Estrategias de ciberseguridad para la protección de la infraestructura cibernética de las (pymes), mediante el estudio de vectores de ataque para fortalecer la seguridad informática

Julián Alexis Largo Piedrahita

Tutor

Christian Hernán Obando Ibarra

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Dedicatoria

Este trabajo es dedicado a mi madre, hermana y tía quienes me impulsaron a continuar con mis estudios universitarios y crecer profesionalmente.

Agradecimientos

Agradezco a mi tutor por su apoyo y orientación durante la realización de este trabajo de grado, lo cual me permitió cumplir con las expectativas establecidas

Resumen

En la actualidad, (PYMES) presentan desafíos es sus infraestructuras, dado que es un sector muy susceptible a los diferentes vectores ataque que afectan la continuidad operativa de los recursos tecnológicos y activos de la organización. Es fundamental que las pymes comprendan y entiendan la existencia de estos vectores de ataque cibernéticos a los que están expuestos y los métodos y tácticas que utilizan los ciberdelincuentes para las víctimas divulguen información sensible. es esencial que las pymes desarrollen posturas de ciberseguridad mediante el uso de herramientas de código abierto y la implementación de programas de educación en seguridad informática, con el fin de minimizar y contrarrestar las amenazas que dañan gravemente la estabilidad operativa de las pymes en el entorno digital. Además, las pymes al adoptar buenas prácticas de ciberseguridad en sus organizaciones garantizan protección y confianza a los usuarios como clientes, ya que aplicar estas estrategias de seguridad ayudan a minimizar estas amenazas que afectan cada día la infraestructura cibernética de las pymes.

Finalmente, las pymes que fomentan una cultura en sensibilización en ciberseguridad en capacitando a los empleados en cómo puede reconocer el vector de ataque phishing, dado que esta la amenaza más común hoy en día que utilizan los ciberdelincuentes para que las victimas compartan información personal y privada.

Palabras clave: Ciberseguridad, PYMES, Phishing, Protección de datos, Intrusiones Informáticas, Pymes, Vectores de Ataque, Código Abierto Amenazas y Vulnerabilidades

Abstract

Currently, small and medium-sized enterprises (SMEs) face challenges in their infrastructures, as this sector is highly vulnerable to different attack vectors that affect the operational continuity of the organization's technological resources and assets. It is essential for SMEs to understand and recognize the existence of these cyberattack vectors to which they are exposed, as well as the methods and tactics used by cybercriminals to make victims disclose sensitive information. Therefore, it is crucial for SMEs to develop cybersecurity postures through the use of open-source tools and the implementation of information security education programs, in order to minimize and counteract threats that severely damage their operational stability in the digital environment. Moreover, when SMEs adopt good cybersecurity practices within their organizations, they provide protection and build trust with their users and customers, since applying these security strategies helps reduce the threats that impact the cyber infrastructure of SMEs every day. Finally, SMEs that promote a culture of cybersecurity awareness by training employees on how to recognize phishing attack vectors which remain the most common threat used by cybercriminals today to trick victims into sharing personal and private information strengthen their overall resilience against cyber risks.

***Keywords*:** Cybersecurity, SMEs, Phishing, Data Protection, Computer Intrusions, attack vectors, open source threats and vulnerabilities

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Glosario

Amenaza

Son los tipos de actividades que pueden afectar gravemente cualquier sistema tecnológico de una empresa. además "para un sistema informático es una circunstancia que tiene el potencial de causar daños o pérdidas. Es decir, las amenazas pueden dar lugar a un ataque en el equipo." (Avenía, 2017)

Ciberdelincuentes

Son personas que aprovechan de los recursos digitales para cometer delitos informáticos en el propósito de tener un beneficio mutuo. También estas son "actividades delictivas que se llevan a cabo a través de medios tecnológicos. Los ciberdelincuentes atacan a personas, empresas, entidades de distintos tipos y gobiernos con diferentes objetivos: tanto para destruir o dañar sus sistemas informáticos y sus conexiones." (Unir, 2020)

Ciberseguridad

Son métodos y tácticas que se emplean para salvaguardar los recursos tecnológicos e informáticos. De tal modo, esto permite la "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados." (Valoyes, 2019)

Código abierto (open source)

Se refiere al software que permite que cualquier tipo de persona este tenga acceso, además este lo pueda modificar para que tengan nuevas mejoras, funciones y sea adaptable a las necesidades específicas. También es "un método de desarrollo de software en el que los desarrolladores voluntarios contribuyen a un proyecto en particular y donan todo su código fuente y sus esfuerzos de documentación al público para el beneficio de todos." (Jiang, 2022)

Infraestructura cibernética

son los sistemas tecnológicos digitales que lo componen una organización, como el software, hardware, redes, servidores entre otros. además, también

son “el conjunto de dispositivos físicos y aplicaciones de software que se requieren para operar toda la empresa.” (UNSA, 2019)

Pymes

Son las pequeñas y medianas empresas que proporciona crecimientos significativos y económicos a un país. además, las pymes “se definen como una unidad económica que desarrolla cualquier tipo de actividad empresarial, operada por una persona natural o jurídica con un nivel de recursos reducidos, un rango establecido de trabajadores y niveles de ventas.” (Muñoz, 2019)

Sistemas informáticos

son los elementos con que los usuarios tiene interacción sea el software o el hardware para agilizar los procesos de gestión de actividades específicas para generar competitividad y eficiencia empresarial. Además, también son un “conjunto de elementos físicos y lógicos que se encargan de recibir, guardar y procesar datos para luego entregarlos en forma de resultados.” (Universidad, 2023)

Vectores de ataque

Son las modalidades que utilizan los atacantes informáticos para tener acceso no autorización a los sistemas informáticos de una organización. También un vector de ataque “Es una ruta o método específico utilizado por un atacante para ingresar o comprometer un sistema o red.” (Cilleruelo, 2024)

Vulnerabilidad

“es una debilidad del sistema informático que puede utilizarse para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.” (Avenía, 2017)

Introducción

La transformación digital ha modificado de manera acelerada la forma en que operan las organizaciones en Colombia, impulsando la adopción de herramientas tecnológicas para optimizar procesos administrativos, comerciales y financieros; sin embargo, este proceso de modernización también ha incrementado la exposición a riesgos asociados con la ciberseguridad; la capacidad limitada de muchas pequeñas y medianas empresas para invertir en infraestructura tecnológica especializada ha dejado espacios de vulnerabilidad que pueden ser explotados por actores maliciosos. La dependencia creciente de sistemas de facturación electrónica, plataformas en la nube y servicios de banca digital, han convertido las pymes en un objetivo frecuente de ataques que buscan comprometer la disponibilidad, integridad y confidencialidad de la información.

En este escenario, los ciberdelitos no solo representan una amenaza técnica, sino también un riesgo económico y legal para las PYMES colombianas. las pérdidas asociadas a un incidente pueden abarcar desde la interrupción temporal de operaciones hasta sanciones regulatorias por incumplimiento de normas de protección de datos. además, la reputación empresarial se ve comprometida cuando clientes y proveedores perciben que la organización carece de mecanismos efectivos para proteger la información que le confían. Por esta razón, la ciberseguridad se configura como un componente esencial en la sostenibilidad de las PYMES, exigiendo estrategias claras que permitan anticipar amenazas, implementar tecnologías de defensa y consolidar prácticas que fortalezcan la resiliencia digital en el ámbito empresarial.

Las pymes colombianas, que constituyen más del 99 % del tejido empresarial formal, se encuentran en un entorno digital que avanza con rapidez, pero que también incrementa su exposición a riesgos cibernéticos. la limitada inversión en infraestructura tecnológica y la

carencia de equipos especializados en seguridad informática han generado que ataques como phishing, ransomware, malware y denegaciones de servicio que se conviertan en amenazas recurrentes. Estas modalidades de intrusión no solo buscan obtener datos financieros o credenciales de acceso, sino que también afectan la disponibilidad de servicios esenciales como la facturación electrónica, la gestión de inventarios y la atención a clientes. en un escenario nacional donde la digitalización de procesos se ha convertido en una condición para la competitividad, este panorama sitúa a las PYMES como uno de los blancos más atractivos para los atacantes.

De acuerdo con informes de seguridad en la región, Colombia registra millones de intentos de ataque al año dirigidos específicamente a PYMES; la ingeniería social se manifiesta como la táctica preferida, explotando la confianza de los empleados y la falta de protocolos internos para inducir la entrega de información sensible; al mismo tiempo, la utilización de vulnerabilidades en sistemas desactualizados permite el despliegue de programas maliciosos capaces de paralizar por completo la operación empresarial; la identificación precisa de estos vectores y la comprensión de su impacto directo en la continuidad del negocio constituye la primera fase para formular estrategias efectivas de defensa en este sector.

En Colombia, las PYMES enfrentan limitaciones presupuestales que reducen su capacidad para adquirir soluciones de ciberseguridad comerciales, ante este desafío, las herramientas de código abierto han surgido como una alternativa accesible y flexible, al no requerir licenciamiento y ofrecer funcionalidades avanzadas. Estos programas como pfSense**,** orientado a la gestión de cortafuegos y redes privadas virtuales o ClamAV, diseñado para la detección de software malicioso en servidores y estaciones de trabajo. Con estos ejemplos se constituyen de cómo las empresas pueden fortalecer su seguridad a bajo costo; asimismo, Snort y

Wazuh amplían las capacidades de detección y respuesta ante incidentes, lo que permite una vigilancia constante del tráfico de red y la identificación de patrones maliciosos en tiempo real.

La adopción de estas plataformas open source, no está exenta de retos, la configuración y administración de sistemas open source demanda personal capacitado, lo que puede ser una limitación para muchas PYMES; aun así, la ventaja de poder personalizar los módulos de seguridad y adaptarlos a las condiciones de cada organización convierte a estas herramientas en un recurso estratégico para el sector empresarial colombiano. su implementación gradual, empezando por soluciones básicas y avanzando hacia sistemas integrales de gestión de incidentes, permite crear una infraestructura digital más resistente frente a los vectores de ataque que caracterizan al entorno nacional.

Más allá de las herramientas tecnológicas, la seguridad digital de las PYMES depende de la adopción de prácticas organizacionales que fortalezcan su capacidad de respuesta ante amenazas como la gestión de contraseñas seguras, la activación de autenticación multifactor y la actualización periódica de software son medidas mínimas que reducen significativamente el riesgo de intrusiones. A esto se suma la importancia de implementar copias de seguridad en la nube y en medios desconectados, las cuales garantizan la recuperación de información en caso de incidentes de *ransomware* u otras infecciones críticas; la estandarización de estas prácticas dentro de las pymes colombianas contribuye a crear un nivel básico de resiliencia en contextos donde los recursos tecnológicos suelen ser limitados.

En el entorno nacional, las entidades reguladoras y los gremios empresariales promueven lineamientos para que las PYMES adopten prácticas de ciberseguridad sin necesidad de inversiones desproporcionadas. La Ley 1581 de 2012, por ejemplo, obliga a proteger la información personal de clientes y empleados, lo que convierte la seguridad digital en un

requisito legal además de técnico. De tal modo, siguiendo estas directrices, las PYMES no solo evitan sanciones económicas, sino que también fortalecen la confianza de proveedores y consumidores, lo que resulta clave para su sostenibilidad en mercados cada vez más digitalizados. además, estas recomendaciones se convierten en un puente entre la teoría de la ciberseguridad y su aplicación práctica en el contexto colombiano.

El ser humano es, en la mayoría de los casos, el punto de entrada preferido por los atacantes. Las PYMES en Colombia enfrentan la constante amenaza de que sus empleados sean víctimas de phishing, llamadas fraudulentas o suplantaciones en redes sociales, debido a la escasa formación en temas de seguridad digital. La sensibilización del personal requiere procesos continuos que combinen talleres prácticos, simulaciones de ataques y difusión de protocolos claros de actuación frente a incidentes sospechosos. De este modo, los trabajadores desarrollan la capacidad de reconocer mensajes engañosos, remitentes irregulares o solicitudes inusuales de información, reduciendo las probabilidades de que un ataque prospere.

La cultura preventiva en materia de ciberseguridad debe integrarse al día a día de la organización, más allá de capacitaciones aisladas. En el contexto colombiano, donde aplicaciones como WhatsApp y redes sociales se utilizan de manera frecuente en entornos laborales, la exposición a intentos de fraude se amplifica. Instruir al personal para desconfiar de mensajes inesperados, confirmar identidades a través de canales oficiales y reportar de inmediato situaciones sospechosas fortalece la defensa digital desde la base misma de la organización. La sensibilización de los empleados no solo mitiga el riesgo de incidentes, sino que también convierte al capital humano en la primera línea de protección frente a los ciberdelincuentes.

Planteamiento del Problema

Hoy en día, las (pymes) en Colombia son un sector primordial para la economía, pero también a su alto crecimiento este se enfrenta a todo tipo de vectores de ataques cibernéticos que puede comprometer los sistemas informáticos de la organización. según (kaspersky, 2022) el 43% de las empresas han sido afectadas por ciberataques en los últimos años. Además reporta que "solo en 2023, Kaspersky bloqueó 30 millones de intentos de ataque contra pequeñas y medianas empresas en Colombia, y de ellos, más de 22 millones fueron intentos de ataque de phishing." (Itsitio, 2023) Estos ataques pueden resultar en la pérdida de datos críticos, perder confianza de los usuarios, afectación en la imagen de la empresa, sanciones legales y pérdidas monetarias significativas, que en algunos casos extremos pueden conllevar al cierre de la empresa.

En base a las consideraciones anteriores, las pymes colombianas faltan medidas robustas de seguridad y concientización de los propietarios de las empresas a sus empleados de las amenazas cibernéticas que están expuestos al no tener una protección adecuada en los sistemas informáticos. además, también hay que tener en cuenta que estas empresas no cuentan con los recursos financieros para desarrollar estrategias de ciberseguridad, lo que las convierte un blanco fácil para los ciberdelincuentes. De tal forma, "Para las pymes tiene limitaciones presupuestarias, lo cual se dificulta a menudo la aplicación de políticas integrales de ciberseguridad y además La falta de personal capacitado en entorno de seguridad cibernética." (Tuteja, 2024)

Sin embargo, este sector empresarial aún tiene las creencias que los ciberataques solo les pasan a las grandes organizaciones empresariales, dado por el hecho de ser pymes no les va a pasar ningún incidente de ciberseguridad. Por otro lado "las pymes se encuentran en un entorno cada vez más digitalizado, lo que les brinda oportunidades emocionantes, pero también plantea

desafíos significativos en términos de ciberseguridad.” (CyberEOP, 2025) lo cual al tener crecimientos económicos y de sostenibilidad adquieren nuevas herramientas tecnológicas para mejorar y agilizar sus procesos operativos, pero omiten que estas herramientas también tienen sus vulnerabilidades, lo que hay que contemplar la importancia de la ciberseguridad.

También hay que tener en cuenta, las pymes colombinas son susceptible a los ciberataques por su ingenuidad en ciberseguridad, lo que las convierte el objetivo principal de los ciberdelincuentes para ejecutar sus programas maliciosos, además los métodos y tácticas de ingeniería social para que las victimas divulguen información sensible a los ciber atacantes. “las pymes pueden albergar datos valiosos de sus clientes, como información de tarjetas de crédito o datos personales, convirtiéndolas en blancos ideales para los ataques cibernéticos.” (Docusign, 2023)

¿Cuáles son las estrategias de ciberseguridad a través de los vectores de ataque de seguridad informática que están expuestas las PYMES en Colombia?

Justificación

La ciberseguridad se ha transformado como un pilar fundamental para las (PYMES) colombianas, al tener como evidencia la situación problemática del poco interés, conocimiento e inversión en seguridad, donde se determina que este sector no cuenta con medidas suficientes de seguridad para proteger los sistemas informáticos ante los ciberataques. Estos ataques informáticos pueden causar daños significativos como robo de información, datos personales de los clientes, interrupciones en los sistemas, afectación en la imagen de la empresa, pérdidas económicas y financieras. “Estos ataques informáticos representan un costo considerable para las empresas de América Latina, puesto que pierden 2 millones de dólares por el impacto de los ciberataques” (Ccit, 2024)

En Base a lo anterior, la evolución de las nuevas innovaciones de las tecnologías de la información y el crecimiento de la interconexión de los sistemas informáticos aumentan los vectores de ataques cibernéticos en las (PYMES) en Colombia, los cuales están expuestas a sufrir ataques informáticos por el simple de hecho de no establecer medidas de ciberseguridad suficientes para proteger sus organizaciones. De tal modo, “A medida que las tecnologías emergentes superan a las medidas tradicionales de seguridad cibernética, muchas empresas tienen dificultades para invertir adecuadamente en ciberseguridad, las herramientas informáticas y las estrategias adecuadas para protegerse contra estos vectores de ataque que están en constante evolución.” (Hiscox, 2024)

Es por esto, las pymes pueden emplear medidas adecuadas de seguridad oportunas para minimizar impactos negativos ante los ciberataques como fomentar cultura de ciberseguridad entre los dueños de la empresas y empleados, los equipos de cómputo y dispositivos móviles que cuenten con programas de protección antimalware o spyware y usar de manera eficiente los

recursos informáticos para fines laborales entre otros aspectos de protección y seguridad. “Al tomar medidas de ciberseguridad esto ayuda a contrarrestar los vectores de ataque para proteger la información confidencial de las pymes y adoptando posturas en seguridad cibernética.” (Edorteam, 2024)

Por medio de esto, es de vital importancia que las (pymes) entiendan y comprendan los diferentes tipos de vectores cibernéticos que están expuestas, Lo cual esto permite proponer estrategias de ciberseguridad efectivas para minimizar los ciberataques y además fortalecer la seguridad en los sistemas informáticos. También hay que tener en cuenta emplear estas nuevas estrategias es fundamental investigar herramientas tecnológicas de ciberseguridad open source (código abierto) para garantizar y asegurar que estas puedan responder ante los vectores ataque cibernéticos en el entorno empresarial de las pymes. Además “Los clientes valoran la confianza al hacer negocios con pymes que demuestran un uso eficaz y responsable de la tecnología y son más atraídos a hacer negocios con esas empresas”. (Tuteja, 2024)

Objetivos

Objetivo General

Analizar estrategias de ciberseguridad destinadas a la protección de la infraestructura cibernética a través de un estudio de vectores de ataque de seguridad informática para las (PYMES) que permitan la generación de recomendaciones efectivas de herramientas open source que fortalezcan la defensa contra amenazas cibernéticas.

Objetivos específicos

Identificar los principales tipos vectores de ataques de ciberseguridad que afectan a las pymes, mediante la revisión de fuentes bibliográficas y bases científicas, con el propósito que tengan conocimiento de la gravedad de las amenazas cibernéticas que están expuestas.

Describir diversas herramientas de ciberseguridad de código abierto (open source) que permitan la protección de las infraestructuras cibernéticas en las pymes, a través de la revisión de material bibliográfico y cibergráfico

Proponer recomendaciones sobre las buenas prácticas de ciberseguridad mediante fuentes en línea para que las pymes tengan concientización sobre la importancia de la seguridad informática en sus organizaciones.

Plantear pautas de sensibilización en ciberseguridad a través de material de fuentes en línea para que los empleados reconozcan los vectores de ataque que emplean los ciberdelincuentes para que las victimas divulguen información confidencial.

Marco Referencial

Marco conceptual

Ciberseguridad

La ciberseguridad se entiende como la disciplina orientada a proteger infraestructuras tecnológicas y flujos de información frente a ataques digitales que comprometen la integridad, disponibilidad y confidencialidad de los datos. Para las PYMES colombianas, este concepto adquiere una dimensión estratégica debido a que gran parte de sus procesos administrativos, financieros y comerciales se encuentran hoy digitalizados. Asimismo, al ser organizaciones con limitados recursos para invertir en protección informática, se convierten en un blanco atractivo para los ciberdelincuentes. por esta razón, la ciberseguridad no debe percibirse únicamente como una obligación técnica, sino como una medida que resguarda la continuidad de los negocios, preserva la confianza de los clientes y garantiza el cumplimiento de normas como la Ley 1581 de 2012 sobre protección de datos personales (aws.amazon, 2023)

Ransomware: El ransomware constituye uno de los ataques más agresivos que enfrentan las PYMES en Colombia. Consiste en el secuestro de información mediante su encriptación, lo que impide el acceso a documentos, bases de datos y sistemas críticos. Posteriormente, los atacantes exigen un rescate económico a cambio de la liberación de los archivos, casos reportados en el país evidencian que incluso empresas del sector salud y de servicios han quedado paralizadas durante días, con consecuencias económicas y legales. en el entorno de las PYMES, este tipo de ataque puede significar la pérdida definitiva de información sensible, afectando tanto la reputación de la organización como la confianza de proveedores y clientes (kaspersky, 2022)

Phishing

El phishing representa el vector de ataque más común contra las PYMES colombianas, según reportes de entidades de ciberseguridad, este se caracteriza por la utilización de mensajes fraudulentos que aparentan provenir de fuentes legítimas, como bancos o entidades gubernamentales, con el objetivo de obtener contraseñas, números de tarjetas u otros datos confidenciales. En Colombia, el uso masivo del correo electrónico y la mensajería instantánea aumenta la exposición a este riesgo; muchas PYMES carecen de protocolos internos de verificación, lo que permite que los empleados caigan en el engaño y cedan información crítica para el negocio. Una adecuada política de formación y detección de correos sospechosos puede reducir considerablemente este tipo de incidentes (BBVA, 2023)

Malware o Programas Maliciosos

El malware comprende una amplia gama de programas diseñados para infiltrarse en los sistemas sin autorización, desde virus y troyanos hasta spyware y gusanos, en Colombia, las PYMES suelen ser víctimas de malware distribuido a través de dispositivos externos infectados o de enlaces en correos electrónicos que aparentan ser legítimos; además de robar información financiera y datos personales. los atacantes utilizan los recursos de cómputo de estas empresas para lanzar ataques a terceros, exponiendo a las organizaciones a sanciones o pérdidas de credibilidad. el uso de soluciones antimalware actualizadas y políticas de seguridad en la manipulación de archivos externos constituye una práctica necesaria para mitigar este riesgo (Py, 2024)

Amenaza

Una amenaza en el ámbito de la ciberseguridad se refiere a cualquier evento con la capacidad de generar un impacto negativo sobre la operación o los activos de una organización; para las PYMES colombianas, las amenazas más frecuentes provienen del acceso no autorizado, la modificación o destrucción de datos y la denegación de servicios digitales; estas acciones pueden ocasionar desde interrupciones operativas hasta sanciones legales por

incumplimiento en la protección de la información. la identificación temprana de las amenazas y su clasificación en función del riesgo se convierte en una práctica indispensable para estas empresas, ya que les permite priorizar recursos y esfuerzos de protección (Hernandez, 2022)

Vulnerabilidad

Las vulnerabilidades son deficiencias en sistemas, aplicaciones o procesos internos que permiten la explotación por parte de agentes maliciosos. en el caso de las PYMES colombianas, suelen estar asociadas con software desactualizado, contraseñas débiles o ausencia de protocolos de respaldo de información. Estas debilidades, aunque en apariencia menores, constituyen la puerta de entrada para ataques que afectan seriamente la operatividad empresarial; es fundamental distinguir que mientras las amenazas representan la posibilidad de un daño, las vulnerabilidades son las condiciones que permiten que dicho daño se materialice. por ello, la gestión de vulnerabilidades incluyendo su identificación, priorización y mitigación deben integrarse a las políticas de seguridad informática de toda organización (Riveros, 2020)

Vectores de Ataque

Los vectores de ataque son las rutas utilizadas por los ciberdelincuentes para explotar vulnerabilidades e irrumpir en los sistemas; en el contexto colombiano, los más frecuentes en las PYMES incluyen el phishing, los ataques de ransomware y las denegaciones de servicio; estos vectores no solo buscan la obtención de información valiosa, sino también la interrupción de la continuidad operativa y el debilitamiento de la confianza empresarial. el incremento de la digitalización en áreas como facturación electrónica, comercio en línea y servicios de banca digital ha ampliado la superficie de ataque, han obligado a las PYMES a diseñar protocolos de respuesta específicos frente a cada vector (López, 2023)

Pymes

Las pequeñas y medianas empresas representan la columna vertebral de la economía colombiana. Según cifras oficiales, constituyen el 99,5 % de las unidades empresariales formales y generan cerca del 40 % del Producto Interno Bruto. Su clasificación en

micro, pequeñas y medianas empresas está regulada por la Ley 590 de 2000 (BBVA, 2024), la cual establece parámetros relacionados con el número de trabajadores y el nivel de activos; pese a su importancia económica, estas organizaciones enfrentan limitaciones financieras y tecnológicas que reducen su capacidad de invertir en infraestructura de ciberseguridad. en consecuencia, su exposición a ataques es elevada, el fortalecimiento de la seguridad informática en este sector no solo contribuye a proteger los recursos tecnológicos, sino que además se traduce en un factor de competitividad en mercados nacionales e internacionales (Riva, 2020)

Marco Teórico

Antecedentes Internacionales

"En un contexto donde la digitalización avanza sin pausa, las pequeñas y medianas empresas en España enfrentan una serie de preocupaciones significativas en cuanto a seguridad cibernética. En los últimos años España ha registrado un aumento significativo en el número de ciberataques- Según informes, el 60% de las empresas españolas han sido víctimas de algún ataque. Además, los costos relacionados con la recuperación de datos y sistemas después de un ciberataque pueden ser muy elevados. Según (Calvo, 2023) un informe independiente del Observatorio de Digitalización de Go Daddy 2023, en colaboración con Advenís, las principales inquietudes de las pymes españolas en este ámbito son las siguientes: Exposición de los datos de los clientes (53 %). Pérdida de tiempo en la resolución de problemas (51 %). Pérdida de confianza por parte de los clientes (48 %). Pérdidas económicas (47 %). Indisponibilidad del sitio web durante un tiempo (46 %) Estas preocupaciones subrayan la importancia de mejorar y anticiparse a los riesgos asociados con la seguridad cibernética. La reputación de la empresa y la continuidad del negocio están en juego, por lo que es esencial contar con medidas preventivas sólidas y soluciones adecuadas". (Barcelona, 2024)

El Panorama de Amenazas de Kaspersky (que analizó datos de enero a agosto de 2021 y el mismo periodo de 2022), reveló que, en 2022, se bloquearon 2,366 ataques de malware y 110 mensajes fraudulentos (*phishing*) por minuto en América Latina. Los resultados también indican que la región se ha convertido en un importante centro de amenazas financieras a nivel mundial y que el uso de la piratería ha vuelto a ser uno de los principales vectores de infección. De acuerdo con el estudio, los ciberataques en la región han variado mucho durante la pandemia. Entre enero y septiembre de 2020, se produjo un aumento de 64% en el bloqueo de ataques con malware. Le

siguió un descenso del 39% entre septiembre de 2020 y enero de 2022, cuando la actividad maliciosa volvió a los niveles previos a la pandemia. Sin embargo, entre enero y mayo de este año, se registró un aumento del 30%. Considerando los primeros ocho meses de 2022, registramos un total de 817 millones de intentos de ataques en América Latina, lo que representa 2,366 bloqueos por minuto" (kaspersky, 2022)

Antecedentes Nacionales

"En el año 2021 se registraron más de 41 billones de intentos de ciberataques en el mundo, de los cuales aproximadamente siete billones tuvieron como destino a Colombia; este panorama refleja cómo los delitos informáticos se han convertido en una actividad cada vez más lucrativa para los atacantes; de acuerdo con la Fiscalía General de la Nación, el número de incidentes en el país creció un 30 % con respecto al año 2020, lo que demuestra una tendencia ascendente en la frecuencia y sofisticación de las amenazas digitales; ahora bien, aunque tanto entidades públicas como privadas han impulsado iniciativas para reforzar sus medidas de seguridad, estas aún resultan insuficientes; en consecuencia, situaciones como el secuestro de información, los ataques de ransomware o las vulneraciones de día cero continúan presentándose y ocasionan pérdidas económicas considerables, ya que numerosas organizaciones han tenido que efectuar pagos de rescate para recuperar datos críticos". (Guzmán, 2022)

Por otra parte, en el contexto colombiano se han evidenciado varios casos que ilustran con claridad la magnitud del problema; en diciembre de 2022, Empresas Públicas de Medellín (EPM) reportó un ataque que afectó su plataforma tecnológica y, con ello, la prestación de los servicios de energía y agua en diferentes territorios. Asimismo, en noviembre de 2022, el Grupo Keralty (Sanitas) denunció una intrusión que comprometió la información personal de más de 241.000 usuarios; más adelante, en mayo de 2023, la plataforma SECOP II, esencial para los

procesos de contratación pública, estuvo inactiva por más de 30 horas, lo que generó un impacto directo en operaciones estatales de gran relevancia (Renata, 2023)

De esta manera, los antecedentes muestran que los ciberataques no se circunscriben a corporaciones multinacionales, sino que también alcanzan a empresas nacionales, incluidas las pequeñas y medianas (PYMES), que representan la mayor parte del tejido productivo colombiano; para este sector, las consecuencias de un ataque van más allá de la pérdida de información, ya que también generan interrupciones en la continuidad de los servicios, pérdida de confianza por parte de clientes y aliados estratégicos, sanciones legales, y en casos extremos la imposibilidad de mantener las operaciones comerciales.

En este sentido, resulta evidente que las PYMES colombianas enfrentan un doble desafío: limitar sus vulnerabilidades a pesar de sus limitados recursos financieros y, al mismo tiempo, incrementar sus capacidades de defensa en un entorno digital cada vez más hostil a diferencia de las grandes corporaciones que cuentan con infraestructura avanzada y equipos especializados en seguridad informática. las PYMES suelen carecer de personal capacitado, herramientas de protección y políticas claras en ciberseguridad, por consiguiente, los incidentes de EPM, Grupo Keralty y SECOP II no solo representan ejemplos aislados, sino también advertencias sobre los riesgos latentes que afectan a organizaciones de todo tamaño y sector.

En consecuencia, se hace necesario reconocer que el panorama nacional exige medidas concretas y diferenciadas para las PYMES, por un lado, la adopción de herramientas tecnológicas de bajo costo y código abierto constituye una alternativa viable para mitigar riesgos; por otro lado, la capacitación continua del talento humano permite que los empleados identifiquen intentos de fraude, correos fraudulentos o actividades sospechosas, reduciendo así la superficie de exposición de las empresas; además, la creación de una cultura organizacional en

torno a la seguridad digital que contribuya a que las PYMES no solo respondan de manera reactiva a los ataques, sino que también anticipen las amenazas antes de que comprometan sus activos más valiosos.

Finalmente, al considerar la relevancia de las PYMES dentro de la economía colombiana, resulta indispensable comprender que la protección de este sector no debe limitarse a iniciativas aisladas de carácter empresarial, por el contrario, es necesario articular esfuerzos entre el Estado, los gremios y las compañías proveedoras de servicios tecnológicos para garantizar un entorno de seguridad digital que favorezca la sostenibilidad de estas organizaciones, de lo contrario, la exposición creciente a la ciberdelincuencia seguirá escalando, incrementando el riesgo de interrupción de operaciones y debilitando la competitividad del sector en un mercado cada vez más digitalizado.

Marco Legal

El ecosistema digital en Colombia ha evolucionado con rapidez, transformando la manera en que las organizaciones interactúan con clientes, proveedores y entidades estatales, este proceso, aunque beneficioso, también ha incrementado la exposición a riesgos relacionados con la seguridad de la información; las pequeñas y medianas empresas (PYMES), que representan la mayor parte del tejido empresarial del país, suelen enfrentar limitaciones de recursos económicos y tecnológicos, lo que las convierte en actores especialmente vulnerables frente a delitos informáticos, robo de datos y fraudes electrónicos.

En este escenario, el marco legal colombiano y las referencias internacionales resultan esenciales para estructurar políticas de prevención y respuesta; a continuación, se presentan los principales instrumentos legales y normativos, organizados en tablas con explicación previa para facilitar su comprensión y aplicación en el contexto de las PYMES.

Ley 1273 de 2009 de Delitos informáticos, es considerada el punto de partida para la protección penal de la información y los datos en Colombia. Su importancia radica en que tipificó de manera clara conductas asociadas al uso indebido de sistemas informáticos y redes de comunicación, estableciendo sanciones de carácter punitivo; en el caso de las PYMES, esta normativa actúa como un llamado a la implementación de controles técnicos y organizativos que eviten incidentes de seguridad, ya que las sanciones previstas incluyen tanto multas como penas privativas de la libertad; la ley no solo busca castigar al infractor, sino también generar un marco de prevención que impulse a las empresas a proteger sus activos digitales.

Tabla 1

Artículos Principales De La Ley 1273 De 2009

Artículo	Conducta tipificada	Descripción y sanción
269A	Acceso abusivo	Ingreso total o parcial a un sistema informático sin autorización o fuera de lo pactado. Pena: prisión de 48 a 96 meses y multa de 100 a 1.000 SMLMV.
269B	Obstaculización ilegítima	Impedir, obstaculizar o afectar el funcionamiento normal de un sistema informático, sus datos o una red de telecomunicaciones. Pena: prisión de 48 a 96 meses y multa de 100 a 1.000 SMLMV.
269C	Interceptación de datos	Interceptar datos informáticos en su origen, tránsito o destino sin orden judicial, incluyendo emisiones electromagnéticas. Pena: prisión de 36 a 72 meses.
269D	Daño informático	Alterar, borrar, destruir o deteriorar datos y sistemas de tratamiento de información. Pena: prisión de 48 a 96 meses y multa de 100 a 1.000 SMLMV.
Uso de software malicioso	269I	Hurto por medios informáticos
	269J	Transferencia no consentida
Violación de datos personales		
Suplantación de sitios web		

Producir, traficar, distribuir o introducir malware dentro o fuera del territorio nacional. Pena: prisión de 48 a 96 meses y multa de 100 a 1.000 SMLMV.	Crear o difundir páginas electrónicas fraudulentas con fines ilícitos. Pena: prisión de 48 a 96 meses y multa de 100 a 1.000 SMLMV. Manipular sistemas o redes electrónicas para sustraer recursos. Pena: según artículo 240 del Código Penal.
Obtener, divulgar, modificar o vender datos personales sin autorización legítima. Pena: prisión de 48 a 96 meses y multa de 100 a 1.000 SMLMV.	Obtener transferencias ilícitas de activos mediante fraude informático. Pena: prisión de 48 a 120 meses y multa de 200 a 1.500 SMLMV.

*Nota***.** Ley de delitos informáticos. Adaptado de. Ley 1273 De 2009, diario oficial 47.223, 5 De enero De 2009. República De Colombia. https://normograma.dian.gov.co/dian/compilacion/docs/ley_1273_2009.htm

Conpes 3701 de 2011, Política Nacional de Ciberseguridad y Ciberdefensa

constituye la base de la política pública en ciberseguridad y ciberdefensa en Colombia; este documento, elaborado por el Departamento Nacional de Planeación, reconoce que las amenazas digitales no solo afectan a las instituciones públicas, sino también al sector privado, incluyendo a las PYMES; su importancia radica en que establece lineamientos estratégicos para fortalecer las capacidades del Estado y fomentar la colaboración con empresas privadas en la gestión de incidentes.

Las PYMES encuentran en este plan una oportunidad para acceder a programas de capacitación, utilizar canales oficiales para denunciar incidentes y alinearse con prácticas de seguridad reconocidas a nivel nacional e internacional.

Tabla 2

Lineamientos Principales Del Conpes 3701 De 2011

Objetivo	Medida definida	Relevancia para PYMES
Prevención y control	Creación del colCERT (Grupo de Respuesta a Emergencias Cibernéticas)	Permite a las PYMES reportar incidentes y recibir apoyo especializado en la gestión de ataques cibernéticos.
Coordinación interinstitucional	Comisión Intersectorial de Ciberseguridad	Ofrece un canal de articulación entre el sector público y privado, donde las PYMES pueden participar en iniciativas conjuntas.
Capacitación en ciberseguridad	Programas de formación	Integración de legislación	Ajuste y fortalecimiento normativo

Brinda acceso a entrenamientos para mejorar las capacidades técnicas de las PYMES frente a riesgos cibernéticos. Genera un marco regulatorio	actualizado que impacta directamente en las políticas empresariales de protección de datos.

*Nota***.** Documento conpes 3701. Adaptado de. consejo nacional de política económica y social conpes *3701,* lineamientos de política para ciberseguridad y ciberdefensa. Republica Colombia. (2011). https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Además de la Ley 1273 y del Conpes 3701, el país ha emitido un conjunto de normas que refuerzan la protección de datos personales y la seguridad en el sector privado, estas disposiciones son de carácter obligatorio y afectan directamente la manera en que las empresas, sin importar su tamaño, deben gestionar la información sensible de sus clientes, proveedores y empleados.

Para las PYMES, estas normas implican el diseño de políticas de privacidad, el registro de bases de datos ante la Superintendencia de Industria y Comercio y la adopción de medidas preventivas que reduzcan la exposición a incidentes de seguridad.

Tabla 3

Normativa Complementaria Nacional

Norma	Contenido principal	Impacto en PYMES
Ley 1581 de 2012	Establece el régimen general de protección de datos personales.	Obliga a las PYMES a crear políticas de privacidad y cumplir con el registro de bases de datos ante la SIC.
Decreto 1377 de 2013	Reglamenta la Ley 1581 sobre autorización y tratamiento de datos.	Define los mecanismos para que las PYMES soliciten autorización a titulares de datos y manejen su información conforme a la ley.
Decreto 620 de 2020	Lineamientos de seguridad de la información en el sector privado.	Obliga a implementar medidas técnicas y administrativas mínimas para resguardar la información en procesos tecnológicos.

*Nota***.** Decreto 620 de 2020. Tomado de. Ministerio de Tecnologías de la Información y las Comunicaciones. Mintic (2020).

https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=118337

Si bien en Colombia las normas nacionales tienen carácter obligatorio, existen marcos de referencia internacionales que han sido adoptados de manera voluntaria por muchas empresas, incluidas las PYMES; estos estándares proporcionan metodologías claras y guías prácticas para la gestión de riesgos de ciberseguridad, la gobernanza tecnológica y la implementación de controles de protección; en el caso de las PYMES colombianas, la adopción parcial o total de estas

metodologías permite mejorar la gestión interna, elevar el nivel de seguridad digital y, en muchos casos, ganar la confianza de clientes internacionales que exigen certificaciones como la ISO 27001.

Tabla 4

Marcos De Referencia Internacionales En Ciberseguridad

Referencia	Propósito	Uso recomendado para PYMES
NIST Cybersecurity Framework	Ayuda a gestionar y reducir riesgos de ciberseguridad mediante cinco funciones: identificar, proteger, detectar, responder y recuperar.	Guía práctica para priorizar inversiones en seguridad según recursos disponibles.
Enfocado en gobernanza de TI y control de procesos tecnológicos.		Recomendado para PYMES que desean profesionalizar su gestión y alinear la TI con objetivos de negocio.
ISO/IEC 27001 de	Norma internacional para sistemas	Permite certificaciones que generan confianza en clientes, especialmente en mercados internacionales.
gestión de seguridad de la información.		Facilita la mejora de operaciones tecnológicas y soporte al cliente.
Marco de gestión de servicios de TI basado en buenas prácticas.		Proporciona un enfoque estructurado para evaluar vulnerabilidades y
Metodología para análisis y gestión de riesgos tecnológicos.		priorizar medidas de seguridad.

*Nota***.** Marcos internacionales de ciberseguridad y seguridad informática. Adaptado de. National Institute of Standards and Technology. Nist. (2013). https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf *;* Un marco para la alineación y la

gobernanza. White, Sarah. *(2023).* https://www.cio.com/article/228151/what-is-cobit-a-framework-for-alignment-and-governance.html ; Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología Magerit. Gómez, Enrique. (2019). https://www.revistas.upse.edu.ec/index.php/rctu/article/view/429/348 *;* International Organization for Standardization. Iso. (2022*).* https://cdn.standards.iteh.ai/samples/82875/726bcf58250e43d9a666b4d929c8fbdb/ISO-IEC- 27001-2022.pdf *;* Optimización de los procesos de mesa de ayuda: Un enfoque desde ITIL Paredes, Marco. (2018). https://www.revistaespacios.com/a18v39n51/a18v39n51p20.pdf

Además de las normas nacionales e internacionales, existen guías prácticas diseñadas específicamente para pequeños negocios, estas recomendaciones destacan medidas preventivas que no requieren grandes inversiones, pero que tienen un impacto significativo en la reducción de riesgos digitales; para las PYMES colombianas, la aplicación de estas prácticas es fundamental, ya que constituyen el primer nivel de defensa contra amenazas comunes como el phishing, el ransomware o la pérdida de información por falta de respaldo.

Tabla 5

Medidas Recomendadas De Ciberseguridad Para PYMES

Medida	Aplicación práctica
Actualización de software	Mantener sistemas operativos, aplicaciones y navegadores actualizados con parches de seguridad.
Generar respaldos periódicos en la nube o en dispositivos externos almacenados en lugares seguros.	
Cifrado de dispositivos	Proteger con encriptación computadoras, tablets, teléfonos inteligentes y discos externos.
Contraseñas seguras y MFA	Establecer contraseñas robustas y habilitar autenticación multifactor en sistemas críticos.
Wi-Fi	Configurar redes inalámbricas con protocolos WPA2 o WPA3 y cambiar credenciales por defecto.
Capacitación del personal	Realizar entrenamientos periódicos sobre ciberseguridad y detección de fraudes.
Plan de respuesta a incidentes	Establecer protocolos de acción frente a ataques, con roles definidos y comunicación hacia clientes.

*Nota***.** Small Business Cybersecurity Guide. Adapdato de. National Institute of Standards and Technology. Nist. (2013). https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf

Marco Contextual

"La Ley 590 de 2000 establece la clasificación de las micro, pequeñas y medianas empresas en Colombia, define a la pyme como toda unidad de explotación económica, gestionada por persona natural o jurídica, en actividades industriales, agropecuarias, comerciales o de servicios, tanto en áreas rurales como urbanas; la clasificación se determina a partir de dos parámetros: el número de trabajadores y el valor de los activos; una mediana empresa emplea entre cincuenta y uno (51) y doscientos (200) trabajadores, con activos totales entre 5.001 y 15.000 salarios mínimos mensuales legales vigentes (SMMLV); la pequeña empresa se caracteriza por una planta laboral de entre once (11) y cincuenta (50) trabajadores, y activos totales entre 501 y 5.000 SMMLV. Finalmente, la microempresa se define por contar con un máximo de diez (10) empleados y activos inferiores a 501 SMMLV; la ley añade que, en casos de combinaciones de parámetros, prevalece el criterio de los activos como factor de clasificación. Además, extiende los beneficios y programas establecidos a los artesanos colombianos y contempla disposiciones de equidad de género en el marco del Plan Nacional de Igualdad de Oportunidades para la Mujer". (congreso de colombia, 2000)

El peso de este sector en la estructura empresarial es significativo. Según cifras de Confecámaras, en 2022 existían 1,7 millones de empresas formales activas, de las cuales el 99,5% correspondían a mipymes; de este universo, el 92% eran microempresas, el 5,9% pequeñas, el 1,6% medianas y apenas el 0,5% grandes. Por su parte, el Directorio de Estadísticas de Empresas (DEE) del DANE estimó en 2021 un total de 5,7 millones de unidades productivas, incluyendo informales, lo que refleja que gran parte de la actividad empresarial nacional se concentra en el estrato microempresarial; el aporte económico de este segmento se aproxima al

40% del Producto Interno Bruto, consolidándolo como un pilar de la economía colombiana (BBVA, 2024)

Figura 1

El Universo Mipyme

Nota. Mirada a las Mipymes en Colombia. Tomado de. Bbvaresearch. González, juan. (2024). https://www.bbvaresearch.com/wp-content/uploads/2024/02/202401_MiPymes_Colombia-1.pdf

El crecimiento de las mipymes ha generado impactos sostenidos en la generación de empleo, el desarrollo de nuevos mercados y la dinamización de la economía regional; no obstante, este mismo crecimiento las expone a vulnerabilidades específicas en el entorno digital. en los últimos años, se ha evidenciado que el sector es un objetivo recurrente de ataques informáticos debido a su limitado conocimiento en ciberseguridad y a la fragilidad de sus infraestructuras tecnológicas. en Colombia los ciberataques contra pymes no solo se traducen en pérdidas económicas y sanciones legales, sino también en afectaciones a la confianza de clientes y proveedores, lo que compromete la

continuidad de las operaciones.

La realidad colombiana muestra que, mientras las pymes son responsables de gran parte de la generación de empleo y de la competitividad en mercados emergentes, también enfrentan riesgos tecnológicos que amenazan su sostenibilidad. el desafío se centra en la adopción de prácticas de seguridad digital y en el fortalecimiento de capacidades técnicas que permitan consolidar este sector más resiliente frente a las dinámicas del cibercrimen.

Principales Vectores de Ataques de Ciberseguridad en las Pymes Vectores de Ataque en las Pymes

Los vectores de ataque constituyen las técnicas utilizadas por los ciberdelincuentes para explotar debilidades en los sistemas informáticos de las pequeñas y medianas empresas, (Cilleruelo, 2024) explica que dichos vectores representan rutas de intrusión que buscan comprometer la confidencialidad, integridad y disponibilidad de los recursos digitales. en el caso colombiano, la situación es especialmente sensible, ya que muchas pymes no cuentan con infraestructura tecnológica especializada ni con equipos dedicados a la seguridad de la información, lo que incrementa la probabilidad de incidentes que comprometan la operación diaria.

El Conpes 3701 de 2011 ya advertía que este tipo de organizaciones presentaban una vulnerabilidad significativa en materia de seguridad digital, debido a la escasa inversión y al bajo nivel de madurez en prácticas de gestión de riesgos. esta condición convierte a las pymes en objetivos prioritarios para los atacantes, quienes aprovechan las brechas de seguridad para ejecutar campañas masivas de fraude, extorsión o robo de información sensible, la identificación de estos vectores resulta indispensable para desarrollar mecanismos de defensa adaptados a las condiciones económicas y técnicas del contexto colombiano (conpes, 2011)

Ataques de Phishing

El phishing es una técnica de suplantación que consiste en enviar correos electrónicos o mensajes fraudulentos con apariencia legítima para obtener credenciales o datos financieros. (By Sosmatic, 2023) describe que los atacantes inducen a las víctimas a hacer clic en enlaces manipulados o a descargar archivos contaminados, aprovechando la confianza en entidades conocidas; una modalidad frecuente es el *Business Email Compromise*, en la que se suplanta a

directivos de alto nivel con el fin de ordenar transferencias no autorizadas o manipular transacciones comerciales; este vector afecta de forma particular a las pymes colombianas, que dependen del correo electrónico como principal canal de comunicación con clientes y proveedores.

La Ley 1581 de 2012 obliga a las empresas en Colombia a implementar medidas de seguridad para proteger los datos personales, y la Superintendencia de Industria y Comercio ha sancionado a organizaciones que no lograron prevenir filtraciones ocasionadas por campañas de phishing; el impacto de este ataque no se limita al robo de información, sino que también compromete la continuidad operativa y genera desconfianza en el mercado; en sectores como el comercio y los servicios profesionales, donde las pymes constituyen la mayoría de los actores económicos, el phishing se convierte en un riesgo recurrente que puede poner en riesgo la estabilidad financiera y la reputación empresarial

Ataques de Ransomware

El ransomware se manifiesta como un código malicioso que cifra los archivos corporativos y exige un rescate económico a cambio de su liberación. (Jaimovich, 2024) explica que este vector se propaga a través de adjuntos maliciosos, enlaces fraudulentos o vulnerabilidades no parcheadas. En Colombia, el *Centro Cibernético de la Policía Nacional* reportó un incremento en incidentes de este tipo durante 2023, destacando que gran parte de las víctimas fueron pymes sin esquemas de respaldo confiables ni políticas de recuperación ante desastres; la consecuencia inmediata es la paralización de procesos como facturación, gestión de inventarios o atención a clientes.

El *Conpes 3995 de 2020* advierte que este tipo de ataques tiene un alto impacto económico en las empresas de menor tamaño, dado que carecen de los recursos necesarios para

pagar rescates o para restaurar sistemas mediante procesos forenses. Además, las interrupciones prolongadas pueden conducir al incumplimiento de obligaciones tributarias o contractuales, exponiendo a las organizaciones a sanciones adicionales; este panorama evidencia la necesidad de que las pymes colombianas desarrollen planes de continuidad de negocio y refuercen la cultura de seguridad digital entre sus empleados.

Ataques con Malware

El malware agrupa diversas formas de software malicioso, como virus, troyanos o spyware, diseñados para infiltrarse en sistemas con el fin de robar información o alterar su funcionamiento. (Trevino, 2024) sostiene que la instalación de malware ocurre mediante vulnerabilidades sin parchear, dispositivos externos contaminados o técnicas de ingeniería social; en Colombia, la Cámara Colombiana de Informática y Telecomunicaciones ha indicado que más del 60 % de los incidentes reportados en pymes involucran algún tipo de malware, lo que pone en riesgo bases de datos de clientes y transacciones financieras.

El *Conpes 3995 de 2020* recomienda la adopción de controles mínimos de protección, como el uso de antivirus actualizados y la aplicación regular de parches de seguridad; sin embargo, la limitada inversión tecnológica en pymes dificulta la implementación de estas medidas. en muchos casos, los ataques de malware se traducen en pérdida de información sensible, espionaje industrial o incluso utilización de la infraestructura de la empresa como plataforma para nuevos ataques, ampliando así las consecuencias más allá de la propia organización.

Ataques de Denegación de Servicio (DDoS)

Un ataque de denegación de servicio distribuido busca saturar un servidor o una aplicación con solicitudes masivas hasta agotar sus recursos y dejarla inoperante. (Security, 2022) documenta que este vector se ha convertido en una herramienta recurrente para interrumpir la disponibilidad de portales empresariales; en Colombia, ColCERT ha señalado que varias pymes con presencia en comercio electrónico han reportado interrupciones relacionadas con ataques DDoS, lo que les ha impedido procesar pagos o atender solicitudes en línea.

Para empresas pequeñas que dependen de la venta digital como fuente principal de ingresos, la indisponibilidad temporal puede tener consecuencias significativas; además de las pérdidas económicas directas, se genera un impacto reputacional que afecta la fidelización de los clientes; en este contexto, las pymes colombianas deben implementar medidas de mitigación como el uso de servicios de protección en la nube y el monitoreo constante del tráfico de red, tal como recomiendan los lineamientos nacionales en ciberseguridad.

Ataques de Intermediario (MITM)

El ataque de intermediario consiste en la interceptación de comunicaciones entre dos partes para acceder a datos sensibles sin que los involucrados lo perciban. (Gregg Lindemulder, 2024) señala que este vector permite robar credenciales, información financiera o datos de autenticación; en Colombia, donde el uso de redes Wi-Fi públicas es común para reducir costos de conectividad, las pymes se exponen con frecuencia a este tipo de amenazas; la vulneración de correos corporativos o plataformas de banca en línea constituye un riesgo recurrente que puede derivar en fraudes financieros de alto impacto.

El *Conpes 3995 de 2020* subraya la importancia de implementar protocolos de cifrado en las comunicaciones y de fomentar la cultura de seguridad digital en las organizaciones; la *Ley*

1581 de 2012 refuerza esta necesidad al exigir medidas adecuadas para la protección de datos personales, lo que obliga a las empresas a garantizar que la información de clientes y proveedores se transmita de forma segura; la falta de estas medidas no solo expone a las pymes a pérdidas económicas, sino también a sanciones legales por negligencia en la gestión de información sensible

Ataques de Fuerza Bruta

Los ataques de fuerza bruta se basan en la generación automática de múltiples combinaciones de contraseñas hasta descubrir la correcta. (López, 2023) explica que esta técnica resulta eficaz cuando los usuarios utilizan credenciales débiles o repetidas, lo que permite a los atacantes comprometer servicios críticos; en Colombia, el *Centro Cibernético de la Policía Nacional* ha identificado un aumento en reportes de accesos no autorizados a sistemas de pymes debido al uso de contraseñas poco seguras, principalmente en portales de acceso remoto y sistemas de facturación electrónica.

El impacto de este vector se amplifica en organizaciones que no cuentan con autenticación multifactor ni con políticas de renovación periódica de contraseñas; además de comprometer aplicaciones críticas como la contabilidad o la gestión de nómina, estos ataques pueden derivar en la manipulación de registros financieros, lo que expone a las empresas a incumplimientos frente a la DIAN; la adopción de mecanismos de autenticación avanzada se presenta como una necesidad urgente para mitigar este riesgo en el entorno colombiano.

Ataques de Inyección SQL

La inyección SQL ocurre cuando un atacante introduce comandos maliciosos en formularios de aplicaciones web que interactúan con bases de datos. (Fortinet Inc, 2024) explica

que este vector permite visualizar, modificar o eliminar información sensible de los sistemas comprometidos; en Colombia, muchas pymes utilizan aplicaciones de gestión en línea para manejar inventarios, clientes y proveedores, lo que las convierte en un objetivo recurrente de este tipo de ataque; la explotación exitosa compromete directamente la confidencialidad de los datos y afecta la integridad de las operaciones.

La *Ley 1273 de 2009* tipifica como delito el acceso abusivo a sistemas informáticos, y la Superintendencia de Industria y Comercio sanciona a las organizaciones que no aplican medidas mínimas de seguridad en sus plataformas; la inyección SQL no solo implica pérdidas técnicas, sino también la posibilidad de sanciones económicas por la exposición de datos personales protegidos por la *Ley 1581 de 2012*; esto refuerza la necesidad de que las pymes colombianas fortalezcan la validación de entradas en sus aplicaciones y desarrollen prácticas de pruebas de penetración periódicas (Colombia, 2009)

Ataques de Día Cero

Los ataques de día cero se caracterizan por explotar vulnerabilidades desconocidas para las cuales aún no existe parche disponible. (Jaimovich, 2024) señala que este tipo de incidentes resulta particularmente peligroso porque se ejecutan en el lapso en que el fabricante no ha publicado una solución; en Colombia, ColCERT ha advertido que las pymes suelen tardar semanas en aplicar actualizaciones, lo que amplía la ventana de exposición a este tipo de amenazas; esta demora se debe, en gran parte, a la carencia de equipos de monitoreo avanzado y a la dependencia de proveedores externos.

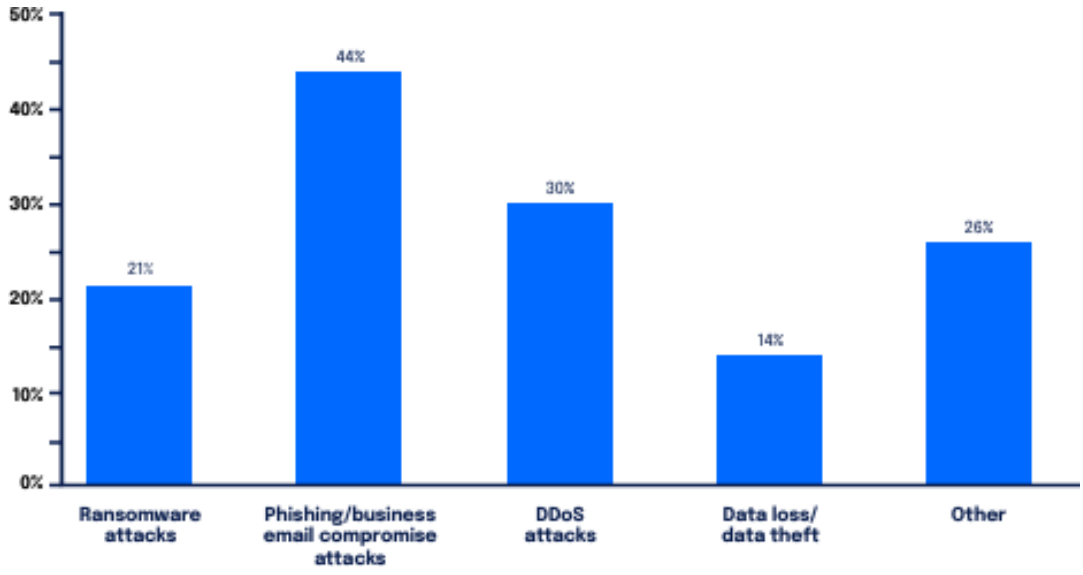
El resultado de un ataque de día cero puede incluir la instalación de puertas traseras, accesos remotos encubiertos o interrupciones en servicios críticos; la falta de detección temprana aumenta el riesgo de que los atacantes mantengan control persistente sobre la infraestructura; el

Conpes 3995 de 2020 recomienda la implementación de procesos de gestión de vulnerabilidades y actualizaciones proactivas, lo que obliga a las pymes colombianas a desarrollar planes internos de revisión periódica de parches y a establecer acuerdos de soporte con proveedores que les permitan reducir la exposición frente a este vector

En base a las consideraciones anteriores, según (DigitalOcean, 2023) los principales vectores de ataque que experimentaron las pymes en el año 2023 con la encuesta realizada a 550 pymes por la compañía por la compañía Digital Ocean.

Figura 2

Vectores Ataque Experimentaron Las Pymes En El Año 2023



Nota. How startups and SMBs are viewing security threats in 2023. Tomado de. Small businesses and cybersecurity. digitalocean. (2023). https://anchor.digitalocean.com/rs/113-DTN-266/images/Security-Report_DigitalOcean.pdf?mkt_tok=MTEzLURUTi0yNjYAAAGKx5z_ZPYAC-86Rzqj2H8M5CcpHbripszTaynvLi2kXVlcELdKklw7mS0mGPb8wSRtXMcKXZ4Jj6Ji8

Tal como se observa en la **Figura 2**, el vector de ataque más recurrente reportado por las pymes durante 2023 corresponde al *phishing* y al compromiso del correo electrónico corporativo, con un 44 % de incidencia, seguido por los ataques de denegación de servicio distribuido (DDoS) con un 30 %, el ransomware con un 21 % y otras modalidades con un 26 %. Estas cifras confirman que el phishing continúa siendo el vector predominante a nivel internacional.

En Colombia, el Ministerio de Tecnologías de la Información y las Comunicaciones publicó en 2023 que las pymes de sectores comercio y servicios fueron las más afectadas por phishing y ransomware, lo que coincide con las tendencias globales. estos resultados reflejan la prevalencia de técnicas dirigidas a la manipulación de usuarios mediante correos electrónicos fraudulentos, así como la afectación de la disponibilidad de servicios críticos y el cifrado de información empresarial. la interpretación de estas cifras permite comprender que las pequeñas y medianas empresas son un objetivo constante de los atacantes, debido a su limitada capacidad de inversión en medidas de ciberseguridad y a la ausencia de políticas internas de protección de datos.

La realidad nacional refleja que la carencia de políticas de ciberseguridad y de inversiones en protección tecnológica incrementa la exposición a estos vectores, el desconocimiento de las amenazas y la baja implementación de medidas como autenticación multifactor o respaldos periódicos aumenta la vulnerabilidad. en este sentido, las recomendaciones del *Conpes 3995 de 2020* enfatizan la necesidad de generar capacidades internas de seguridad digital en las pymes colombianas, con el fin de garantizar continuidad operativa y proteger la información de clientes y proveedores frente a los riesgos descritos.

Ante este panorama, resulta indispensable que las pymes colombianas reconozcan los vectores de ataque a los que se encuentran expuestas y comprendan las consecuencias de no

implementar mecanismos de seguridad. un incidente de este tipo puede derivar en pérdidas económicas significativas, sanciones legales por incumplimiento de la *Ley 1581 de 2012* en materia de protección de datos personales, daños a la reputación organizacional e incluso la interrupción definitiva de las operaciones. la adopción de una cultura de ciberseguridad dentro de la organización constituye un factor esencial para garantizar la continuidad del negocio, ya que el conocimiento previo de los principales vectores de ataque facilita la puesta en marcha de controles técnicos, administrativos y legales acordes con el contexto empresarial colombiano

Con el fin de sintetizar los principales vectores de ataque y proporcionar una herramienta práctica de gestión para las pequeñas y medianas empresas en Colombia, se presenta a continuación unas señales de alerta en la operación, controles mínimos y recomendados, así como métricas sugeridas para evaluar la eficacia de las medidas de ciberseguridad.

Tabla 6

Matriz Operativa Para Priorización En Pymes

Vector	Señales en operación	Control mínimo	Control recomendado	Métrica sugerida
Phishing / BEC	correos con cambios de cuenta, dominios similares	MFA; SPF/DKIM/DMARC “quarantine”; bloqueo adjuntos	DMARC “reject”; verificación fuera de banda; playbook pagos	clics en simulación <5%; MFA ≥95%; reporte <15 min
Ransomware	cifrado súbito; notas de rescate	copias 3-2-1; parches críticos; segmentación básica	EDR/XDR; revisión RDP/VPN; privilegios mínimos	RTO <24 h; parches <7 d; endpoints con EDR
Malware	instaladores no verificados; macros	AV actualizado; restricción de ejecución	listas blancas; sandbox; DNS filtrado	detecciones/100 endpoints; firmas al día
DDoS	caídas de portal; picos anómalos	CDN; WAF; rate limiting	mitigación con ISP; geobloqueo	uptime; TPS en pico; eventos de mitigación
MITM	alertas de cert.; Wi-Fi abierta	TLS forzado; HSTS; VPN	DoH/DoT; cert. cliente; detección “evil twin”	% tráfico cifrado; incidentes por cert.

Fuerza bruta	intentos fallidos masivos	MFA; bloqueo por intentos; higiene de cuentas	passkeys; detección de anomalías; "password leak check"	bloqueos/h; MFA ≥95%
Inyección SQL	errores de BD; entradas no validadas	consultas preparadas; validación	WAF; SAST/DAST; pentesting	hallazgos críticos cerrados; tiempo de remediación
Día cero	avisos del fabricante; exploits emergentes	inventario; mitigaciones; segmentación	virtual patching; escaneo de exposición	tiempo de reacción; % activos inventariados

Nota. Tipos de ataques cibernéticos. Adaptado de. Buenas prácticas internacionales de seguridad de la información, incluyendo el National Institute of Standards and Technology Cybersecurity Framework. Nist csf. (2024). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf , la norma iso/iec 27001:2022. (2022). https://cdn.standards.iteh.ai/samples/82875/726bcf58250e43d9a666b4d929c8fbdb/ISO-IEC-27001-2022.pdf , lineamientos nacionales de ciberseguridad establecidos en el *Conpes 3995. (2020)*. https://colaboracion.dnp.gov.co/cdt/Conpes/Econ%C3%B3micos/3995.pdf

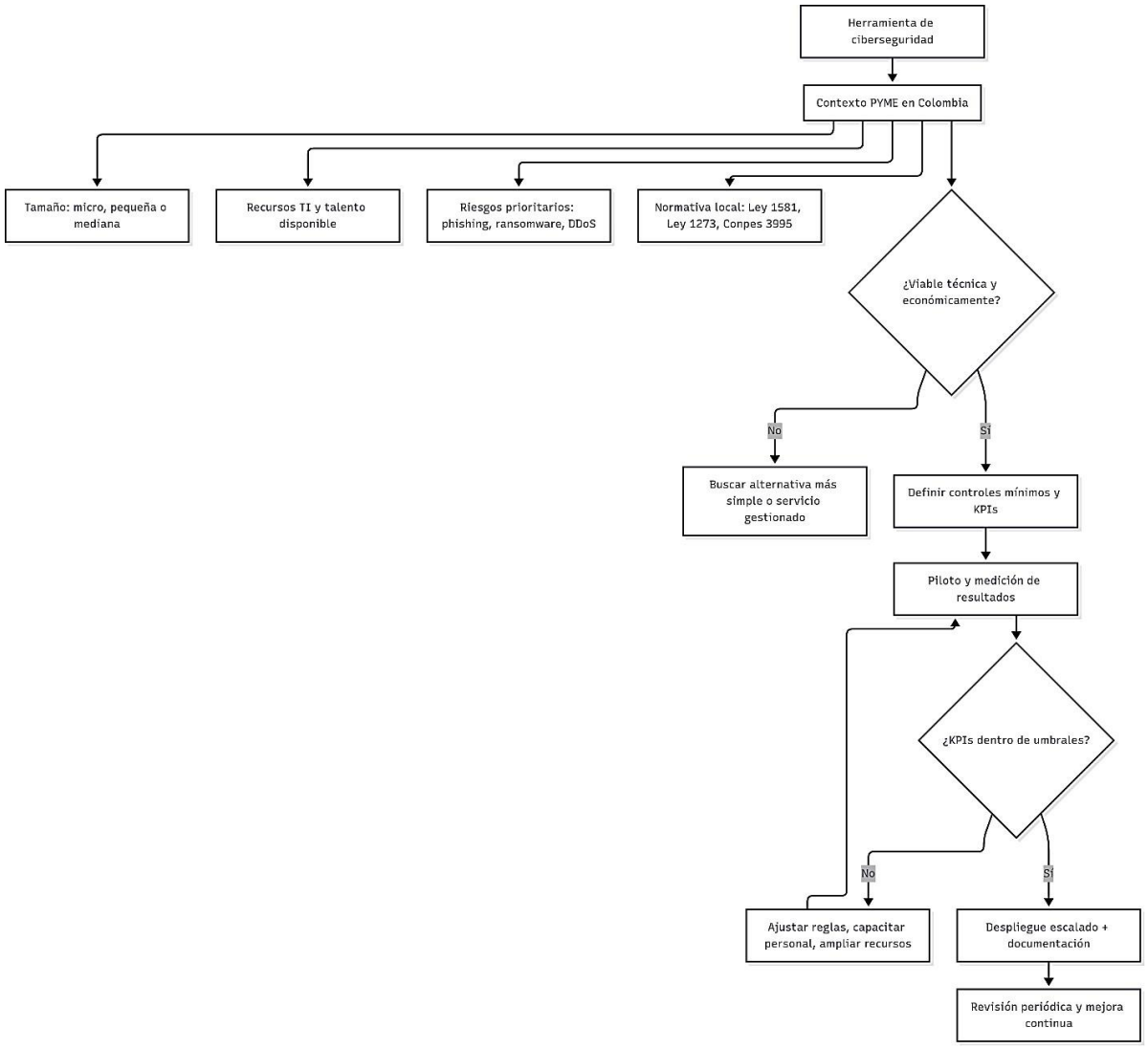
Ciberseguridad de Código Abierto (open source)

El software de código abierto, conocido como *open source*, se caracteriza por permitir el acceso al código fuente, lo que facilita su inspección, modificación y mejora por parte de cualquier desarrollador. Según (Zendesk, 2024)este tipo de programas se distinguen por su transparencia, la posibilidad de aplicar diferentes licencias y su capacidad de adaptación a otros productos, factores que han favorecido su crecimiento en los mercados globales. en el ámbito empresarial, las soluciones de código abierto han reducido costos significativos y han permitido que organizaciones pequeñas y medianas incorporen herramientas tecnológicas avanzadas a sus infraestructuras. para las pymes colombianas que enfrentan limitaciones presupuestales y de personal especializado, la adopción de este tipo de software representa una oportunidad estratégica para implementar medidas de ciberseguridad accesibles y escalables.

Como se observa en la **Figura 3**, el análisis crítico de herramientas de ciberseguridad en PYMES colombianas requiere integrar aspectos técnicos, económicos y normativos para garantizar una implementación efectiva en el contexto nacional.

Figura 3

Ciberseguridad en el Contexto de las PYMES Colombianas



Nota. El diagrama representa las etapas de evaluación crítica de una herramienta de ciberseguridad en pymes colombianas, incluyendo viabilidad técnica y económica, adecuación normativa (ley 1581 de 2012, https://esdegue.edu.co/sites/default/files/Normatividad/LEY%20TRATAMIENTO%20DE%20DA TOS%20-%20LEY%201581%20DE%202012.pdf , Ley 1273 De 2009. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492 y el ciclo de mejora continua. conpes 3995. (2020).https://colaboracion.dnp.gov.co/cdt/Conpes/Econ%C3%B3micos/3995.pdf

Herramientas Open Source (Código Abierto) Analizadas

PfSense. se ha consolidado como una alternativa de firewall de código abierto ampliamente utilizada, especialmente en pequeñas y medianas empresas que requieren soluciones de seguridad flexibles y asequibles. Su funcionamiento se basa en el sistema operativo FreeBSD, lo que le otorga escalabilidad y estabilidad en entornos corporativos. Entre sus principales aportes se destacan las políticas de filtrado de tráfico, el soporte para redes privadas virtuales (VPN) y la posibilidad de integrar funciones como servidores proxy, balanceo de carga y protección contra ataques distribuidos de denegación de servicio; estas características lo convierten en una opción versátil que puede adaptarse tanto a redes locales de menor escala como a infraestructuras más complejas (Pineda, 2023)

En el caso de las pymes colombianas, su carácter open source constituye una ventaja significativa, ya que elimina los costos de licenciamiento asociados a firewalls comerciales y permite reducir gastos sin sacrificar capacidades técnicas. Esto es especialmente relevante en organizaciones que enfrentan presupuestos restringidos, donde la personalización de la plataforma resulta clave para ajustar las reglas de seguridad a procesos tan diversos como la atención al cliente, las transacciones en línea o el trabajo remoto seguro. Sin embargo, esta misma flexibilidad viene acompañada de una limitación: la dependencia del soporte comunitario, que, si bien es activo y colaborativo, no garantiza tiempos de respuesta inmediatos en escenarios críticos. En Colombia, donde los ataques de ransomware y phishing contra pymes han aumentado de forma sostenida (MinTic, 2024) esta falta de respaldo formal puede convertirse en un factor de riesgo, sobre todo en regiones intermedias y rurales donde no siempre se cuenta con personal especializado en TI.

Así, aunque pfSense ofrece una plataforma robusta y adaptable que facilita a las pymes fortalecer su seguridad perimetral con una inversión mínima, su implementación exige una evaluación realista de las capacidades internas para gestionar incidentes. En ciudades como Bogotá o Medellín, donde es posible acceder a servicios de consultoría externa, puede consolidarse como una solución estratégica; no obstante, en contextos menos tecnificados, el ahorro inicial en licencias puede verse neutralizado por la necesidad de invertir en capacitación o contratar expertos, lo que obliga a las empresas a ponderar cuidadosamente la relación entre costo y sostenibilidad operativa.

Tabla 7

Funcionalidades Principales De Pfsense Y Pymes Colombianas

Funcionalidad	Descripción técnica	Aplicación en pymes colombianas
Firewall	Permite configurar reglas avanzadas para bloquear o permitir tráfico según direcciones IP, puertos o protocolos.	Protege redes pequeñas contra accesos no autorizados, spam y malware sin necesidad de soluciones comerciales.
VPN	Incluye soporte para redes privadas virtuales que cifran el tráfico a través de Internet.	Facilita el trabajo remoto seguro, cada vez más frecuente en empresas de servicios y consultorías.
Túneles seguros	Posibilita la comunicación cifrada entre diferentes redes privadas mediante enlaces sitio-a-sitio.	Útil para pymes con sedes en distintas ciudades de Colombia que necesitan conexión segura y constante.
Integraciones	Puede integrarse con otras herramientas open source como IDS/IPS o sistemas de monitoreo de red.	Permite ampliar capacidades de seguridad a bajo costo, adaptándose al crecimiento de la empresa.

Seguridad de capa de aplicación	Ofrece servicios como proxy inverso, filtrado de contenido, control de acceso, cifrado y mitigación de ataques DDoS.	Aporta protección adicional a servidores web y aplicaciones críticas, especialmente en negocios en línea.

*Nota***.** Funciones integrales del firewall pfsense. Adaptado de. Herramientas de Ciberseguridad open source. Pineda, Mateo. (2023). http://revista.escolme.edu.co/index.php/cies/article/view/479/520

Endian Firewall Community. Se presenta como una alternativa de código abierto que ofrece protección básica en navegación web, correo electrónico y acceso remoto mediante VPN. Para el caso colombiano, su valor radica en la posibilidad de reutilizar hardware en desuso, lo que resulta atractivo para pymes de comercio y servicios que operan con presupuestos limitados y necesitan un control inicial sobre sus redes. Sin embargo, su capacidad de escalamiento es reducida frente a firewalls más robustos como pfSense, lo que puede convertirse en un problema cuando la empresa experimenta un crecimiento acelerado o requiere gestionar amenazas más sofisticadas. En regiones intermedias del país, donde la conectividad y el soporte técnico son limitados, Endian puede brindar una defensa razonable contra amenazas comunes como spam, malware en correos electrónicos o accesos remotos inseguros. No obstante, su aplicación demanda considerar que la protección que ofrece se orienta más a la prevención de incidentes básicos y que, en el largo plazo, puede requerir migraciones hacia soluciones más avanzadas, lo que implica costos adicionales de tiempo y capacitación.

Tabla 8

Funcionalidades Principales De Endian Firewall Community

Funcionalidad	Descripción técnica	Utilidad en pymes colombianas
Seguridad de correo y web	Implementa servicios básicos de protección para la navegación y el correo electrónico.	Protege contra spam y sitios maliciosos, muy relevante en empresas con alto flujo de comunicaciones digitales.
Acceso remoto seguro	Ofrece conexión VPN e interconexión de sedes mediante túneles cifrados.	Permite a empleados acceder de forma segura desde ubicaciones remotas, útil en teletrabajo y sucursales.
Monitoreo y reporte en tiempo real	Genera visualizaciones y reportes del tráfico de red en tiempo real.	Facilita la supervisión de incidentes y ayuda a los administradores a detectar anomalías de manera temprana.
Manejo de eventos	Envía notificaciones automáticas por correo electrónico ante eventos críticos.	Permite reaccionar de manera más rápida ante intentos de intrusión o fallos de la red.
Firewall de estado	Controla el acceso a los recursos internos de la red con reglas configurables.	
Prevención de intrusos	Analiza el tráfico en busca de amenazas internas y externas.	Garantiza que solo usuarios autorizados accedan a sistemas sensibles de la empresa. Mitiga ataques comunes como intrusiones o propagación de

malware en la red corporativa.

Nota**.** Firewall código abierto endian. Adaptado de. las descripciones de funcionalidades de Endian Firewall Community. Bit, Victor. (2021). https://www.conlasredes.info/2021/10/endian- firewall-proteccion-de-codigo.html?m=1 y Comunidad de Endian UTM vs Firewalls de Endian. Endian. (2025). https://www.endian.com/community/features/

Snort. constituye una de las herramientas más reconocidas en la detección de intrusiones, utilizada en múltiples soluciones de seguridad comerciales. Su capacidad para analizar el tráfico en tiempo real y aplicar reglas adaptables lo hace especialmente útil en pymes colombianas con alto volumen de transacciones digitales, como plataformas de comercio electrónico y call centers. La crítica principal en el contexto nacional es que la herramienta exige conocimientos técnicos avanzados para configurar las reglas de detección y administrar registros, lo que limita su aprovechamiento en empresas que carecen de áreas de TI formalmente consolidadas. Aunque Snort puede ofrecer un nivel de protección sofisticado, el riesgo es que quede subutilizado si la organización no cuenta con personal capacitado para interpretarlo y actualizarlo constantemente. En la práctica, esto significa que su aplicación en Colombia es viable en pymes que, aunque pequeñas, han logrado acceder a asesoría externa o que integran estudiantes y técnicos en formación que pueden encargarse de la operación del sistema.

Tabla 9

Funcionalidades De Snort Y Su Aplicación En Pymes Colombianas

Funcionalidad	Descripción técnica	Aplicación en pymes colombianas
Grabación de paquetes	Registra paquetes de red en disco y los organiza en directorios según dirección IP y host.	Permite conservar evidencia de incidentes para análisis forense en empresas que manejan datos críticos. Ayuda a detectar ataques en curso en negocios con alto volumen de transacciones en línea.
Monitor de tráfico en tiempo real	Supervisa el tráfico de red entrante y saliente, alertando sobre paquetes sospechosos.	
Reglas adaptables	Utiliza un lenguaje de reglas flexible para diferenciar entre tráfico legítimo y malicioso.	Posibilita a las pymes personalizar la seguridad según sus procesos y servicios digitales.
Coincidencia de contenido	Clasifica reglas por protocolo y contenido, empleando un comparador de patrones múltiples.	Mejora la eficiencia en la detección de amenazas web y correo electrónico en empresas de servicios.
Huellas de sistemas operativos Análisis de protocolos	Identifica la plataforma del sistema operativo a través de su pila TCP/IP única.	Facilita la identificación de dispositivos no autorizados en la red de la pyme.
	Inspecciona paquetes en diferentes capas de protocolo para una revisión detallada del tráfico.	Contribuye a prevenir intrusiones complejas y ataques a protocolos críticos usados en operaciones locales.

*Nota***.** Funciones integrales y aplicabilidad de Snort. Adaptado de. Funcionalidades y explicación de snort como un ids/ips. Cibersegurity inc. Zenarmor. (2022). https://www.zenarmor.com/docs/network-security-tutorials/what-is-snort

ClamAV. representa una solución antimalware de código abierto ampliamente utilizada para la revisión de correos y archivos en servidores. En Colombia, su pertinencia se asocia con la alta dependencia de las pymes en el correo electrónico como canal principal de comunicación con clientes y proveedores. Su motor de detección, respaldado por actualizaciones de Cisco, brinda una cobertura básica contra troyanos, gusanos y malware móvil, lo cual puede reducir de forma significativa los riesgos de infección en empresas con poca capacidad de inversión. El análisis crítico muestra que, si bien es una herramienta ligera y gratuita, carece de soporte formal, lo que obliga a depender de comunidades y foros para resolver incidentes. En un país donde muchas pymes carecen de personal en ciberseguridad, esta limitación puede dificultar la respuesta ante infecciones graves. No obstante, su uso en combinación con prácticas como respaldos periódicos y segmentación de la red convierte a ClamAV en un primer paso razonable para fortalecer la seguridad informática en organizaciones pequeñas.

Tabla 10

Funcionalidades Principales De Clamav

Funcionalidad	Descripción técnica	Aplicación en pymes colombianas
Escaneo rápido de archivos	Diseñado para analizar de manera ágil documentos y directorios en busca de malware.	Facilita la revisión de correos y archivos compartidos en empresas con alto volumen de intercambio digital.
Protección en tiempo real	ClamOnAcc ofrece detección y bloqueo inmediato en versiones modernas de Linux.	Adecuado para servidores de correo corporativos que requieren neutralizar amenazas antes de su ejecución.
Detección amplia de malware	Reconoce millones de virus, troyanos, gusanos, macros y malware móvil.	Proporciona defensa básica contra infecciones comunes en estaciones de trabajo y servidores de pymes.
Motor de firmas avanzado	Su entorno permite crear rutinas de detección complejas y distribuir actualizaciones de forma remota.	Favorece la actualización constante frente a nuevas amenazas, aun en empresas con recursos limitados.
Firmas verificadas	Solo ejecuta definiciones de firmas que estén autenticadas para garantizar confiabilidad. Puede	Reduce riesgos de falsos positivos y asegura la estabilidad en entornos empresariales pequeños.
Escaneo de archivos comprimidos	inspeccionar archivos comprimidos y proteger contra bombas de archivo que buscan saturar el sistema.	Relevante en organizaciones que reciben archivos comprimidos con frecuencia, como agencias de servicios o comercio electrónico.

*Nota***.** Funciones de antivirus open source ClamAV. Adaptado de. las características técnicas y documentación. ClamAV. (2025). https://docs.clamav.net/ y complementado con observaciones de Pineda, Mateo. (2023). http://revista.escolme.edu.co/index.php/cies/article/view/479/520

El Xygeni Open Source. es una herramienta emergente orientada a la seguridad en la cadena de suministro de software, con funciones para detectar vulnerabilidades en bibliotecas externas y controlar licenciamientos. En el contexto colombiano, esta solución resulta especialmente relevante para startups de desarrollo de software y empresas tecnológicas en crecimiento, que dependen de repositorios externos para crear sus productos. El análisis crítico indica que su adopción todavía es incipiente en América Latina, lo que implica que las pymes que intenten implementarla enfrentarán retos de capacitación y adaptación a entornos poco explorados. Sin embargo, su capacidad para detectar riesgos en dependencias y prevenir ataques de día cero es particularmente valiosa en un entorno donde el desarrollo de aplicaciones digitales es cada vez más común en sectores como Fintech (tecnología financiera), e-commerce (comercio electrónico) y educación virtual. En este sentido, Xygeni puede convertirse en una ventaja competitiva para pymes tecnológicas colombianas que aspiran a exportar servicios y deben cumplir estándares internacionales de seguridad

Tabla 11

Funcionalidades Principales De Xygeni Open Source

Funcionalidad	Descripción técnica	Aplicación en pymes colombianas
Identificación integral de componentes	Detecta y cataloga con precisión cada componente de código abierto en uso.	Permite a startups y desarrolladores locales garantizar transparencia en sus proyectos de software.
Detección de malware en tiempo real	Realiza análisis continuo para identificar y bloquear malware justo después de su publicación.	Reduce riesgos de ataques de día cero en empresas que dependen de aplicaciones en línea.
Priorización de riesgos	Aplica un enfoque contextual para jerarquizar vulnerabilidades y asignar recursos a las más críticas.	Ayuda a pymes de software a optimizar esfuerzos de seguridad con presupuestos limitados.
Gestión avanzada de licencias y políticas	Simplifica el control de licencias de software de código abierto y garantiza cumplimiento normativo.	Evita riesgos legales en organizaciones que reutilizan múltiples bibliotecas externas.
Monitoreo continuo y alertas	Ofrece supervisión constante, detección temprana y reducción de falsos positivos.	Proporciona a las empresas un sistema de seguridad confiable sin necesidad de adquirir soluciones costosas.

Nota. Funciones integrales de Xygeni**.** Adaptado de. las características técnicas de Xygeni presentadas. Pineda, Mateo. (2023). http://revista.escolme.edu.co/index.php/cies/article/view/479/520 Xygeni. (2024). https://xygeni.io/es/blog/top-8-open-source-security-tools/#xygeni y Witts, Joel. (2024). https://expertinsights.com/devsecops/the-top-software-composition-analysis-tools

John the Ripper. es un software de auditoría de contraseñas que emplea técnicas de fuerza bruta y ataques de diccionario para identificar credenciales débiles. Su aporte en el contexto colombiano es relevante porque la gestión inadecuada de contraseñas sigue siendo una de las vulnerabilidades más frecuentes en las pymes, especialmente en sectores administrativos y de servicios que utilizan sistemas de facturación electrónica o banca en línea. Sin embargo, esta herramienta demanda conocimientos avanzados en pruebas de penetración y seguridad ofensiva, lo que implica que su uso no es viable en todas las empresas. El análisis crítico evidencia que su mayor valor está en auditorías internas o en ejercicios de consultoría especializada, donde puede detectar contraseñas repetidas o poco seguras y orientar la implementación de políticas más estrictas en línea con la Ley 1581 de 2012. En consecuencia, más que una solución de uso cotidiano, John the Ripper debe verse como un recurso puntual que ayuda a diagnosticar debilidades humanas en la gestión de credenciales y a reforzar la cultura de seguridad digital.

Tabla 12

Funcionalidades Principales De John The Ripper

Funcionalidad colombianas	Descripción técnica	Aplicación en pymes
Compatibilidad con múltiples algoritmos	Modo de descifrado personalizable	Descifra hashes generados por algoritmos como DES, MD5, bcrypt, AES y SHA.
Técnicas avanzadas de descifrado		Emplea ataques de diccionario, fuerza bruta, tablas arcoíris y modo incremental para probar combinaciones.
Ataques basados en reglas y listas de palabras		Permite configurar reglas y listas personalizadas para mejorar la efectividad de los descifrados.
Velocidad y rendimiento optimizado		Usa todos los núcleos de CPU y GPU compatibles (CUDA, OpenCL) para acelerar procesos de descifrado.
Compatibilidad entre plataformas		Funciona en Linux, Windows, macOS y arquitecturas variadas, incluidas distribuciones de pentesting.

Los administradores pueden ajustar parámetros para centrarse en contraseñas simples o complejas.	Permite evaluar contraseñas en diversos sistemas usados en entornos de oficina y servidores locales. Ayuda a identificar credenciales débiles y reducir riesgos de accesos no autorizados en la empresa. Facilita auditorías internas de contraseñas en empleados que suelen usar claves simples o repetidas. Reduce tiempos de prueba en auditorías de seguridad en pymes con recursos computacionales limitados. Se adapta a entornos heterogéneos en empresas que combinan diferentes sistemas operativos. Permite pruebas diferenciadas según el nivel de seguridad requerido por el área o servicio.	
Monitoreo en tiempo real sobre el número de contraseñas descifradas y el tiempo transcurrido.	Ofrece información continua	Brinda visibilidad en auditorías de seguridad, facilitando la toma de decisiones inmediatas.

*Nota***.** Funciones de herramienta ciberseguridad john the ripper. Adaptado de. las descripciones técnicas sobre John the Ripper como herramienta de auditoría de contraseñas.

Globalcybersecuritynetwork. (2025). https://globalcybersecuritynetwork.com/blog/top- cybersecurity-tools/#John_the_Ripper y Luz de, Sergio. (2024). https://www.redeszone.net/tutoriales/seguridad/crackear-contrasenas-john-the-ripper/

Wazuh. es una de las plataformas open source más completas para la gestión centralizada de incidentes, combinando capacidades de SIEM y XDR. En el caso de Colombia, su utilidad es evidente en pymes de sectores críticos como salud, educación y servicios financieros, donde la información sensible requiere auditorías constantes y trazabilidad frente a normas nacionales e internacionales. La crítica principal es que su implementación supone una inversión mayor en infraestructura y talento humano especializado, lo que la hace menos accesible para microempresas o negocios familiares. No obstante, aquellas pymes medianas que logran implementarla obtienen un sistema integral que permite recopilar datos de seguridad, supervisar configuraciones, automatizar respuestas ante incidentes y cumplir con exigencias regulatorias. En un entorno nacional caracterizado por ataques crecientes de ransomware y phishing, Wazuh ofrece la posibilidad de evolucionar de un esquema reactivo a uno preventivo y proactivo, lo que contribuye a consolidar una resiliencia digital más sólida.

Tabla 13

Funcionalidades Principales De Wazuh

Funcionalidad	Descripción técnica	Aplicación en pymes colombianas
Recopilación de datos de seguridad	Integración con MITRE ATT&CK	Los agentes instalados en los puntos finales recolectan información del sistema y reportan incidentes.
Monitoreo en tiempo real		Supervisa la actividad del sistema y las aplicaciones para detectar anomalías y amenazas.
Supervisión de configuraciones		Identifica errores o configuraciones inseguras en los sistemas de TI.
Cumplimiento normativo		Incluye auditorías basadas en marcos como PCI DSS, HIPAA, GDPR y NIST SP 800-53.
Escalabilidad y flexibilidad		Puede adaptarse a entornos locales, virtualizados y en la nube, consolidando la seguridad en un solo sistema.
Respuesta automática		Ofrece autodefensa mediante eliminación de archivos maliciosos y bloqueo de conexiones sospechosas.

Clasifica los eventos de seguridad según tácticas y técnicas de adversarios.	Brinda visibilidad sobre la seguridad de equipos de oficina y servidores usados en pequeñas empresas. Permite a las pymes identificar ataques en curso antes de que comprometan la continuidad del negocio. Ayuda a evitar fallos que puedan exponer información sensible en empresas con recursos técnicos limitados. Facilita a las pymes ajustarse a regulaciones locales y estándares internacionales de seguridad. Beneficia a negocios en expansión que integran servicios en la nube sin perder control de la seguridad. Reduce la dependencia de intervención manual, optimizando recursos en empresas con equipos reducidos. Mejora la capacidad de análisis y reacción en pymes frente a amenazas persistentes avanzadas

(APT).

*Nota***.** Funciones de wazuh. Adaptado de. Ciberseguridad y código abierto: la experiencia de wazuh y datasec Datasec. (2024). https://cuti.org.uy/destacados/ciberseguridad-y-codigo-abierto- la-experiencia-de-datasec-y-wazuh/

Figura 4

Herramientas Ciberseguridad De Código Abierto (Open Source)

Nota. Código abierto en ciberseguridad: un análisis profundo. Tomado de. Análisis de aspectos selectos del mundo matizado del código abierto en ciberseguridad. Haleliuk, Ross, (2022). https://ventureinsecurity.net/p/open-source-in-cybersecurity-a-deep

Cada una de estas estas herramientas de ciberseguridad tienen flexibilidad a las necesidades según la pyme, lo cual estas tienen adaptabilidad que poder ajustarse a la infraestructura pymes. también al ser open source, no tiene un soporte o un proveedor formal, ya que el soporte que se emplea es comunitario lo que permite en compartir conocimientos, soluciones, incidentes de ciberseguridad, lo que conlleva a enfrentarse a nuevas amenazas o vectores de ataque puedan comprometer los sistemas informáticos de las pymes. en la

ciberseguridad al utilizar estas herramientas de código abierto (open source), se benefician las pymes, sino también las pymes a nivel global que colaboran en conjunto para enfrentarse a nuevas amenazas y vectores de ataque, con el fin de proporcionar soluciones para fortalecer la ciberseguridad en las pymes.

Las herramientas de ciberseguridad de código abierto representan una alternativa estratégica para las pymes en Colombia, ya que permiten acceder a funcionalidades avanzadas sin asumir costos de licenciamiento; no obstante, como plantean autores como (Witts, 2024)su adopción exige evaluar cuidadosamente la capacidad interna de cada empresa para configurarlas, administrarlas y mantenerlas actualizadas; en la práctica, lo recomendable es que las organizaciones avancen de forma progresiva: en una primera fase, implementar soluciones básicas como pfSense y ClamAV; posteriormente, fortalecer la detección de intrusos mediante Snort y la auditoría de contraseñas con John the Ripper; y finalmente, consolidar un sistema integral de gestión de incidentes con Wazuh o herramientas especializadas como Xygeni en el caso de startups de software; esta priorización permite a las pymes avanzar en madurez digital, adaptando la tecnología a sus necesidades y alineándose con los marcos normativos colombianos.

Análisis crítico y Aplicación para PYMES en Colombia

En Colombia, las pequeñas y medianas empresas representan más del 90 % del tejido empresarial y concentran una parte esencial del empleo formal y de la dinámica económica. Sin embargo, su exposición a riesgos digitales ha crecido de manera significativa en los últimos años, en un contexto donde los intentos de ciberataques superaron los 36 000 millones durante 2024, situando al país como el segundo más afectado de América Latina. Esta situación se traduce en una presión adicional para las PYMES, que no cuentan con los mismos recursos

financieros, infraestructura tecnológica ni personal especializado que las grandes corporaciones. Los sectores de salud, manufactura, transporte, comercio y educación figuran entre los más golpeados, principalmente por depender de sistemas con escasos controles de seguridad, configuraciones básicas y una baja frecuencia de actualización de software.

El panorama de amenazas que enfrentan las PYMES también se ha transformado. En el último año ha cobrado fuerza el modelo de ransomware como servicio (RaaS), que facilita a actores maliciosos la utilización de kits de ataque sin grandes conocimientos técnicos, lo que ha multiplicado la cantidad de ofensivas dirigidas a organizaciones de menor tamaño. Frente a esto, se ha expandido el uso de campañas de phishing hiperpersonalizadas, diseñadas para imitar a entidades nacionales como la DIAN o bancos locales, con el fin de obtener credenciales de acceso y datos sensibles. Estas prácticas encuentran terreno fértil en empresas con bajo nivel de capacitación de su personal, donde persiste la percepción de que la ciberseguridad es un tema secundario o exclusivo de grandes compañías, cuando en realidad los incidentes reportados muestran que las PYMES constituyen un blanco recurrente.

Ante este contexto, el Estado colombiano ha reforzado su papel regulador y de acompañamiento a través de la Estrategia Nacional de Seguridad Digital 2025–2027. Esta hoja de ruta busca consolidar la gobernanza digital en el país, elevar la ciberresiliencia de los sectores productivos y actualizar el marco normativo frente a la evolución de las amenazas. De forma complementaria, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y entidades aliadas han puesto en marcha programas de becas y capacitaciones gratuitas en seguridad digital, con más de 10 000 cupos dirigidos a empresarios y trabajadores. A estos esfuerzos se suman cursos ofrecidos por el SENA y alianzas con empresas internacionales que certifican competencias en temas como gestión de incidentes, protección de datos y seguridad en

la nube. No obstante, la distribución territorial de estas oportunidades no es homogénea, pues la mayoría se concentra en grandes capitales, dejando rezagadas a empresas de regiones intermedias y rurales.

La capacidad de las PYMES para mejorar su postura de seguridad dependerá, en consecuencia, de varios factores interconectados. La escasez de talento humano especializado continúa siendo una de las principales limitaciones, lo que obliga a depender de servicios externos o consultorías temporales. A esto se suman los limitados presupuestos dedicados exclusivamente a ciberseguridad, que dificultan inversiones sostenidas en infraestructura y monitoreo continuo. El éxito en el fortalecimiento de la protección digital no reside únicamente en la adquisición de tecnologías, sino en la posibilidad de mantener procesos de actualización permanente, indicadores de desempeño claros y programas de concienciación dirigidos a todos los niveles de la organización. Así, indicadores como el porcentaje de empleados capacitados en simulacros de phishing, la proporción de sistemas con autenticación multifactorial o la frecuencia de respaldos verificados ofrecen un camino tangible para evaluar si las PYMES colombianas avanzan hacia una mayor ciber resiliencia en medio de un entorno cada vez más hostil.

Recomendaciones de Buenas Prácticas de Ciberseguridad para las Pymes

El sector de las pequeñas y medianas empresas en Colombia se caracteriza por un bajo nivel de madurez en materia de ciberseguridad, lo que las convierte en un blanco preferente para múltiples vectores de ataque que amenazan la continuidad de sus operaciones; a diferencia de las grandes compañías que cuentan con áreas especializadas y presupuestos robustos, muchas pymes operan con recursos limitados, sin procesos estandarizados de protección digital; esta situación se agrava en un entorno donde las transacciones en línea, la facturación electrónica y la gestión de clientes mediante plataformas digitales son cada vez más comunes; frente a este panorama, resulta indispensable adoptar un conjunto de prácticas de seguridad que combinen medidas técnicas, organizacionales y formativas, adaptadas a las realidades económicas y operativas de las pymes colombianas. (By Sosmatic, 2023)

Concientización del Personal

La primera barrera frente a los ataques cibernéticos no es tecnológica, sino humana. Como subraya (Lozano, 2024), la capacitación periódica del personal es fundamental para que los trabajadores desarrollen la capacidad de reconocer amenazas y actuar de forma preventiva; en Colombia, donde muchas pymes dependen de equipos pequeños y multitarea, la construcción de una cultura organizacional en seguridad requiere integrar la formación en el día a día de la empresa. De tal forma, no basta con impartir charlas ocasionales; es necesario implementar simulaciones periódicas de correos de phishing, crear canales de comunicación oficiales para reportar incidentes y promover la discusión de casos reales de ataques ocurridos en el país; con ello, el capital humano se convierte en la primera línea de defensa, reduciendo el riesgo de caer en fraudes digitales o manipulaciones sociales que suelen explotar el desconocimiento de los empleados.

Gestión De Contraseñas y Autenticación

El uso de credenciales débiles continúa siendo una de las vulnerabilidades más explotadas en ciberataques. (Sánchez, 2021) destacan que las contraseñas extensas, únicas y generadas aleatoriamente son más resistentes a los intentos de fuerza bruta; para las pymes colombianas, una estrategia viable consiste en adoptar gestores de contraseñas que automaticen la creación y el almacenamiento seguro de claves, complementados con políticas internas que obliguen a renovarlas trimestralmente. además, la incorporación de mecanismos de autenticación multifactor, por ejemplo, mediante códigos enviados al teléfono móvil o aplicaciones como Google Authenticator, añade una capa de seguridad adicional que dificulta el acceso no autorizado. estas medidas son especialmente relevantes en áreas sensibles como los sistemas contables, las bases de datos de clientes y los portales de banca en línea, donde un incidente puede comprometer tanto los recursos financieros como la confianza de los usuarios.

Actualización de Software y Dispositivos

El mantenimiento regular de sistemas y equipos constituye otra práctica crítica para prevenir vulnerabilidades. (Bravent, 2024) explica que la aplicación de parches en sistemas operativos, aplicaciones y dispositivos de red permite neutralizar fallos de seguridad antes de que sean explotados en ataques de día cero. en Colombia, muchas pymes utilizan software heredado o versiones sin licencia, lo que aumenta el riesgo de exposición a amenazas conocidas; frente a esta situación, resulta necesario establecer políticas de actualización cada quince días, documentar los cambios realizados e incluir mecanismos de control que permitan verificar que todos los equipos están en su versión más reciente; de este modo, se disminuye la probabilidad de incidentes derivados de infraestructuras obsoletas, que suelen ser aprovechadas por atacantes para propagar malware o interrumpir servicios críticos.

Soluciones Antimalware y Protección Centralizada

El despliegue de software antivirus y antimalware sigue siendo un pilar fundamental para contener amenazas como troyanos, ransomware y spyware; de acuerdo con (Ciberseguridad, 2024) estas soluciones deben implementarse de forma centralizada para garantizar uniformidad en las políticas de protección; en el contexto colombiano, donde muchas pymes cuentan con equipos heterogéneos y no siempre disponen de administradores dedicados, resulta clave seleccionar herramientas que permitan gestionar actualizaciones, reportes y cuarentenas desde un único panel de control. con ello, la empresa puede reducir tiempos de respuesta, asegurar que ningún dispositivo quede desprotegido y mantener un monitoreo constante de los incidentes. además, esta práctica transmite confianza a clientes y socios, quienes valoran que los datos compartidos estén resguardados frente a posibles filtraciones o infecciones.

Evaluación Periódica de Riesgos

El fortalecimiento de la resiliencia digital depende de la capacidad de identificar vulnerabilidades antes de que sean explotadas. (Slack, 2023) sostiene que los análisis de riesgos permiten orientar los recursos hacia las áreas más críticas, evitando inversiones dispersas o poco efectivas; en las pymes colombianas, esta práctica puede tomar la forma de evaluaciones trimestrales que incluyan pruebas de penetración, simulaciones de ataques de ransomware y diagnósticos de configuración de servidores; estas evaluaciones deben acompañarse de indicadores de cumplimiento, como el porcentaje de vulnerabilidades corregidas en cada ciclo, para medir de manera objetiva los avances logrados; así, la gestión del riesgo se convierte en un proceso continuo que permite mejorar progresivamente la postura de seguridad de la organización.

Incorporación de Talento Especializado

La disponibilidad de personal experto en ciberseguridad es un factor que marca la diferencia en la capacidad de respuesta frente a incidentes. (Lara, 2023) enfatiza que contar con profesionales certificados o con servicios de seguridad gestionados incrementa el nivel de protección de las pymes; en Colombia, donde muchas empresas carecen de presupuesto para mantener un área de TI robusta, externalizar la ciberseguridad hacia proveedores especializados puede ser una estrategia costo-efectiva. esta decisión no solo fortalece la capacidad de reacción ante ataques, sino que también proyecta confianza hacia los clientes y socios comerciales, quienes perciben un compromiso activo con la protección de los datos. Además el acompañamiento de expertos facilita la selección de tecnologías adecuadas, evitando gastos innecesarios en soluciones poco pertinentes para el tamaño de la empresa.

Respaldo y Recuperación de Información

La protección de los datos no se limita a evitar que sean robados o corrompidos, sino también a garantizar que puedan recuperarse ante un incidente. (McLennan, 2023) resalta que las copias de seguridad deben realizarse de manera programada y almacenarse en medios físicos y en la nube de forma complementaria. para las pymes colombianas, una práctica viable es programar respaldos automáticos semanales en la nube y mensuales en dispositivos externos desconectados de la red, conocidos como copias offline. adicional, también resulta indispensable realizar pruebas trimestrales de restauración para confirmar que los archivos pueden recuperarse de manera eficaz. estas medidas permiten mantener la continuidad operativa frente a desastres naturales, ataques de ransomware o fallos técnicos, garantizando que la información esencial para el negocio esté siempre disponible.

Aprovechamiento de Lecciones Aprendidas

Cada incidente de seguridad constituye una oportunidad de aprendizaje. (Bdoargentina, 2024) advierte que más del 80% de las pymes han sufrido brechas de seguridad en algún momento, lo que subraya la importancia de documentar causas raíz, registrar experiencias y retroalimentar las políticas internas. en el contexto colombiano, donde los reportes formales suelen ser escasos, la sistematización interna de incidentes permite evitar la repetición de errores y desarrollar protocolos más ágiles de respuesta. este aprendizaje organizacional fomenta una cultura de mejora continua que fortalece la preparación ante amenazas futuras y crea un historial útil para la toma de decisiones estratégicas.

Integración con Marcos Normativos

Finalmente, la consolidación de todas estas prácticas depende de su integración con estándares reconocidos que garanticen su sostenibilidad. (Nist, 2024) ofrece un marco flexible que facilita alinear las estrategias de seguridad con objetivos empresariales, detectar brechas y definir controles ajustados a las necesidades de cada organización. En el caso colombiano, este proceso puede complementarse con lineamientos emitidos por MinTIC y gremios empresariales, que promueven buenas prácticas adaptadas a la realidad local. como subraya (González, 2024) vincular la seguridad digital con la estrategia empresarial asegura la continuidad del negocio y fortalece la confianza de los clientes, mientras que (kaspersky, 2022) recuerda que muchas medidas preventivas no dependen de grandes inversiones, sino de la organización y constancia en la ejecución. de tal manera, las pymes colombianas pueden avanzar hacia un modelo de seguridad progresivo, sostenible y coherente con su capacidad operativa.

Figura 5

7 hábitos de Ciberseguridad para Proteger Tu pyme

*Nota***.** Seguridad informática en la pymes. Tomado de. 7 pasos para garantizar la ciberseguridad en tu Pymes. Prodwaregroup (2025). https://blog.prodwaregroup.com/es/perfiles/infografia-7- pasos-para-garantizar-la-ciberseguridad-en-tu-pyme/

De tal modo, al emplear estas buenas prácticas de ciberseguridad se fortalecen las defensas de seguridad para minimizar las amenazas cibernéticas también hay que tener en cuenta la ciberseguridad es muy fundamental, ya que la información es un activo muy primordial tanto para las organizaciones como la vida personal de un ciudadano; además, una empresa cuando

demuestra el interés en ciberseguridad en su entorno manifiesta confianza en sus clientes o usuarios lo cual les permite ser más competitivos y mejorar relaciones con otras organizaciones.

En el entorno nacional, proveedores tecnológicos, gremios y entidades públicas difunden lineamientos específicos para PYMES. (kaspersky, 2022) plantea medidas preventivas que complementan los esfuerzos internos de las empresas, mientras que (González, 2024) subraya la importancia de integrar la seguridad digital con la estrategia empresarial para mantener continuidad y confianza; estos aportes permiten que las PYMES adapten las prácticas de seguridad a sus condiciones financieras y operativas, garantizando que la protección de los datos no dependa exclusivamente de grandes inversiones, sino también de procesos organizados y consistentes.

Tabla 14

Plan de Buenas Prácticas de Ciberseguridad para PYMES

Área de acción	Acciones recomendadas	Contexto colombiano	Métrica de avance
Concientización del personal	Realizar talleres breves sobre phishing y malware; simulaciones internas trimestrales.	Útil en empresas con poco personal y alta rotación, comunes en comercio y servicios.	Al menos 80% de empleados identifica correos falsos en simulación.
Contraseñas y autenticación	Adoptar gestores de contraseñas; exigir MFA en sistemas críticos.	Prioritario en plataformas de facturación electrónica y banca en línea.	100% de usuarios con MFA activado en correos corporativos.
Actualización de software	Establecer política de parches cada 15 días; crear inventario tecnológico.	ciberseguridad.	protocolos.
		Respaldo de información	Respaldos automáticos
Antimalware y protección	Implementar antivirus/antimalware centralizado con administración remota.	semanales en la nube y mensuales offline; pruebas trimestrales de restauración.	
Evaluación de riesgos	Realizar pruebas de penetración, simulaciones de ransomware y auditorías trimestrales.		
		Lecciones aprendidas documentar causas raíz para retroalimentar	Registrar incidentes y
Talento especializado	Contratar personal certificado o tercerizar servicios gestionados de		

Muchas pymes operan con software desactualizado o sin licencia. Adecuado en pymes con equipos heterogéneos y sin área de TI dedicada. Sectores como retail y manufactura dependen de sistemas críticos de inventario y facturación. La externalización es viable frente a restricciones presupuestales. Relevante en pymes afectadas por ransomware en ciudades como Medellín y Cali. En Colombia se reportan pocos incidentes formales, por lo que la sistematización interna es clave.		90% de equipos actualizados en cada ciclo. Reportes centralizados con 0 equipos sin protección. 70% de vulnerabilidades corregidas en cada ciclo. Designación formal de responsable o contrato firmado con proveedor. 100% de respaldos verificados con recuperación exitosa. Documento interno actualizado tras cada incidente.	
Marco normativo y sostenibilidad	Alinear prácticas al NIST y a lineamientos de MinTIC; realizar auditorías internas anuales.	Relevante para cumplir con Ley 1581 de 2012 y lineamientos de protección de datos	personales.

Entrega de plan de	acción con al menos 5	mejoras priorizadas.	

---

*Nota***.** Recomendaciones de buenas prácticas de ciberseguridad. Adaptado de. Cómo desarrollar una cultura de ciberseguridad en la empresa. Lozano, Pablo. (2024). https://openwebinars.net/blog/como-desarrollar-cultura-ciberseguridad-empresa/

En primer lugar, la publicación de la “Guía de Pymes Ciberseguras” por la Cámara de Comercio de Bogotá en 2023 no puede entenderse de manera aislada, ya que responde a un escenario en el cual las denuncias por delitos informáticos crecieron de manera acelerada en el país, con un aumento del 175 % entre 2019 y 2022. De hecho, el Centro Cibernético de la Policía señaló un incremento sostenido del 45 % en los promedios anuales, lo que evidencia que las PYMES colombianas enfrentan un entorno cada vez más riesgoso.

Asimismo, la cooperación con actores privados, como el curso gratuito de Movistar Empresas lanzado en 2024, complementa las iniciativas de las cámaras de comercio, puesto que introduce contenidos prácticos sobre autenticación multifactor y protección de redes, elementos que difícilmente se consolidan en los programas tradicionales. De esta manera, se configura un ecosistema en el que la capacitación y la transferencia de conocimiento se convierten en una prioridad compartida entre gremios y empresas tecnológicas.

Por otra parte, resulta significativo que las Cámaras de Comercio regionales, como la de Medellín y la de Cali, integren la ciberseguridad dentro de programas más amplios de transformación digital. En este sentido, no solo ofrecen guías o talleres, sino que también proponen rutas de aprendizaje adaptadas a la realidad empresarial local. Así, las PYMES antioqueñas y vallecaucanas logran incorporar la seguridad digital en sus planes de crecimiento, aunque todavía persisten brechas relacionadas con infraestructura obsoleta y baja cultura organizacional en materia tecnológica.

Finalmente, al contrastar estas iniciativas con la dinámica empresarial nacional que refleja cerca de 300 000 nuevas unidades creadas cada año, se observa una tensión evidente: mientras la creación de empresas crece, las capacidades de protección digital avanzan de forma desigual. En consecuencia, la articulación de instrumentos locales (guías, talleres y checklists)

con lineamientos nacionales (como los protocolos del CSIRT Gobierno y la Circular 002 de la SIC) aparece como una estrategia clave para disminuir la vulnerabilidad estructural de las PYMES en Colombia.

Tabla 15

Programas y Lineamientos de Ciberseguridad para PYMES en Colombia

Entidad (jurisdicción)	Instrumento / actividad (año)	Naturaleza	Alcance declarado	Riesgos priorizados en Colombia (2024–2025)	Brechas observadas en PYMES colombianas	Síntesis de controles priorizados (vinculación técnica con el tema de trabajo)	Indicadores y umbrales propuestos (KPI/KRI)	Articulación institucional	Relevancia territorial / sectorial
Cámara de Comercio de Bogotá (Bogotá–Región)	"Guía de Pymes Ciberseguras" (2023)	Guía práctica	Mipymes y comercios con operación digital	Suplantación y fraude; phishing/BEC; fuga de datos; exposición por contraseñas débiles	Uso limitado de MFA; ausencias en políticas de parches; sensibilización irregular	Autenticación multifactor en correo y banca; gestores de contraseñas; campañas periódicas anti-phishing; hardening básico (servicios expuestos, Wi-Fi, DNS filtrado)	≥95 % de cuentas con MFA; tasa de clics en simulaciones < 5 %; tiempo de reporte interno < 15 min	Apoyo a inscripción en programa externo de preparación cibernética; referencia a protección de datos personales	Comercio minorista y servicios intensivos en facturación electrónica (Bogotá y municipios aledaños)

Entidad (jurisdicción)	Instrumento / actividad	Naturaleza	Alcance declarado	Riesgos priorizados en Colombia	Brechas observadas en	Síntesis de controles priorizados	Indicadores y umbrales propuestos	Articulación institucional	Relevancia territorial / sectorial
CCB + Cyber Readiness Institute (Bogotá–Región)	Programa gratuito de preparación cibernética (activo)	Capacitación modular	Pequeñas y medianas empresas	Riesgo humano (contraseñas, USB), phishing, equipos sin parches, nube mal configurada	Plantillas con rotación; inventarios de TI incompletos	Ciclo quincenal de parches; bloqueo de macros; filtros anti-phishing; autenticación reforzada; mínimo privilegio; verificación fuera de banda para pagos	90 % de endpoints con parches críticos < 7 d; ≥80 % del personal aprueba simulaciones; 100 % de cuentas críticas con MFA	Inscripción desde portal distrital y ruta CRI	Sectores servicios y comercio regional
Cámara de Comercio de	"Guía de protección de	Guía normativa-	Empresas afiliadas y comunidad	Incidentes de tratamiento indebido;	Ausencia de inventarios	Gobierno de consentimientos; inventario y	% bases clasificadas; % sistemas con	Coordinación con SIC para gestión de	Antioquia (servicios,

Entidad (jurisdicción)	Instrumento / actividad (año)	Naturaleza	Alcance declarado	Riesgos priorizados en Colombia (2024–2025)	Brechas observadas en PYMES colombianas	Síntesis de controles priorizados (vinculación técnica con el tema de trabajo)	Indicadores y umbrales propuestos (KPI/KRI)	Articulación institucional	Relevancia territorial / sectorial
Medellín para Antioquia	datos personales” (actualizada)	operativa		filtraciones; riesgos legales	y clasificación de datos; cifrado parcial	clasificación; cifrado en tránsito/almacenamiento; bitácora de actividades	cifrado; TMR* de solicitudes de titulares	PQRS de titulares	comercio electrónico)
Cámara de Comercio de Medellín para	“Checklist para evitar incidentes de	Lista de verificación	Empresas de la jurisdicción	Accesos no autorizados; pérdida/modificación de datos	Procedimientos de respuesta no consolidad	Registro sistemático de incidentes; controles mínimos	% controles cumplidos por ciclo; tiempo de cierre de hallazgos;	Reporte a SIC cuando proceda; adopción de formatos	Multisectorial con foco en MIPYME

Antioquia	seguridad de datos" (2021, vigente)			os; documentación de incidentes dispareja	administrativos y técnicos; pruebas de restauración; listas blancas	éxito de restauración trimestral	internos		
Cámara de Comercio de Cali (Valle del Cauca)	"Ciberseguridad en Acción: Protege tu Empresa" y "Buenas prácticas de ciberseguridad" (programación	Ruta de formación / eventos	Empresariado regional	Riesgos por malas prácticas del personal; exposición de activos conectados; fraudes en línea	Capacitación intermitente; carencia de playbooks operativos	Políticas de contraseñas; segmentación de red; endurecimiento de servicios expuestos; simulaciones trimestrales; verificación fuera de banda	Detecciones/10 0 endpoints; % tráfico cifrado; cumplimiento de simulacros ≥ 2/año	Articulación con programas de transformación digital	Valle del Cauca; e-commerce y manufactura ligera

2024–
2025)

Entidad (jurisdicción)	COLCERT (nacional)	Instrumento / actividad (año)	(recurrencia) Lineamientos para gestión y reporte de incidentes (2025)	Naturaleza		Alcance declarado	públicas; referencia para privados	Riesgos priorizados en Colombia (2024–2025)	"Graves/Muy graves"; coordinación interinstitucional; respuesta y mejora
	COLCERT				Servicio / guía				
Cámara de Comercio de Bucaramanga (Santander)	T (nacional)	Talleres y jornadas "ciberseguridad para empresas / prioridad empresarial"	y formatos de reporte Servicios y ABC del proceso de gestión de incidentes; "Reportar	Taller presencial/en línea	pública	Afiliados regionales	Sector público; orientador para privados	Ingeniería social, ransomware, fraude en pagos	Ransomware, denegación de servicio, intrusiones
MinTIC / CSIRT Gobierno –				Lineamiento y protocolo		Entidades		Eventos	

Brechas observadas en PYMES colombianas Ausencia de respaldos verificados; controles de acceso débiles Sub- reporte en privados; clasificación desigual	Desconocimiento de etapas y canales formales	Síntesis de controles priorizados (vinculación técnica con el tema de trabajo) Copias 3-2-1 con pruebas trimestrales; control de	accesos; listas blancas; bloqueo por intentos y passkeys Registro formal; análisis causa-raíz; plan de mejoras por ciclo; reporte a CSIRT Gobierno/COL CERT Flujo de	notificación; clasificación; coordinación con sectorial (p. ej., financiero)	Indicadores y umbrales propuestos (KPI/KRI) 100 % respaldos con restauración validada; bloqueos/h ante fuerza bruta; % MFA en cuentas críticas	% incidentes reportados; tiempo de contención; # mejoras implementadas /semestre % incidentes con radicado; tiempo de notificación < 24 h; cumplimiento de etapas	Articulación institucional Canales de denuncia/soporte local; derivación a CSIRT financiero según caso Escalamiento	formal; uso de formato Versión 3; referencia Decreto 338/2022 Coordinación con CSIRT sectoriales (financiero, defensa)	Relevancia territorial / sectorial Santander; servicios B2B Nacional;

sectores con servicios	esenciales un	Cobertura nacional

Entidad (jurisdicción)	Instrumento / actividad (año)	Naturaleza	Alcance declarado	Riesgos priorizados en Colombia (2024–2025)	Brechas observadas en PYMES colombianas	Síntesis de controles priorizados (vinculación técnica con el tema de trabajo)	Indicadores y umbrales propuestos (KPI/KRI)	Articulación institucional	Relevancia territorial / sectorial
	incidente ”								
Superintendencia de Industria y Comercio – SIC (nacional)	Circular Externa 002 del 21/08/2024: tratamiento de datos personale	Lineamiento regulatorio	Responsables/encargados de tratamiento (incluye PYMES)	Riesgos de privacidad en IA; modelos que procesan datos personales	Evaluaciones de impacto inexistentes; trazabilidad limitada	DPIA/PIA; idoneidad-necesidad-razonabilidad-proporcionalidad; medidas demostrables; registro de actividades	% sistemas con DPIA vigente; revisiones anuales de riesgo; TMR* solicitudes de titulares	Supervisión SIC; compatibilidad con Ley 1581/2012	Transversal, IA en marketing/soporte/analítica

	s en sistemas							
Confecámaras (nacional, base RUES)	de IA “Dinámica de creación de empresas 2024” (publicado 30/01/2025)	Estadística sectorial	Universo pyme formal —	Brecha de cobertura de programas vs. nacimientos empresariales por región	Priorización de intervención y metas de adopción (MFA, parches, respaldo) por sector/territorio	Cobertura de capacitación = empresas formadas / universo RUES; % nuevas con controles mínimos	Articulación con cámaras territoriales	Distribución por comercio, alojamiento/comida, manufactura
MinCIT – Estudios Económicos	“Informes de tejido empresarial” (últ.	Serie mensual / tablero	Empresas registradas (RUES) + micronegocios (DANE	Falta de series enlazadas con métricas	Tablero nacional: % adopción MFA; parches < 7 d; éxito de	KPIs por actividad CIIU y tamaño; variación mensual	Vinculación con cámaras y gremios para metas por región	Seguimiento a micro y pequeñas por dinámica sectorial

actualizac ión 29/08/2025)	Emicron)	de ciberseguridad	restauración; tasa de incidentes reportados

Entidad (jurisdicción)	Instrumento / actividad (año)	Naturaleza	Alcance declarado	Riesgos priorizados en Colombia (2024–2025)	Brechas observadas en PYMES colombianas	Síntesis de controles priorizados (vinculación técnica con el tema de trabajo)	Indicadores y umbrales propuestos (KPI/KRI)	Articulación institucional	Relevancia territorial / sectorial
DANE (nacional)	Encuesta de Microneg ocios (Emicron, 2025 I-trim)	Estadísti ca oficial	Micronegocios (≤ 9 ocupados)	— informalidad; conectividad	Alta tecnológica dispar	Estratificación de intervenciones y rutas de formación	% micronegocios con conectividad y MFA; % respaldo básico	Cruce con MinCIT/Confecámaras para focalización	Comercios de barrio y servicios personales
Policía Nacional – Centro Cibernético / CCIT /	CSIRT Financiero	Balance e indicadores de ciberam enazas	(2024–2025)	Reportes y alertas	Empresas y ciudadanía	Aumento de denuncias por delitos informáticos (≈ +23 % vs.	2023); intentos de afectación masivos; actividad	ransomware (LockBit/Interlock)	Planes de continuidad incompletos; canales de denuncia poco

usados	Respaldo 3-2-1 con pruebas; EDR/XDR; revisión de RDP/VPN; playbooks de pagos y fraude; WAF/CDN para picos de tráfico; coordinación con	CSIRT financiero	RTO < 24 h; endpoints con EDR ≥ 90 %; DMARC “reject” en dominios; eventos de mitigación DDoS por trimestre	Denuncia ante Policía; coordinación con ColCERT y CSIRT sectoriales	Financiero, salud, energía y retail con portales transaccionales

Nota. Programas de ciberseguridad para las pymes de Colombia. Tomado de. La información procede de Cámaras de Comercio, entidades estatales. Camara De comercio de bogota. (2023). https://economistacolombia.com/empresarial/camara-de-comercio-de- bogota-lanza-guia-de-ciberseguridad-para-pymes/ y gremios colombianos, con énfasis en iniciativas de capacitación, regulación. (2025). https://confecamaras.org.co/wp-content/uploads/2025/01/dinamica-creacion-empresas-colombia-2025.pdf y estadísticas empresariales dirigidas a pequeñas y medianas empresas. (2025). https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf

Como se observa en la ***Error! Not a valid bookmark self-reference.***, la ruta de adopción escalonada permite identificar qué herramientas de ciberseguridad son más pertinentes para las PYMES colombianas según su tamaño y recursos disponibles

Figura 6

Herramientas De Ciberseguridad En PYMES colombianas

Nota. Diagrama elaborado, muestra la progresión de adopción de herramientas de ciberseguridad en función del tamaño de la pyme en Colombia con inclusión de indicadores clave de desempeño (kpis) en cada etapa y un ciclo de revisión periódica

Pautas De Sensibilización en Ciberseguridad para que los Empleados Reconozcan los Vectores de Ataque que Emplean los Ciberdelincuentes para que las Victimas Divulguen Información Confidencial

Las pequeñas y medianas empresas en Colombia constituyen un sector especialmente vulnerable a los vectores de ataque empleados por los ciberdelincuentes; una de las razones principales es la limitada formación de los empleados en temas de seguridad digital, lo que los convierte en blancos fáciles de manipulación a través de correos electrónicos, llamadas fraudulentas o mensajes en redes sociales; tal como lo plantean diferentes especialistas, la falta de sensibilización constituye una de las debilidades más explotadas por los atacantes, pues permite que mediante técnicas de ingeniería social se obtenga información confidencial que compromete tanto a las personas como a la organización.

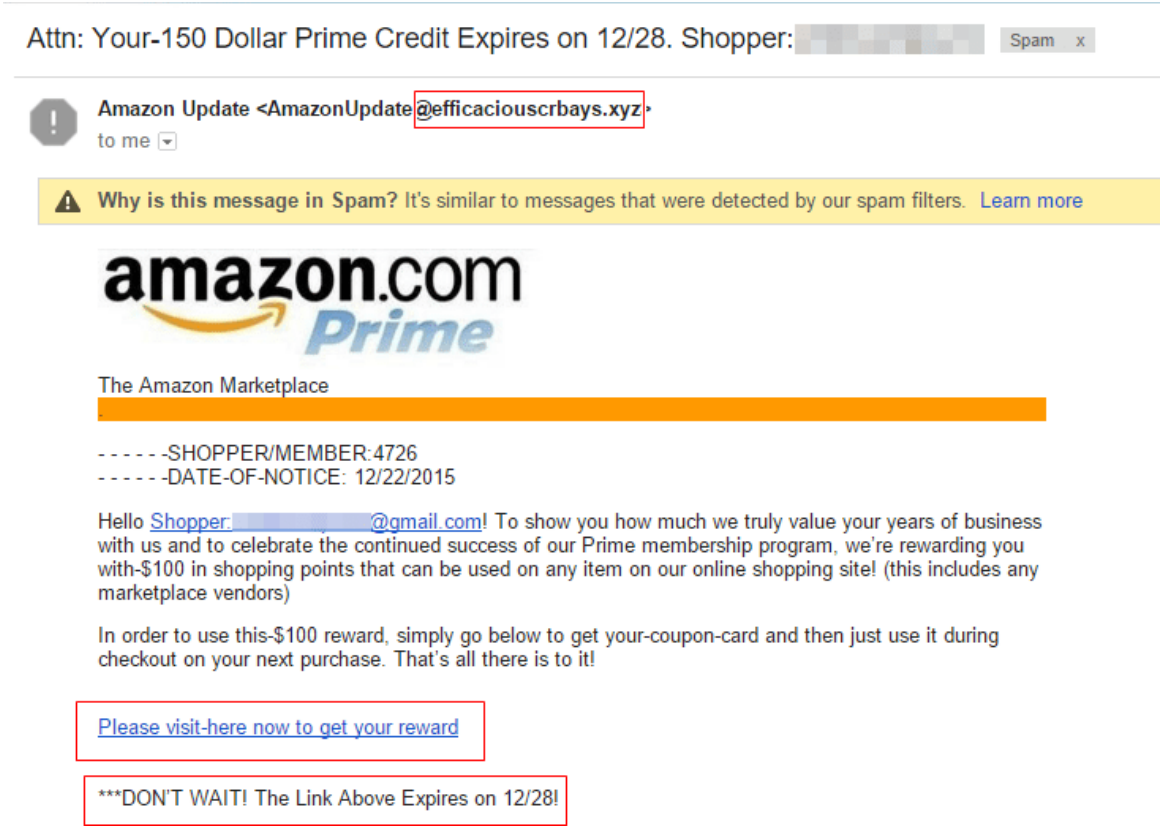
Dentro de los múltiples vectores de ataque, el phishing es uno de los más recurrentes y efectivos. Según (Tithink, 2018)este tipo de ataque se materializa principalmente a través de correos electrónicos fraudulentos diseñados para persuadir a la víctima de entregar credenciales o instalar software malicioso; su éxito radica en la capacidad de imitar comunicaciones legítimas de bancos, proveedores o entidades públicas, aprovechando la confianza de los empleados; en este contexto, es indispensable que las pymes desarrollen programas de capacitación que enseñen a reconocer las señales más comunes del phishing.

Entre los aspectos más relevantes a identificar se encuentran las direcciones de remitentes sospechosos que buscan pareceres legítimos, los errores de ortografía y redacción frecuentes en estos mensajes, así como los asuntos de correos que apelan a la urgencia para obtener credenciales o información sensible; también es necesario prestar atención a enlaces incluidos en el cuerpo del mensaje, que redirigen a páginas falsas, y a los archivos adjuntos que pueden

contener malware disfrazado de facturas o documentos de uso habitual; de acuerdo con (Tithink, 2018), reconocer estas señales constituye un primer paso para que los empleados eviten caer en las trampas de los atacantes.

Figura 7

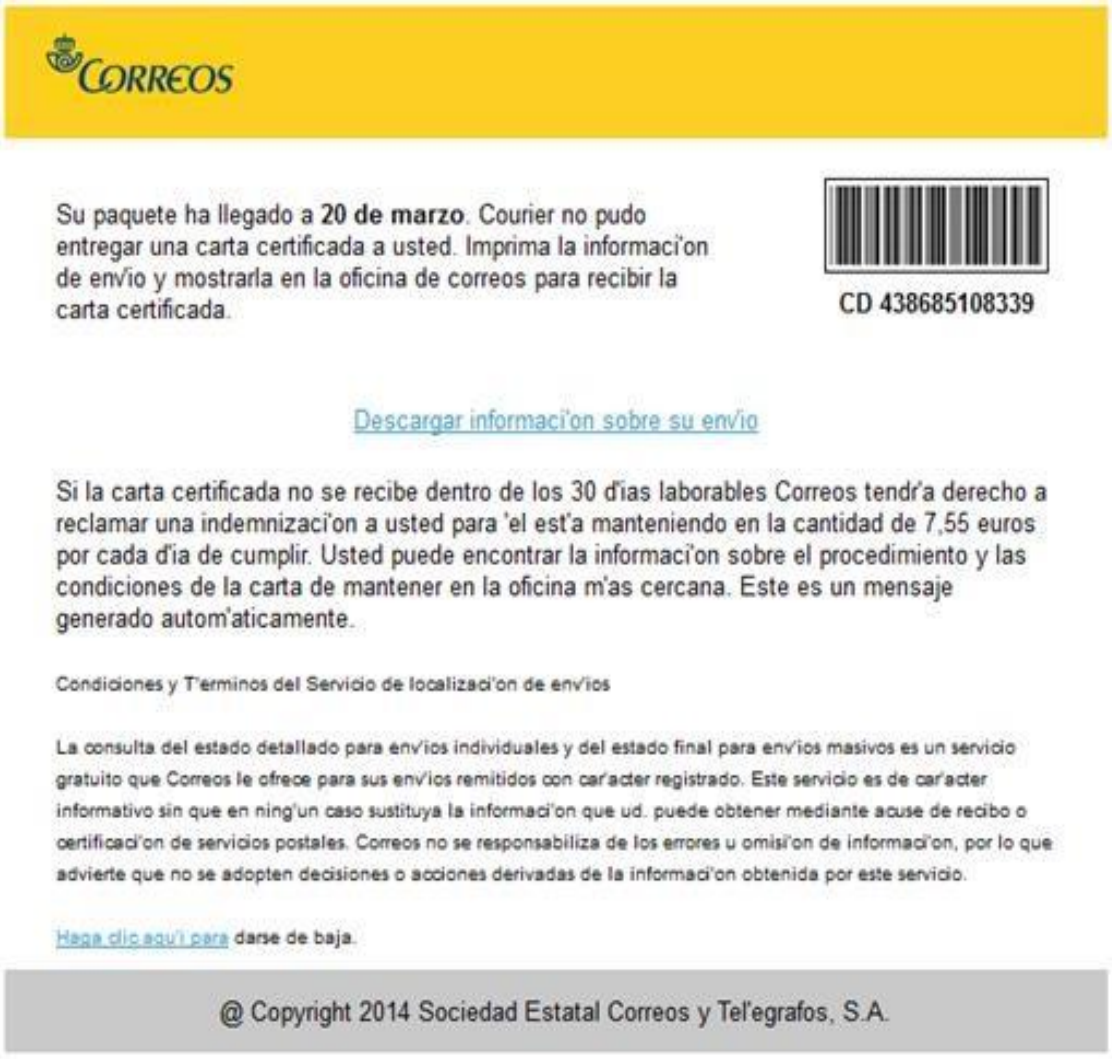
Correos Desconocidos



Nota. Vectores de ataque, aprende a identificarlos. Tomado de. Vectores de ataque. Tithink. (2018). https://www.tithink.com/es/2018/10/19/vectores-de-ataque-aprende-a-identificarlos/

Figura 8

Mala Ortografía Y Gramática

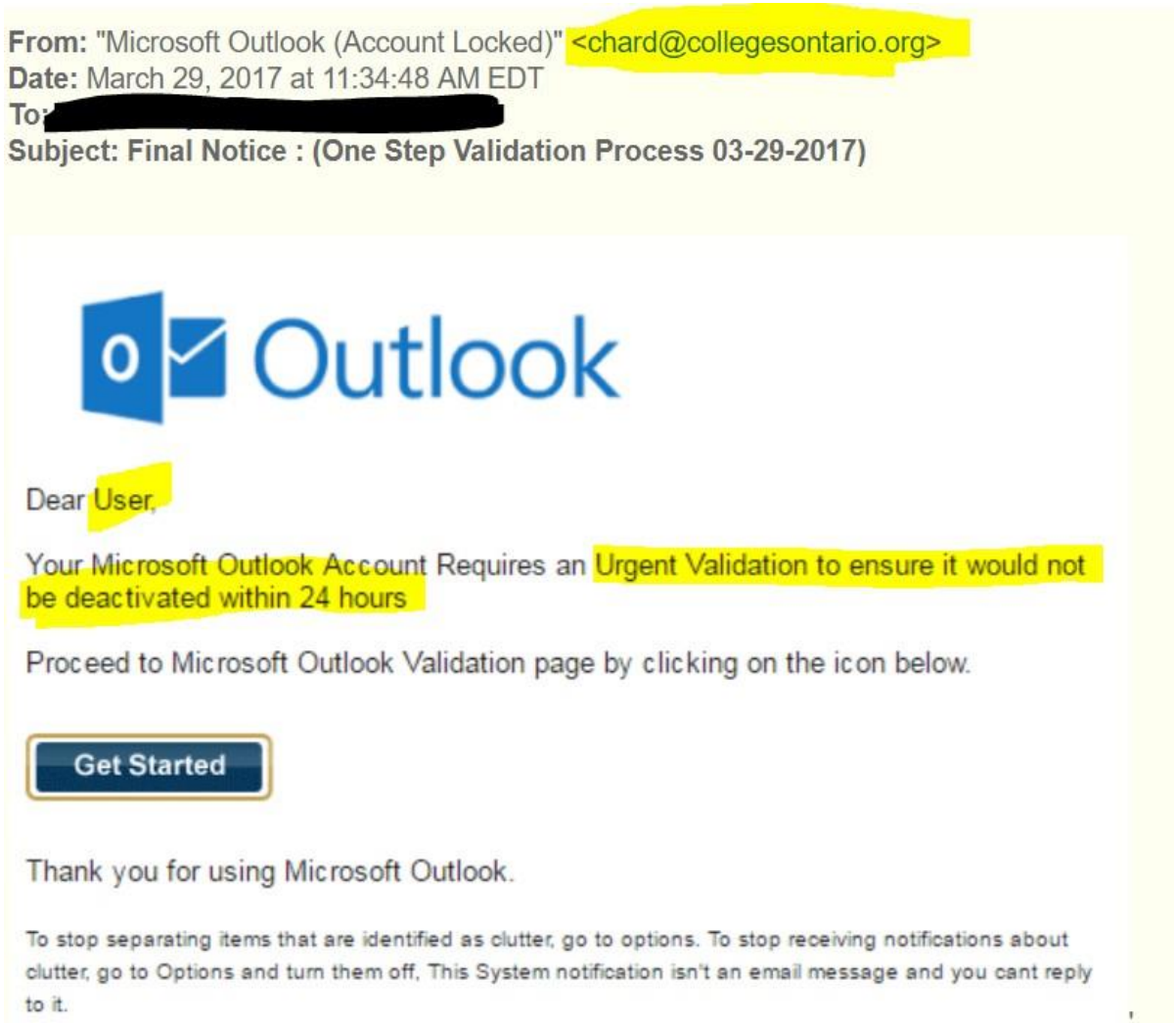


Nota. Vectores de ataque, aprende a identificarlos. Tomado de. Vectores de ataque. Tithink. (2018).

https://www.tithink.com/es/2018/10/19/vectores-de-ataque-aprende-a-identificarlos/

Figura 9

Direcciones Email Extrañas



Nota. Vectores de ataque, aprende a identificarlos. Tomado de. Vectores de ataque. Tithink. (2018). https://www.tithink.com/es/2018/10/19/vectores-de-ataque-aprende-a-identificarlos/

Ahora bien, el phishing no es la única amenaza. La ingeniería social también se materializa en llamadas telefónicas fraudulentas que apelan a la confianza, la emoción o el miedo de la víctima. (Lara, 2023) explica que estas llamadas se presentan bajo modalidades como la suplantación de ejecutivos bancarios que ofrecen créditos atractivos, las falsas notificaciones de premios inexistentes o incluso las extorsiones mediante supuestos secuestros; en todas estas variantes, el

denominador común es el intento de manipular psicológicamente a la persona para que entregue datos sensibles, transfiera dinero o permita accesos indebidos.

Para mitigar este tipo de riesgos, las pymes deben implementar procesos de sensibilización que incluyan ejemplos prácticos y simulaciones internas; es fundamental que los empleados aprendan a desconfiar de solicitudes inusuales, mantengan la calma frente a llamadas que apelan a la urgencia y confirmen la información a través de canales oficiales antes de actuar; de igual manera, resulta esencial que reconozcan que ni las entidades bancarias ni los organismos estatales solicitan contraseñas, consignaciones o pagos por vía telefónica.

Figura 10

No caigas en ataques de ingeniería social

*Nota***.** Modalidades de ingeniería social. Tomado de. no caigas en ataques de ingeniería social. smartekh. (2024).

https://mx.pinterest.com/pin/424745808611978987/

En síntesis, la protección contra estos vectores de ataque no depende exclusivamente de herramientas tecnológicas, sino de la sensibilización y el entrenamiento constante de los empleados. Para el caso colombiano, donde el uso de WhatsApp y redes sociales como Facebook e Instagram es parte cotidiana del entorno laboral y personal, se hace aún más urgente educar al personal en la gestión adecuada de su información; evitar la publicación de datos privados, desconfiar de mensajes desconocidos y verificar siempre la identidad de quien solicita información son prácticas que refuerzan la seguridad empresarial.

Por lo tanto, el mecanismo más efectivo para blindar a las pymes frente a amenazas de phishing e ingeniería social es la construcción de una cultura preventiva; un programa de sensibilización estructurado en fases que combine talleres iniciales, simulaciones prácticas y retroalimentación con base en incidentes reales que permitan que los empleados no solo reconozcan las tácticas de los ciberdelincuentes, sino que también desarrollen la capacidad de actuar con criterio y responsabilidad; al transformar a los trabajadores en agentes conscientes y preparados, las pymes fortalecen sus defensas digitales y aseguran la continuidad de sus operaciones frente a un panorama de amenazas en constante evolución.

Tabla 16

Modalidades De Ingeniería Social Y Pautas De Prevención

Vector de ataque	Características o señales de alerta	Pautas de prevención para empleados
Phishing por correo	clientes	Mensajes con errores ortográficos; remitentes sospechosos; asuntos que apelan a la urgencia; enlaces o archivos adjuntos falsos.
Estafas telefónicas (Ejecutivo bancario)		Supuesto agente de banco ofrece créditos atractivos con la condición de realizar consignaciones.
Estafas telefónicas (Premio en concurso) Estafas telefónicas (Secuestro simulado) Redes sociales y WhatsApp		Llamadas donde anuncian premios inexistentes (vehículos, dinero, electrodomésticos) a cambio de pagos o consignaciones. Llamadas que simulan el secuestro de un familiar, con voces llorando o mensajes urgentes para presionar.
Suplantación de proveedores o		Mensajes con enlaces desconocidos; perfiles falsos; solicitudes de datos personales o

financieros.	Verificar siempre el remitente y el
Correos o llamadas	dominio corporativo; no abrir
que imitan a	enlaces ni adjuntos sin
proveedores	confirmación; reportar correos
habituales, con	sospechosos al área responsable.
variaciones	Conocer el nombre del asesor
mínimas en	bancario real; recordar que ninguna
direcciones de	entidad pide claves ni pagos
correo o dominios.	anticipados; colgar la llamada y
	confirmar con el banco.
	Mantener la calma, no dejarse llevar
	por la emoción; confirmar en
	canales oficiales; nunca entregar
	dinero ni productos a desconocidos.
	Verificar de inmediato con el
	supuesto familiar; no ceder a la
	presión; contactar a la Policía o línea
	de emergencias.
	Configurar privacidad en redes
	sociales; evitar publicar información
	personal sensible; no abrir enlaces
	de desconocidos ni compartir datos.
	Confirmar pagos o solicitudes a
	través de un segundo canal de
	comunicación; establecer protocolos
	de validación de identidad.

*Nota***.** Métodos de ingeniería social. Adaptado de. los vectores de ataque Tithink. (2018). https://www.tithink.com/es/2018/10/19/vectores-de-ataque-aprende-a-identificarlos/ y técnicas de ingeniería social. Malagon, Juan. (2023). https://repository.unad.edu.co/bitstream/handle/10596/55080/jcmalagonl-.pdf?sequence=3&a

Conclusiones

En primer lugar, se evidenció que las pequeñas y medianas empresas constituyen un sector altamente expuesto a los vectores de ataque cibernéticos. Esto obedece, principalmente, a sus restricciones presupuestales y a la limitada disponibilidad de personal especializado en seguridad informática, lo cual deriva en la ausencia de políticas sólidas de prevención y respuesta. como consecuencia de estas insuficiencias, los incidentes como el phishing, el ransomware, el malware o los ataques de denegación de servicio (DDoS) adquieren una probabilidad mayor de materializarse y en caso de hacerlo, generan efectos que trascienden el plano tecnológico para impactar la reputación organizacional y la continuidad de las operaciones. en este sentido, comprender con detalle la naturaleza de los vectores, así como sus efectos sobre la información crítica, lo cual es un punto de partida inicial indispensable para diseñar estrategias defensivas que se ajusten a las necesidades del sector pymes.

De igual forma, el análisis permitió demostrar que las herramientas de código abierto se posicionan como una opción estratégica de especial valor para las pymes; a diferencia de las soluciones comerciales, que suelen ser costosas y de limitada adaptabilidad. las plataformas de código abierto (open source) entre ellas pfSense, Endian, Snort, ClamAV, Wazuh o John the Ripper brindan funcionalidades avanzadas de firewall, detección de intrusiones, monitoreo de tráfico, antivirus y gestión de incidentes sin necesidad de realizar inversiones desproporcionadas. A esto se suma que, al estar respaldadas por comunidades de desarrolladores colaborativos, se actualizan con frecuencia y perfeccionan de manera continua sus capacidades frente a amenazas emergentes. de este modo, la implementación de estas herramientas no solo fortalece la infraestructura tecnológica, sino que también ofrece a las pymes una solución flexible, escalable y sostenible a largo plazo.

También se subraya que la adopción de buenas prácticas de ciberseguridad constituye un complemento fundamental al uso de tecnologías específicas. dichas prácticas abarcan la gestión de contraseñas seguras, la actualización permanente de software, la instalación de programas antimalware, la realización periódica de respaldos de información, la evaluación sistemática de riesgos y en la medida de lo posible, la vinculación de personal con formación especializada seguridad. en efecto, cuando estas acciones se aplican de manera coordinada, no solo disminuyen de forma significativa la probabilidad de éxito de los ataques, sino que también promueven una cultura organizacional orientada hacia la seguridad y la confianza digital, lo que implica de manera directa en la fidelización de clientes y en la consolidación de relaciones con aliados estratégicos.

Por otra parte, se estableció que el factor humano constituye uno de los elementos más sensibles dentro de la ciberseguridad en las pymes. la falta de programas formativos y de sensibilización favorece la eficacia de técnicas de ingeniería social, mediante las cuales los ciberdelincuentes manipulan a los empleados para obtener información confidencial o vulnerar sistemas internos. en consecuencia, es necesario diseñar e implementar procesos permanentes de capacitación que permitan a los trabajadores identificar correos electrónicos fraudulentos, enlaces maliciosos, llamadas engañosas y solicitudes inusuales de datos sensibles. solo a través de la educación y el fortalecimiento de competencias digitales es posible transformar al talento humano en la primera línea de defensa de la organización y reducir de manera significativa la superficie de exposición frente a los vectores de ataque.

La protección de las pymes frente a los riesgos cibernéticos requiere un enfoque integral, en el que confluyan cuatro ejes interdependientes: la identificación de vectores de ataque, la adopción de herramientas de código abierto, la implementación de buenas prácticas

organizacionales y la formación continua del talento humano. En conjunto estos elementos conforman una estrategia articulada que posibilita garantizar la continuidad de los procesos empresariales, fortalecer la confianza digital y promover la sostenibilidad de las organizaciones en un entorno caracterizado por amenazas dinámicas y en constante evolución. De tal modo el cumplimiento de los objetivos del desarrollo de esta monografía, no solo permitió reconocer la magnitud de la problemática, sino también aportar lineamientos concretos que pueden servir como punto de referencia para el diseño de políticas, programas y proyectos orientados a la ciberseguridad de las pymes.

Recomendaciones

En base a la información recolectada en esta investigación y a los aportes del material bibliográfico para esta presente monografía, se recomienda:

Para las futuras investigaciones se recomienda realizar encuestas a este sector pymes, para verificar a que nivel de compresión de ciberseguridad tienen, dado que este sector empresarial tiene poco conocimiento en seguridad informática y de las amenazas cibernéticas en las que están expuestas cada día, ya que si estos son explotados puede afectar gravemente su continuidad operativa.

Así mismo para futuros proyectos de investigación desarrollar unas propuestas de capacitación con herramientas de ciberseguridad open source con máquinas virtuales al personal de las pymes, con el propósito comprendan importancia de la ciberseguridad. En base a lo anterior, proponer nuevas estrategias que se puedan implementar para minimizar las amenazas vectores de ataque y generar una cultura de ciberseguridad para salvaguardar la protección de los recursos e infraestructura cibernética pyme

También se recomienda al sector pyme tener la concientización en invertir en seguridad para sus recursos tecnológicos, ya que cada año se aumenta las cifras de ataques cibernéticos, lo cual generan perdidas monetarias cada año. También hay que tener en cuenta estas buenas prácticas, las herramientas y las recomendaciones de ciberseguridad no los libraran de los vectores de ataque, ya que cada día los ciberdelincuentes aprovechan de las nuevas Innovaciones tecnológicas para desarrollar métodos y tácticas para comprometer los sistemas informáticos de una empresa.

Referencias Bibliográficas

Avenía, C. (2017). Fundamentos de seguridad informática. In *Areandina* (Issue 2). https://digitk.areandina.edu.co/server/api/core/bitstreams/e6647b6c-a261-4ccb-b674-7288c0090b33/content

aws.amazon. (2023). *Qué es la ciberseguridad?* https://aws.amazon.com/es/what-is/cybersecurity/#:~:text=La ciberseguridad es la práctica,cliente y cumplir la normativa

Barcelona, R. (2024). *La ciberseguridad preocupa a las pymes: el 60% han sido víctimas de ataques*. 8 Abril. https://www.lavanguardia.com/economia/20240408/9590136/ciberseguridad-preocupa-pymes-60-han-sido-victimas-ataques.html

BBVA. (2023). *Qué es el phishing y cuáles son sus consecuencias?* Julio 3. https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/spoofing-telefonico.html

BBVA. (2024). *El universo mipyme en Colombia*. Enero. https://www.bbvaresearch.com/wp-content/uploads/2024/02/202401_MiPymes_Colombia-1.pdf

Bdoargentina. (2024). *6 estrategias en ciberseguridad para proteger a las organizaciones*. Octubre 1. https://www.bdoargentina.com/es-ar/publicaciones/categoria-de- publicaciones/grupo-de-publicaciones/como-pueden-los-consejos-mejorar-en- ciberseguridad-6-estrategias-para-proteger-a-las-organizaciones

Bravent, N. (2024). *10 prácticas de ciberseguridad imprescindibles para cualquier negocio*. Julio 3. https://www.bravent.net/noticias/10-practicas-ciberseguridad-imprescindibles- cualquier-negocio/

By Sosmatic. (2023). *Los tipos de ciberataques más comunes que reciben las empresas*. Marzo

17. https://www.sosmatic.com/los-tipos-de-ciberataques-mas-comunes-que-reciben-las-empresas/#:~:text=proteger su información.-,Pymes: objetivo principal de los ciberataques,adaptado siempre a tu empresa

Calvo, L. (2023). *Observatorio sobre digitalización de GoDaddy España 2023*. Agosto 28. https://www.godaddy.com/resources/es/godaddy/observatorio-digitalizacion-2023- marketing

Ccit. (2024). *Ciberseguridad en Colombia: desafíos y perspectivas*. Abril 26. https://www.ccit.org.co/articulos-tictac/ciberseguridad-en-colombia-desafios-y- perspectivas/

Ciberseguridad. (2024). *Internet vs Seguridad: 7 acciones para aumentar la ciberseguridad*. Mayo 9. https://enteldigital.cl/blog/internet-vs-seguridad-7-acciones-para-aumentar-la- ciberseguridad

Cilleruelo, C. (2024). *Qué es un vector de ataque en ciberseguridad?* Junio 19. https://keepcoding.io/blog/que-es-un-vector-de-ataque-en-ciberseguridad/

Clamav. (2025). *Documentación de ClamAV*. https://docs.clamav.net/ Colombia, congreso de. (2009). *LEY 1273 DE 2009*. Enero 5. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492#:~:text=Po r medio de la cual,las comunicaciones%2C entre otras disposiciones

congreso de colombia. (2000). *LEY 590 DE 2000*. Julio 10. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=12672

conpes. (2011). *conpes 3701*. Julio 14. LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA

Cuti. (2024). *Ciberseguridad y código abierto: la experiencia de Datasec y Wazuh*. Junio 7.

https://cuti.org.uy/destacados/ciberseguridad-y-codigo-abierto-la-experiencia-de-datasec- y-wazuh/

CyberEOP. (2025). *Protegiendo a las Pymes: Desafíos en Ciberseguridad*. https://www.cybereop.com/blog/protegiendo-a-las-pymes-desafios-en- ciberseguridad.html

DigitalOcean. (2023). *Small businesses and cybersecurity*. 6. https://anchor.digitalocean.com/rs/113-DTN-266/images/Security-Report_DigitalOcean.pdf?mkt_tok=MTEzLURUTi0yNjYAAAGKx5z_ZPYAC-86Rzqj2H8M5CcpHbripszTaynvLi2kXVlcELdKklw7mS0mGPb8wSRtXMcKXZ4Jj6Ji8

Docusign. (2023). *La ciberseguridad en las PYMES: Por qué es esencial*. Julio 5. https://www.docusign.com/es-mx/blog/desarrolladores/lciberseguridad-en-las-pymes

Edorteam. (2024). *Ciberseguridad para PYMES: protegiendo tu negocio*. Diciembre 10. https://edorteam.com/ciberseguridad-para-pymes-protegiendo-tu-negocio/

Eduardo, N. (2021). *Endian Firewall, protección de Código Abierto.* Octubre 13. https://www.conlasredes.info/2021/10/endian-firewall-proteccion-de-codigo.html?m=1

Endian. (2025). *Comunidad de firewalls de Endian*. https://www.endian.com/community/features/

Fortinet Inc. (2024). *Tipos de ciberataques: ataque DDoS, ransomware y más*. https://www.fortinet.com/lat/resources/cyberglossary/types-of-cyber-attacks

globalcybersecuritynetwork. (2025). *50 herramientas de ciberseguridad que debes conocer en 2025*. Marzo 16. https://globalcybersecuritynetwork.com/blog/top-cybersecurity-tools/#John_the_Ripper

González, P. G. (2024). *Ciberseguridad para las pymes: Buenas prácticas*. Agosto 8.

https://www.beedigital.es/servicios-digitalizar-negocio/ciberseguridad-para-las-pymes- buenas-practicas/

Gregg Lindemulder, M. K. (2024). *Qué es un ataque de intermediario (MITM)?* Junio 11. https://www.ibm.com/mx-es/think/topics/man-in-the-middle

Guzmán, L. M. F. B. G. (2022). *Ataques a entidades de gobierno*. https://www.ccit.org.co/wp-content/uploads/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno- safe-bp.pdf

Hernandez, Y. (2022). *Qué es una amenaza en seguridad Informática y cómo prevenirla?* Abril 18. https://www.dongee.com/tutoriales/que-es-una-amenaza-en-seguridad/ Hiscox. (2024). *Informe de preparación cibernética de Hiscox 2024*. https://www.hiscoxgroup.com/cyber-readiness

Itsitio. (2023). *PyMEs de Colombia registran 30 millones de intentos de ciberataque al año.* Junio 26. https://www.itsitio.com/co/seguridad/pymes-de-colombia-registran-30- millones-de-intentos-de-ciberataque-al-ano/

Jaimovich, D. (2024). *Los 14 tipos de ciberataque más comunes (y cómo prevenirlos).* Septiembre 4. https://blog.invgate.com/es/tipos-de-ciberataque

Jiang, W. (2022). *código abierto*. https://www.sciencedirect.com/topics/computer-science/open- source-project

kaspersky. (2022). *Los ataques financieros crecen en América Latina y aumenta la preocupación por el uso de la piratería*. https://latam.kaspersky.com/blog/panorama-amenazas-latam- 2022/25509/

Lara, C. (2023). *ANÁLISIS DE LAS TÉCNICAS DE INGENIERÍA SOCIAL QUE AMENAZAN LA SEGURIDAD INFORMÁTICA DE USUARIOS DE ENTIDADES FINANCIERAS*.

https://repository.unad.edu.co/bitstream/handle/10596/55080/jcmalagonl-

.pdf?sequence=3&a

López, M. (2023). *Principales vectores de ataque utilizados por ciberdelincuentes*. Enero 14. https://immune.institute/blog/vectores-de-ataque-cibersegurdad/

Lozano, pablo alcarria. (2024). *Cómo desarrollar una cultura de ciberseguridad en la empresa*. Julio 19. https://openwebinars.net/blog/como-desarrollar-cultura-ciberseguridad-empresa/

Luz, S. de. (2024). *Crackea contraseñas rápidamente usando John the Ripper*. Octubre 15. https://www.redeszone.net/tutoriales/seguridad/crackear-contrasenas-john-the-ripper/

McLennan, M. (2023). *Guía de buenas prácticas de ciberseguridad*. Septiembre 3. https://www.marsh.com/co/services/cyber-risk/insights/good-cybersecurity- practices.html

MinTic. (2024). *La ciberseguridad es el camino para crecer y fortalecer los entornos digitales del país": Ministro Lizcano*. Septiembre 20. https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/396032:La- ciberseguridad-es-el-camino-para-crecer-y-fortalecer-los-entornos-digitales-del-pais- Ministro-Lizcano

Muñoz, G. (2019). Las micro, pequeñas y medianas empresas, una estrategia de aplicación de tecnología para aumentar su competitividad. *Espacios*, *40*(20), 1–14. http://www.revistaespacios.com/a19v40n20/19402002.html

Nettix. (2025). *Análisis de PfSense como una alternativa a otros firewalls comerciales*. https://www.nettix.com.pe/blog/firewall/analisis-de-pfsense-como-una-alternativa-a- otros-firewalls-comerciales

Nist. (2024). *El Marco de Seguridad Cibernética (CSF) 2.0 del NIST*. 1–29.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf

Pineda, M. V. (2023). Análisis de herramientas de ciberseguridad de código abierto para la prevención de ciberataques a pequeñas y medianas empresas en Colombia. *Julio 23*, 231–234. http://revista.escolme.edu.co/index.php/cies/article/view/479/520 Py. (2024). *Ciberseguridad en pymes: un asunto que no da espera*. Editorial. https://www.pymas.com.co/ideas-para-crecer/mundo-pyme/ciberseguridad-pymes Renata. (2023). *Colombia segundo lugar en ciberataques en Latinoamérica, conozca los riesgos para evitar incidentes de ciberseguridad*. https://www.renata.edu.co/colombia-segundo- lugar-en-ciberataques-en-latinoamerica-conozca-los-riesgos-para-evitar-incidentes-de- ciberseguridad/

Riva, S. (2020). *¿Qué son las PYMES?* Diciembre 5. https://blog.grupoenroke.com/que-son-las- pymes

Riveros, A. (2020). *Diferencias entre ataque, amenaza y vulnerabilidad en Ciberseguridad.*

Sánchez, P. A. (2021). Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. *Información Tecnológica*, *32*(5), 8. https://doi.org/10.4067/s0718-07642021000500121

Security, C. (2022). *5 vectores de ataque en ciberseguridad que impacta en empresas, personas y gobiernos*. Junio 29. https://www.flane.com.pa/blog/es/5-vectores-de-ataque-en- ciberseguridad-que-impacta-en-empresas-personas-y-gobiernos/

Slack. (2023). *Ciberseguridad en empresas: 10 consejos para mantener tus datos a salvo.* Noviembre 23. https://slack.com/intl/es-es/blog/transformation/ciberseguridad-empresas Tithink. (2018). *Vectores de ataque, aprende a identificarlos*. Octubre 19. https://www.tithink.com/es/2018/10/19/vectores-de-ataque-aprende-a-identificarlos/

Trevino, A. (2024). *Ocho vectores de ataque habituales que las organizaciones deben conocer*. Abril 4. https://www.keepersecurity.com/blog/es/2024/04/04/eight-common-attack- vectors-organizations-need-to-be-aware-of/

Tuteja, A. (2024). *Cómo pueden las pymes convertir el riesgo de ciberseguridad en una oportunidad*. Agosto 18. https://es.weforum.org/stories/2024/08/las-pymes-pueden- convertir-el-riesgo-de-ciberseguridad-en-una-oportunidad-como-hacerlo/

Unir. (2020). iberdelincuencia: qué es, concepto de ciberdelito y tipos. *Unir*. https://www.unir.net/revista/derecho/que-es-ciberdelincuencia/

Universidad, I. I. (2023). *Sistemas informáticos (SI): qué son, características y tipos*. Febrero 13. https://www.ui1.es/blog-ui1/sistemas-informaticos-si-que-son-caracteristicas-y-tipos

UNSA. (2019). UNIDAD 1: Introducción a la Informática Hardware y Software. *Seminario de Informática*, 1–62. https://economicas.unsa.edu.ar/sigeco/archivos/semi_material/U1-DT-IntroduccionalaInformatica.pdf

Valoyes, A. (2019). Ciberseguridad en el 2019 en Colombia. *Ciberseguridad En Colombia*. https://www.emis.com/php/search/doc?pc=CO&dcid=636712564&primo=1%0Ahttps://www.dinero.com/tecnologia/articulo/ciberseguridad-en-el-2019-en-colombia/265858

Witts, J. (2024). *Las 12 mejores herramientas de análisis de composición de software*. Diciembre 3. https://expertinsights.com/insights/the-top-software-composition-analysis- tools/

Xygeni. (2024). *Asegure el desarrollo y entrega de software*. https://xygeni.io/es/blog/top-8- open-source-security-tools/

Zenarmor. (2022). *Explicación de Snort IDS/IPS: qué es, por qué lo necesita y cómo funciona*. Agosto 26. https://www.zenarmor.com/docs/network-security-tutorials/what-is-snort

Zendesk. (2024). *Open Source: qué es, ventajas y diferencias con open API*. Enero 4. https://www.zendesk.com.mx/blog/que-es-open-source/