los datos, lo que impide la alteración o eliminación de la información registrada una vez validada. Esto resulta esencial en el comercio electrónico, donde la integridad de los registros de transacciones y auditorías es crítica tanto para el cumplimiento normativo como para la confianza del cliente.

Además, Blockchain permite una transparencia controlada, en la que todas las partes autorizadas pueden verificar operaciones sin comprometer la confidencialidad de la información. Esto mejora la trazabilidad de productos, la autenticación de identidades y la prevención de fraudes financieros. La automatización mediante contratos inteligentes también reduce los

errores humanos y los riesgos asociados a procesos manuales, aportando eficiencia y seguridad en la gestión de pagos y accesos.

Además, Blockchain presenta limitaciones que deben ser consideradas, especialmente por PYMEs con recursos restringidos. La complejidad técnica es una de ellas; implementar esta tecnología requiere conocimientos especializados en criptografía, desarrollo de contratos inteligentes y gestión de infraestructuras distribuidas.

Otra limitación es el costo de adopción inicial, que si bien ha disminuido con opciones como Blockchain-as-a-Service (BaaS), aún representa una barrera para muchas pequeñas empresas. Esto incluye inversiones en capacitación del personal, integración con sistemas existentes y posibles ajustes normativos.

También existe el reto de la escalabilidad y velocidad de las transacciones, dependiendo del tipo de red Blockchain utilizada. En algunos casos, las transacciones pueden presentar latencias que no son ideales para operaciones en tiempo real como las del comercio electrónico. Finalmente, persiste una falta de claridad normativa en algunos países, lo que genera incertidumbre jurídica sobre el uso de esta tecnología en contextos comerciales.

Recomendaciones Técnicas y Regulatorias

Desde el punto de vista técnico, las PYMEs deben considerar aspectos como la interoperabilidad con sus sistemas actuales, la escalabilidad del modelo Blockchain elegido y los requerimientos de almacenamiento y procesamiento. También se deben adoptar buenas prácticas en criptografía, gestión de claves y contratos inteligentes, evitando implementar soluciones sin el respaldo de expertos o proveedores confiables.

En términos regulatorios, es importante asegurar el cumplimiento de la Ley 1581 de 2012 de Protección de Datos Personales en Colombia y las directrices del marco legal de

ciberseguridad nacional. Las empresas deben tener claridad sobre cómo la información será tratada, almacenada y quién tendrá acceso, especialmente cuando se empleen Blockchains públicas o híbridas. Además, deben considerar estándares internacionales como el NIST Cybersecurity Framework y las guías de la ISO/IEC 27001, que pueden complementar el diseño de una arquitectura de seguridad más robusta.

Futuras Líneas de Investigación en Ciberseguridad y Blockchain

Dada la constante evolución del panorama digital, se abren múltiples líneas de investigación que podrían complementar y extender este trabajo. Una de ellas es el desarrollo de modelos de ciberseguridad basados en Blockchain y **machine learning**, que permitan anticipar y prevenir ataques mediante análisis predictivo. Otra línea relevante es el estudio de Blockchain para asegurar cadenas de suministro digitales en e-commerce, garantizando la trazabilidad desde el proveedor hasta el cliente final.

También se requiere mayor investigación sobre modelos de identidad digital descentralizada aplicados al comercio electrónico, que permitan a los usuarios tener mayor control sobre sus datos personales. Finalmente, se recomienda explorar los impactos de la regulación emergente en tecnologías disruptivas, para alinear las soluciones tecnológicas con el entorno legal y garantizar su sostenibilidad a largo plazo en el sector PYME.

Conclusiones

La presente monografía permitió abordar de manera integral uno de los desafíos más relevantes que enfrentan actualmente las pequeñas y medianas empresas del sector retail y comercio electrónico: la creciente exposición a amenazas cibernéticas en un entorno digital dinámico y altamente vulnerable. A partir del análisis realizado, se evidenció que, a pesar de la criticidad de los riesgos como el ransomware, el phishing, los fraudes en pagos electrónicos o el robo de credenciales, muchas PYMEs aún dependen de soluciones tradicionales de seguridad, centradas en infraestructuras centralizadas que presentan puntos únicos de fallo y son limitadas frente a ataques sofisticados.

Frente a este panorama, la tecnología Blockchain se plantea no solo como una solución tecnológica emergente, sino como una herramienta estratégica que transforma el enfoque con el que se concibe la seguridad informática. Su capacidad para descentralizar la gestión de datos, garantizar la inmutabilidad de la información y permitir la trazabilidad de operaciones en tiempo real posiciona a Blockchain como un mecanismo ideal para fortalecer la resiliencia cibernética de las PYMEs. La integración de contratos inteligentes, el uso de identidades digitales descentralizadas y la automatización segura de procesos son elementos clave que aportan tanto eficiencia como protección en los entornos digitales donde estas empresas operan.

Asimismo, el estudio evidenció que existen barreras reales que limitan la adopción de Blockchain en este tipo de organizaciones, como la falta de conocimiento técnico, los costos iniciales de implementación, la incertidumbre regulatoria y la resistencia al cambio. Sin embargo, también se identificaron soluciones viables como las plataformas BaaS (Blockchain as a Service), que permiten una implementación progresiva, segura y ajustada a las capacidades de

las PYMEs, además de marcos normativos y buenas prácticas que orientan su despliegue responsable.

En cuanto a los objetivos propuestos, el desarrollo del Capítulo 1 permitió realizar un diagnóstico detallado sobre las principales vulnerabilidades a las que se enfrentan las PYMEs del sector retail y comercio electrónico. Se evidenció que muchas de estas empresas carecen de políticas de respaldo seguras, presentan configuraciones débiles en sus sistemas, utilizan contraseñas simples o compartidas, y tienen escasa trazabilidad sobre accesos y modificaciones en sus plataformas digitales. Estas debilidades estructurales incrementan la probabilidad de sufrir ataques como ransomware, phishing, robo de credenciales y fraudes en pagos electrónicos, poniendo en riesgo la continuidad operativa, la confianza del cliente y la integridad de la información.

En el Capítulo 2, se abordaron los fundamentos técnicos y operativos de la tecnología Blockchain, analizando sus propiedades clave como la descentralización, la inmutabilidad, la transparencia y la trazabilidad. Se destacó que Blockchain no solo constituye una solución innovadora, sino que puede integrarse de forma escalonada y estratégica dentro de entornos empresariales con recursos limitados. El capítulo expone cómo características como los contratos inteligentes, la gestión de identidad descentralizada (DID), el uso de registros inmutables y la automatización de eventos de seguridad pueden convertirse en pilares fundamentales para fortalecer la ciberseguridad de estas organizaciones.

El Capítulo 3, estuvo enfocado en el diseño de estrategias concretas que integran soluciones de Blockchain con el propósito de mitigar las vulnerabilidades previamente identificadas. Cada propuesta fue orientada a una debilidad puntual, demostrando su aplicabilidad a partir de escenarios reales y necesidades operativas de las PYMEs. Así, se

propuso el uso de hash criptográficos para validar la integridad de respaldos, mecanismos de autenticación descentralizada para evitar accesos no autorizados, contratos inteligentes para eliminar errores humanos en procesos críticos, y registros distribuidos para auditar accesos y transacciones en tiempo real. Además, se evaluó la viabilidad operativa de estas estrategias, resaltando modelos como Blockchain-as-a-Service (BaaS) que permiten implementar soluciones sin requerir una infraestructura costosa ni conocimientos técnicos avanzados. Estas alternativas demuestran que es factible aplicar esta tecnología incluso en organizaciones con limitaciones estructurales, siempre que exista una planificación estratégica.

En conjunto, los hallazgos de los tres capítulos permiten dar respuesta a la pregunta problémica de esta investigación: sí, es posible que las PYMEs del sector retail y comercio electrónico fortalezcan su resiliencia frente a ciberataques mediante la adopción de tecnologías emergentes como Blockchain, siempre y cuando se orienten a resolver vulnerabilidades específicas, se adapten a las condiciones internas de cada organización y se acompañen de procesos progresivos de adopción, capacitación y alineación normativa.

Finalmente, este trabajo no solo aportó una propuesta concreta de estrategias para la adopción de Blockchain en ciberseguridad, sino que también abrió nuevas líneas de investigación aplicables a la protección de activos digitales, la autenticación de usuarios, la trazabilidad de procesos y la automatización de controles internos. En un sector donde la confianza digital es determinante para la competitividad, las PYMEs

Referencias Bibliográficas

Aarness, A. (2024, June 7). *What is EDR? Endpoint Detection & Response Defined | CrowdStrike*. What Is Endpoint Detection and Response (EDR)? https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/

Alzate, P., Giraldo, D., Alzate, P., & Giraldo, D. (2023). Tendencias de investigación del blockchain en la cadena de suministro: transparencia, trazabilidad y seguridad. *Revista Universidad y Empresa*, *25*(44), 1–29. https://doi.org/10.12804/REVISTAS.UROSARIO.EDU.CO/EMPRESA/A.12451

Antoniucci, A. G., Sierra, M. R., Jesús Báez, A., & Crisafulli, M. (2024). *Informática y derecho revista iberoamericana de derecho informático (segunda época) blockchain y la seguridad de la información en américa y europa blockchain and information security*.

Ardila, F. (n.d.). *Social Commerce, la preferencia de los consumidores al realizar sus compras online-Insight | Keyrus*. Retrieved May 19, 2025, from https://keyrus.com/latam/es/insights/social-commerce-la-preferencia-de-los-consumidores-al-realizar-sus-compras

Atiencia García, Y. L., & Jaramillo Villafuerte, R. F. (2024). Evaluación del impacto de la inteligencia artificial en las prácticas comerciales de las PYMES en el sector de la construcción en San Miguel de Bolívar. *Reincisol.*, *3*(6), 4662–4679. https://doi.org/10.59282/reincisol.V3(6)4662-4679

Augusto Coca, G. (2024). *Evaluación de la implementación de la Industria 4.0 en la cadena de suministro de las Pymes del Sector Textil – Confección localizadas en el*

municipio de Itagüí. https://repository.eia.edu.co/server/api/core/bitstreams/80183cb1-bd83-4c7a-a73f-f6e048c3ba73/content

Babu, S. (2024, September 5). *Las 12 principales amenazas para la seguridad del comercio electrónico y cómo proteger su tienda*. Las 12 Principales Amenazas Para La Seguridad Del Comercio Electrónico y Cómo Proteger Su Tienda. https://geekflare.com/es/e-commerce-security-threats/

Bistamp Learn. (2024, March 8). *Aplicaciones del Blockchain en el Mundo Real*. https://www.bitstamp.net/es/learn/crypto-101/real-world-applications-of-blockchain/?utm_source=chatgpt.com

SAP. (2025). *¿Qué es la tecnología blockchain?* https://www.sap.com/latvia/products/technology-platform/what-is-blockchain.html?utm_source=chatgpt.com

Botero Maria Camila. (2023, September 19). *Ciberataque a IFX Networks: la amenaza que golpea a Colombia*. El Ataque Cibernético Que Sacude a Colombia. https://www.javeriana.edu.co/pesquisa/ciberataque-ifx-networks-colombia/

Burgos, M. F. (2024, September 23). *Integración de tecnología Blockchain para mejorar la eficiencia y seguridad en los procesos de Auditoría interna en gestión empresarial y procesos contables de las PYMES del sector manufacturero en Bucaramanga en el año 2024.* http://repositorio.uts.edu.co:8080/xmlui/bitstream/handle/123456789/17208/F-DC-125__Informe_final_MAIRA%20BURGOS.pdf?sequence=1&isAllowed=y

Checkpoint. (2025). *¿Qué es una violación de datos? - Software Check Point*. https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-a-data-breach/

Congreso de Colombia. (1999). *Ley_527_de_1999*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=4276

Congreso de Colombia. (2012). *Ley_1581_de_2012*. https://www1.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

Cybersecurity Ventures. (2020). *Los delitos cibernéticos costarán al mundo 10,5 billones de dólares anuales para 2025*. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Diario Oficial de la Unión Europea. (2016). *REGLAMENTO (UE) 2016/ 679 DEL PARLAMENTO EUROPEO Y DEL CO NSEJO*. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Docusign. (2022, December 28). *Conoce los 7 mejores métodos de seguridad informática para tu empresa*. Conoce Los 7 Mejores Métodos de Seguridad Informática Para Tu Empresa. https://www.docusign.com/es-mx/blog/desarrolladores/seguridad-informatica

enisa. (2025, March 26). *Panorama de amenazas espaciales de ENISA 2025 | ENISA*. https://www.enisa.europa.eu/publications/enisa-space-threat-landscape-2025

eset. (2024). *Ransomware en 2024: un año récord a nivel de impacto y ganancias | ESET*. https://www.eset.com/ve/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/ransomware-en-2024-un-ano-record-a-nivel-de-impacto-y-ganancias/

García Munguía, M., Moreno Gutiérrez, S., Molina Ruiz, H. D., & Reséndiz, A. (2022). *Vista de Blockchain y la ciberseguridad* (vol 9; pp. 15–20). https://repository.uaeh.edu.mx/revistas/index.php/tepexi/article/view/8695/9069

Gonzales Llorente, P. (2023, June 1). *Ransomware y phishing: qué son y en qué se diferencian*. ¿Qué Es El Ransomware y En Qué Se Diferencia Del Phishing? https://sellolegal.com/blog/que-es-el-ransomware-y-en-que-se-diferencia-del-phishing/

Grigera del Campillo, S. (2022). Ciberseguridad y Blockchain. *Revista Blockchain e Inteligencia Artificial*, *3*. https://doi.org/10.22529/rbia.2021(3)05

Hanafizadeh, P., & Alipour, M. (2024). Taxonomy of theories for blockchain applications in business and management. *Digital Business*, *4*(2). https://doi.org/10.1016/j.digbus.2024.100080

Hancco Quispe, J. K., Borda Colque, J. P., Ticona Salluca, H., Torres-Cruz, F., Aleman Gonzales, L., Mamani Luque, O. M., Supo Gutierrez, J. A., & Laura Murillo, R. P. (2023). *ADOPCIÓN DE ESTRATEGIAS DE CIBERSEGURIDAD PARA LA BLOCKCHAIN*. https://downloads.editoracientifica.com.br/articles/230312490.pdf

Holanda Dias Kershaw, G. H. (2023, December 1). *Statista (2023). Number of Internet and Social Media Users Worldwide as of January 2023. - References - Scientific Research Publishing*. https://www.scirp.org/reference/referencespapers?referenceid=3620487

IBM. (2025). *¿Qué es Blockchain? | IBM*. https://www.ibm.com/es-es/topics/blockchain?utm_source=chatgpt.com

Ingefor, & Bellanato Rodriguez Oscar. (2025, January 2). *Ataques Informáticos y su Impacto en las PYMEs*. https://ingefor.com/mas-del-60-de-las-empresas-cierran-tras-un-ataque-informatico/

ISACA. (2023, December 5). *Blog de ISACA Now 2023: La importancia de la ciberseguridad para las pequeñas empresas*. La Importancia de La Ciberseguridad Para Las Pequeñas Empresas: Aplicación de Los Principios de Confianza Cero. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/the-essentiality-of-cybersecurity-for-small-businesses?utm_source=chatgpt.com

Iso. (2022). *Information security, cybersecurity and privacy protection-Information security management systems-Requirements*. https://ia600500.us.archive.org/6/items/iso27001/iso27001.pdf

ISO. (2023). *ISO - Gestión de identidades: ¿Qué debe saber?* https://www.iso.org/es/seguridad-informacion/gestion-de-identidades

Kim, H. M., & Laskowski, M. (2018, January 1). Toward an ontology-driven blockchain design for supply-chain provenance. *Intelligent Systems in Accounting, Finance and Management*, *25*(1), 18–27. https://doi.org/10.1002/ISAF.1424

Lansiti, M., & Lakhani, K. (2020, February). *La verdad sobre blockchain*. https://hbr.org/2017/01/the-truth-about-blockchain

Ley 1581 de 2012 - Gestor Normativo - Función Pública, Ley 1581 de 2012 (2012). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Lfdecentralizedtrust. (2024). *Cómo Walmart logró una transparencia sin precedentes en la cadena de suministro de alimentos con Hyperledger Fabric*. Ómo Walmart Logró Una Transparencia Sin Precedentes En La Cadena de Suministro de Alimentos Con

Hyperledger Fabric. https://www.lfdecentralizedtrust.org/case-studies/walmart-case-study

Lucía Ramirez Blanco, M., Victoria Arango Olmos, A., Blum de Barberi, C., Carrasquilla Barrera, A., Leonor Cabello Blanco, M., Holmes Trujillo García Ministro de Defensa Nacional Rodolfo Enrique Zea Navarro, C., Ruíz Gómez, F., Custodio Cabrera Báez Ministro de Trabajo Carolina Rojas Hayes, Á., Manuel Restrepo Abondano, J., Victoria Angulo González Ministra de Educación Nacional Ricardo José Lozano Picón, M., Tybalt Malagón González Ministro de Vivienda, J., Territorio Karen Abudinen Abuchaibe, C., María Orozco Gómez, Á., Lucena Barrero, E., Gisela Torres Torres, M., Alberto Rodríguez Ospino, L., & Gómez Gaviria Subdirector General Sectorial Amparo García Montaña Subdirectora General Territorial, D. (2020). *CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL CONPES*. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Mansa Julio. (2024, July 20). *Significado de Blockchain como servicio (BaaS) y actores principales*. https://www-investopedia-com.translate.goog/terms/b/blockchainasaservice-baas.asp?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sge

Peña Valenzuela, D., Sebastián, J., & Castillo, A. (2021). *COMERCIO INTELIGENTE: LA TRANSFORMACIÓN DEL COMERCIO ELECTRÓNICO A LA LUZ DE LAS TECNOLOGÍAS EMERGENTES Y DISRUPTIVAS Profesor nacional invitado*.

Rasectech. (2023, November 8). *¿Qué es la obsolescencia tecnológica y cómo afecta a mi empresa?* ¿Qué Es La Obsolescencia Tecnológica y Cómo Afecta a Mi Empresa? https://blog.rasec-tech.com/2023/11/que-es-la-obsolescencia-tecnologica-y.html?

Roch Moraguez, E. (2025). *Seguridad en Aplicaciones de Comercio Electrónico: Protege a tus Clientes*. Seguridad En Aplicaciones de Comercio Electrónico: Protege a Tus Clientes. https://lovtechnology.com/seguridad-en-aplicaciones-de-comercio-electronico-protege-a-tus-clientes/

Rosales Álvarez, Á., Parra Gutiérrez, B. Y., & Varón Quimbayo, Á. A. (2023). Aplicabilidad de Blockchain en créditos digitales a través de contratos inteligentes en el entorno jurídico. *ReDDI: Revista Digital Del Departamento de Ingeniería*, *7*(2), 1–13. https://doi.org/10.54789/REDDI.7.2.1

Rowntree, L. (2023, June 6). *2023 Data Breach Investigations Report: frequency and cost of social engineering attacks skyrocket | News Release | Verizon*. Informe de Investigaciones Sobre Violaciones de Datos de 2023: La Frecuencia y El Coste de Los Ataques de Ingeniería Social Se Disparan. https://www.verizon.com/about/news/2023-data-breach-investigations-report

SEON. (2025). *High Risk Payment Methods Impacted by Fraud Risk | SEON*. Assessing Fraud in High-Risk Payment Methods. https://seon.io/resources/which-online-payment-methods-have-the-highest-fraud-risk/

Seon. (2025). *Monitorear transacciones cripto usando reglas de riesgo | SEON*. https://seon.io/es/recursos/rastreo-de-transacciones-con-criptomonedas/

Shoemaker, P. (2025). *¿Qué es la identidad descentralizada? Una guía completa*. https://www.identity.com/decentralized-identity/

Sophos. (2024). *TREN DS FROM TH E DARK WEB R A N S O M WA R E I N H1 2024*. https://assets.sophos.com/X24WTUEQ/at/wwf5phjtj9bjvmpqqsbfxc/sophos-2024-threat-report.pdf

Superintendencia de vigilanci y seguridad Privada. (2025). *SARLAFT*. ¿Qué Es El SARLAFT? https://www.supervigilancia.gov.co/sarlaft/publicaciones/10005/sarlaft/

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2), 147–156. https://doi.org/10.1016/J.DCAN.2019.01.005

Tort, L. P. (2023). Web 3.0 y DeFi: Cómo la tecnología blockchain está cambiando las finanzas. *Revista de Contabilidad y Dirección*, *35*(2023), 91–113.

verizon. (2023). *Data Breach Investigations Report Public Sector Snapshot*.

webscale. (2022). *Informe global sobre seguridad del comercio electrónico 2022 - www.webscale.com*. https://www.webscale.com/global-ecommerce-security-report-2022/

Welivesecurity By Eset, & Bocconi Maria. (2023, November 6). *Ataque ransomware al grupo GTD afecta organismos públicos y empresas de Chile y Perú*. Ataque Ransomware al Grupo GTD Afecta Organismos Públicos y Empresas de Chile y Perú. https://www.welivesecurity.com/es/ransomware/ransomware-afecta-grup-gtd-organismos-chile-peru/

Apéndices

Apéndice A

Checklist de Ciberseguridad para PYMEs del Retail y E-commerce

La tabla reúne una lista de verificación con acciones y controles esenciales para fortalecer la seguridad digital en PYMEs del sector retail y comercio electrónico. Incluye medidas preventivas, técnicas y organizacionales para mitigar riesgos y garantizar la protección de datos.

Tabla 5

Lista de Chequeo para Pymes del Retail y E-commerce

Pregunta	Sí / No	Observaciones
¿Cuenta con políticas de seguridad de la información documentadas?	☐ / ☐	
¿Utiliza autenticación multifactor (MFA)?	☐ / ☐	
¿Tiene copias de seguridad regulares y fuera de línea?	☐ / ☐	
¿Monitorea accesos no autorizados a sus sistemas?	☐ / ☐	
¿Usa tecnología Blockchain o BaaS para verificar transacciones críticas?	☐ / ☐	
¿El personal está capacitado en prevención de phishing?	☐ / ☐	

Nota. La tabla presenta un Checklist de ciberseguridad diseñado para PYMEs del retail y e-commerce, que abarca prácticas clave como la protección de datos, la gestión de accesos, la actualización de sistemas y la capacitación del personal. Su propósito es servir como guía de autoevaluación y mejora continua en la gestión de la seguridad informática.

Apéndice B

Cuestionario de Autoevaluación para la Adopción de Blockchain

La tabla contiene un cuestionario de autoevaluación orientado a determinar el nivel de preparación de una PYME para adoptar soluciones basadas en Blockchain. Incluye criterios técnicos, organizacionales y regulatorios que permiten identificar fortalezas y áreas de mejora antes de la implementación.

Tabla 6

Cuestionario de Autoevaluación para la Adopción Blockchain

Autoevaluación	Repuesta
¿Qué tipo de información crítica desea proteger?	
¿Cuenta con personal capacitado en tecnologías emergentes?	
¿Conoce qué proveedores ofrecen servicios BaaS?	
¿Ha sufrido incidentes de seguridad que comprometan datos de clientes?	
¿Necesita trazabilidad de productos o procesos?	

Nota. La tabla muestra un cuestionario estructurado para que las PYMEs del retail y comercio electrónico evalúen su preparación frente a la adopción de tecnologías Blockchain. Contempla aspectos como infraestructura tecnológica, capacitación del personal, cumplimiento normativo y disposición organizacional, facilitando la toma de decisiones estratégicas para su implementación.

Apéndice C

Buenas Prácticas para Pymes que Implementan Blockchain

Identificar procesos críticos donde Blockchain pueda aportar valor (transacciones, trazabilidad, verificación de identidad).

Empezar con pilotos controlados utilizando plataformas de Blockchain-as-a-Service.

Asegurar la compatibilidad con marcos normativos locales (Ley 1581, Ley 527, Decreto 1074, etc.).

Implementar claves criptográficas seguras y planes de recuperación ante pérdida de credenciales.

Asegurar que los datos personales sean tratados conforme a principios de minimización y confidencialidad, incluso dentro de Blockchain.

Usar contratos inteligentes para automatizar pagos, entrega de productos o validaciones de identidad.

Involucrar a todo el personal en una cultura de seguridad y actualización constante.

Apéndice D

Estrategias de Concienciación y Cultura de Seguridad para Pymes

Brindar un conjunto de acciones y recomendaciones para fortalecer la cultura de ciberseguridad en las pequeñas y medianas empresas del sector retail y comercio electrónico, contribuyendo a la reducción de riesgos humanos y fomentando la adopción segura de tecnologías como Blockchain.

La tabla reúne un conjunto de buenas prácticas orientadas a fortalecer la cultura de seguridad en PYMEs del retail y comercio electrónico, fomentando la participación de todo el personal en la protección de la información.

Tabla 7

Buenas Prácticas para Promover la Cultura de Seguridad

Práctica	Descripción
Capacitación periódica	Realizar talleres y charlas cortas sobre phishing, ingeniería social, manejo seguro de datos, uso de contraseñas seguras y actualizaciones.
Simulacros de ciberataques	Ejecutar simulaciones controladas de ataques tipo phishing o ransomware para medir la respuesta del personal y reforzar aprendizajes.
Política clara de uso aceptable	Establecer y comunicar reglas claras sobre el uso de dispositivos, software, internet, correos y redes sociales corporativas.
Designar un "líder de seguridad" interno	Nombrar un responsable que monitoree, comunique y actualice prácticas de seguridad con lenguaje accesible para todos.
Cartelería visible en oficinas	Ubicar posters o recordatorios visuales sobre buenas prácticas de seguridad (ej. "Piensa antes de hacer clic", "Verifica antes de compartir").
Campañas internas mensuales	Enviar boletines o realizar dinámicas temáticas que mantengan vigente la importancia de la ciberseguridad.
Gamificación o incentivos	Implementar sistemas de puntos o premios por buenas prácticas (detectar correos sospechosos, actualizar claves, reportar incidentes).
Fomentar el "error reportable"	Promover una cultura libre de culpa donde cualquier empleado pueda reportar incidentes o errores sin temor a represalias.

Nota. La tabla presenta recomendaciones clave para promover la cultura de seguridad informática en PYMEs, incluyendo acciones como la capacitación continua, la definición de políticas claras, la simulación de incidentes y el reconocimiento de buenas prácticas. Estas medidas buscan consolidar hábitos seguros y un entorno organizacional resiliente frente a amenazas cibernéticas.

Apéndice E

Test para Medir la Concienciación del Equipo

La tabla contiene una prueba diseñada para evaluar el nivel de concienciación del personal frente a amenazas y prácticas de ciberseguridad, identificando fortalezas y áreas que requieren capacitación adicional.

Para la siguiente información si se tienen 6 respuestas “Sí” o más indican buen nivel de concienciación. Menos de 6 requieren reforzar formación.

Tabla 8

Test Concienciación Equipo

¿Reconoces un correo sospechoso o con enlaces maliciosos?	SI / NO
¿Cambias tus contraseñas regularmente y usas contraseñas robustas?	
¿Sabes qué hacer si detectas una actividad anómala en tu correo o sistema?	
¿Utilizas diferentes contraseñas para distintos servicios?	
¿Conoces la política de seguridad de tu empresa?	
¿Sabes cómo y a quién reportar un incidente informático?	
¿Tienes cuidado al abrir archivos adjuntos que no esperabas?	
¿Entiendes los riesgos de compartir información personal o de clientes por canales no cifrados?	

Nota. La tabla presenta una prueba de concienciación dirigido a los equipos de trabajo de PYMEs del retail y comercio electrónico, enfocado en medir el conocimiento sobre riesgos cibernéticos, el manejo seguro de la información y las respuestas adecuadas ante incidentes. Sus

resultados permiten orientar programas de formación y reforzar las políticas de seguridad existentes.

Apéndice F

Conceptos

Ataques DDoS: Ataques de denegación de servicio distribuidos que buscan saturar los servidores y hacer inaccesibles los servicios online.

Blockchain: Tecnología de registro distribuido que almacena datos de forma segura, descentralizada e inmutable, empleando bloques encadenados criptográficamente.

BaaS (Blockchain as a Service): Modelo de prestación de servicios que permite a las empresas utilizar Blockchain a través de plataformas en la nube como AWS, Azure o IBM sin gestionar la infraestructura directamente.

Criptografía: Ciencia que se encarga de proteger la información mediante técnicas de cifrado y autenticación. En Blockchain se utilizan funciones hash y criptografía de clave pública para asegurar integridad y confidencialidad.

Contrato inteligente (Smart Contract): Código programable que se ejecuta automáticamente en Blockchain cuando se cumplen ciertas condiciones. Elimina la necesidad de intermediarios y garantiza transacciones seguras.

Conpes 3995 de 2020: Documento del gobierno colombiano que promueve la adopción de tecnologías emergentes como Blockchain para fortalecer la seguridad digital.

Identidad digital descentralizada (DID): Sistema de autenticación basado en Blockchain donde los usuarios controlan directamente su identidad, sin depender de entidades centrales.

ISO/IEC 27001: Estándar internacional para establecer, implementar y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

Ley 1581 de 2012: Norma colombiana que regula la protección de datos personales y establece principios como seguridad, confidencialidad y consentimiento informado.

Phishing: Técnica de ingeniería social para obtener información confidencial (como credenciales), suplantando identidades mediante correos o sitios falsos.

Resiliencia cibernética: La capacidad de una organización para anticipar, resistir, recuperarse y adaptarse a incidentes cibernéticos que puedan afectar sus sistemas o datos.

Ransomware:Software malicioso que cifra los datos de una organización y exige un pago (rescate) para restaurar el acceso.

Reglamento general de protección de datos (GDPR): Regulación europea que establece directrices estrictas para la protección de datos personales y la privacidad.

Tokenización: Proceso mediante el cual se representa un activo físico o digital como un token en Blockchain, facilitando su trazabilidad y seguridad.

Trazabilidad: Capacidad para seguir el rastro de una transacción o dato a lo largo de una cadena de bloques, garantizando transparencia y verificación.