Revista CIES – ISSN-e 2216-0167. Volumen 14. Número 2. Año 2023. Páginas 221-241. Dirección de Investigaciones – Institución Universitaria Escolme (Medellín, Colombia)

Análisis de herramientas de ciberseguridad de código abierto para la prevención de ciberataques a pequeñas y medianas empresas en Colombia

Mateo Vanegas Pineda
Tecnología en Redes y Seguridad Informática, Institución Universitaria Escolme, Medellín, Colombia, mvanegasp@escolme.edu.co

Alex Mauricio Ávila Quiceno
Docente, Institución Universitaria Escolme, Medellín, Colombia, amavilaq@escolme.edu.co

Recibido: 23/07/2023 - **Aceptado:** 15/08/2023 - **Publicado:** 18/10/2023

RESUMEN

Las pequeñas y medianas empresas en Colombia representan gran parte de la economía del país. Es cada vez más frecuente que una empresa pequeña o mediana que no se encuentre debidamente equipada ante un ataque informático, sea por desconocimiento, informalidad o falta de recursos, no logre una recuperación financiera a causa de las grandes pérdidas generadas por los ciberdelincuentes. El objetivo principal de la investigación es brindar un análisis acerca de las diferentes herramientas de ciberseguridad de código abierto que pueden ser implementadas en la infraestructura tecnológica de una pequeña o mediana empresa como una solución alterna a las herramientas comerciales logrando que esta sea una forma de prevención ante ciberataques tomando como línea base de protección un firewall o cortafuegos, un Sistema de Detección y Prevención de Intrusos (IDS/IPS) y un antivirus. La metodología del trabajo se enfocará en la revisión sistemática de la literatura técnica y un análisis de las diferentes herramientas investigadas. Los principales resultados de la investigación permitirán determinar la viabilidad y las mejores prácticas para la implementación de herramientas de ciberseguridad de código abierto en las pymes, contribuyendo así a fortalecer su seguridad en línea y reducir el riesgo de ciberataques considerando que existen múltiples herramientas y cada una de estas requieren de un conocimiento técnico específico para su implementación y gestión.

Palabras clave: ciberseguridad; herramientas de ciberseguridad; pequeñas y medianas empresas; código abierto; amenazas informáticas.

ABSTRACT

Small and medium-sized enterprises (SMEs) in Colombia represent a significant portion of the country's economy. It is becoming increasingly common for a small or medium-sized company that is not properly equipped to handle a cyberattack, whether due to lack of knowledge, informality, or resource constraints, to suffer financial setbacks due to the substantial losses caused by cybercriminals. The main objective of this research is to provide an analysis of various open-source cybersecurity tools that can be implemented in the technological infrastructure of a small or medium-sized enterprise as an alternative solution to commercial tools, thereby serving as a

preventive measure against cyberattacks. The foundational protection baseline will include a firewall, an Intrusion Detection and Prevention System (IDS/IPS), and an antivirus. The methodology of the study will focus on a systematic review of technical literature and an analysis of the different tools under investigation. The primary outcomes of the research will help determine the feasibility and best practices for implementing open-source cybersecurity tools in SMEs, thus contributing to enhancing their online security and reducing the risk of cyberattacks. It is important to note that there are various tools, each requiring specific technical expertise for implementation and management.

Keywords: cybersecurity; cybersecurity tools; small and medium-sized enterprises; open source; cyber threats.

1. INTRODUCCIÓN

En el mundo moderno, la interconexión de dispositivos para la comunicación se ha convertido en una necesidad para personas, instituciones educativas y organizaciones, grandes y pequeñas. Cada día, se añaden más dispositivos y componentes a esta red conjunta, por lo que de la misma forma aumenta la probabilidad del daño e impacto que pueden tener las ciber amenazas en este ambiente tecnológico, específicamente cuando se trata de un entorno laboral o corporativo (Rea-Guaman et. al, 2017).

Por esto, las organizaciones deben reconocer la importancia de plantear adecuadamente una estrategia que permita salvaguardar y darle el correcto manejo a su activo más valioso: la información. Además del planteamiento de una debida estrategia enfocada a la seguridad de la información y ciberseguridad, dentro de una organización, las tecnologías, los procesos y las personas deben complementarse entre sí con el fin de crear una defensa apropiada contra los ciberataques (Cisco, s.f.).

El principal tipo de ataque que pone en riesgo la continuidad del negocio de entidades empresariales es el ransomware, pues debido a que se trata de un software extorsivo, su finalidad es impedir el uso de los sistemas informáticos hasta que se haya pagado una recompensa al atacante (Kaspersky, s.f.). Hasta el mes de diciembre del año 2022 Colombia registró un incremento del 133% en contraste con el año 2021 con respecto al número de instituciones afectadas por ransomware (Lumu, 2022). Empresas e instituciones grandes como Empresas Públicas de Medellín, EPS Sanitas, Fiscalía General, Universidad Javeriana, entre otras han sido víctima de este ciberataque durante el previo año.

De la misma manera, pequeñas y medianas empresas (pymes) también tienen una presencia significativa en el campo de los ciberataques. Muchas de estas empresas suelen descuidar la seguridad de su información y su infraestructura tecnológica. Según estudios realizados por EIT Digital, Huawei y Fundación Digital Global, hasta diciembre de 2022, el 57% de las pymes en Europa se han visto obligadas a cerrar sus operaciones comerciales a causa de los ciberataques (Forbes, 2022).

El escenario de la ciberseguridad para las pymes en el país colombiano refleja un patrón similar ya que durante los primeros nueve meses del año 2021 se reportaron más de 500 casos de ataques

tipo ransomware contra estas organizaciones (Cámara Colombiana de Informática y Telecomunicaciones, 2021). Esto puede deberse en parte a que muchas de estas empresas, a veces no por elección propia, carecen de formalidad en su establecimiento, lo que genera la falta de herramientas esenciales para enfrentar las amenazas en el ciber espacio.

Las herramientas tanto a nivel de software como de hardware que se encargan de brindar una capa de protección cibernética conllevan múltiples costos, requerimientos y consideraciones para su implementación. Firewall, antivirus, IDS/IPS, EDR, son solo algunos de los componentes que hacen parte de un sistema compuesto que trabaja de forma colaborativa para la ciber protección de una organización. Dicho lo anterior, es natural que sea cada vez más necesario aumentar la inversión para la gestión de ciberseguridad. Según un informe realizado por la compañía Kaspersky, el promedio de presupuesto para la ciberseguridad a nivel global en pequeñas y medianas empresas en el año 2022 fue de 150 mil dólares con un pronóstico que indica que ese valor aumentará en 14% para el siguiente año (Kaspersky, 2022).

Las pequeñas y medianas empresas pueden tener múltiples motivos por los cuales deciden no invertir en tecnología. Algunos motivos pueden ser la falta de experiencia técnica para evaluar la tecnología que mejor se adapte a su negocio, la concentración en las tareas diarias o la incapacidad de distinguir la importancia de la tecnología como una necesidad empresarial crucial. Sin embargo, el factor económico podría ser el principal obstáculo debido a la falta de recursos financieros para invertir en tecnología, ya que en ocasiones esta puede ser costosa. No obstante, es importante que las pymes tengan una línea base que les permita responder fácilmente a áreas de vulnerabilidades, empezando con el entrenamiento básico de su personal en prácticas de ciberseguridad como no abrir correos electrónicos sospechosos o evitar ingresar a sitios web inseguros. En la inversión de ciberseguridad por parte de las pymes, es importante considerar medidas moderadas que estén acorde con los costos totales, incluyendo la adquisición, instalación, mantenimiento, actualizaciones y cualquier otro proceso necesario para garantizar la seguridad de los sistemas (Wang, 2019).

Con base en lo anterior, para esta investigación nos formulamos entonces la siguiente pregunta principal: ¿es viable utilizar herramientas de ciberseguridad de código abierto como alternativa a herramientas comerciales para la prevención de ciberataques en pequeñas y medianas empresas en Colombia? Por lo que nos abre paso a las siguientes preguntas secundarias:

- ¿Cuáles son las principales herramientas de ciberseguridad de código abierto que están disponibles en el mercado para la prevención y manejo de ciberataques?

- ¿Cuáles son las ventajas y desventajas de utilizar herramientas de ciberseguridad de código abierto en las pequeñas y medianas empresas en Colombia?

- ¿Qué recomendaciones y mejores prácticas se deben tener en cuenta en caso de optar por el uso de herramientas de ciberseguridad de código abierto en pequeñas y medianas empresas en Colombia?

El objetivo general de la investigación es analizar la implementación de herramientas de ciberseguridad de código abierto como una alternativa viable y efectiva a las soluciones comerciales para la prevención de ciberataques en pequeñas y medianas empresas en Colombia.

2. METODOLOGÍA O DESCRIPCIÓN DEL PROCESO

La metodología de investigación abordada en este estudio es descriptiva con un enfoque documental, pues este método de investigación abre paso a la necesidad que la información suministrada sea verídica, precisa y sistemática, además permite obtener datos variados, tanto cualitativos como cuantitativos (Guevara et al., 2020). De esta forma, para la metodología definiremos tres fases:

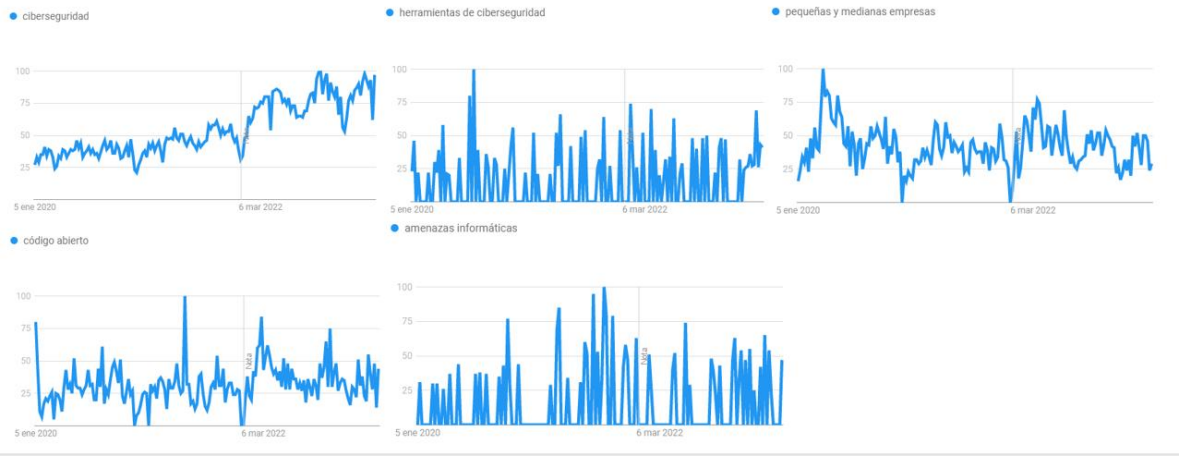
- Fase 1 - Principales herramientas de ciberseguridad: para esta fase se consultó documentación que permitió inicialmente abordar el concepto de ciberseguridad y los tipos de ataques más comunes en las organizaciones para así dar paso a definir las principales herramientas de ciberseguridad de código abierto usadas para prevenir dichos ataques siendo contrastadas con las herramientas comerciales disponibles.

- Fase 2 - Ventajas y desventajas de las herramientas de ciberseguridad de código abierto: en esta fase, mediante las principales herramientas definidas en la fase anterior, se identificaron las ventajas y desventajas más relevantes que deben considerar las pymes en cuanto al uso de estas, en comparación con las herramientas comerciales.

- Fase 3 - Recomendaciones para la implementación de herramientas de ciberseguridad de código abierto: con base en lo expuesto en las fases anteriores, se propuso una serie de recomendaciones que permiten una implementación efectiva para las pymes en Colombia con el fin de que las herramientas de ciberseguridad de código abierto puedan ser una opción para su ciber protección.

Las palabras clave para esta investigación fueron analizadas con la herramienta Google Trends como un apoyo visual en lo que respecta a su relevancia en los últimos tres años. Los resultados se pueden identificar en la Figura 1.

Figura 1
Resultados búsqueda palabras clave en Google Trends



Nota. Elaboración propia con apoyo de la herramienta Google Trends (2023).

Adicionalmente, se consultaron bases de datos tales como los motores de búsqueda Google Scholar y Semantic Scholar, la Red de Revistas Científicas de América Latina y el Caribe, España y Portugal (Redalyc), la biblioteca electrónica SciELO, el Directory of Open Access Journals, las bases de datos ScienceDirect e IEEE Xplore, entre otros sistemas de información.

En cuanto a los criterios de inclusión para la investigación, se establecieron los siguientes:

- Documentos publicados en los últimos 10 años.
- Documentos redactados en español y en inglés.
- Documentos que traten sobre código abierto y sobre herramientas de ciberseguridad.
- Documentos que aborden la problemática de la ciberseguridad en Colombia.
- Documentos que presenten recomendaciones o propuestas de soluciones para mejorar la ciberseguridad en pymes.
- Documentos provenientes de fuentes confiables como revistas científicas, tesis de posgrado o especializaciones, publicaciones gubernamentales y organizaciones especializadas en el tema.
- Portales y sitios web especializados en ciberseguridad y tecnología.

Con respecto a los criterios de exclusión, se establecieron los siguientes:

- Documentación que no aportara al tema de la ciberseguridad o la prevención de ciberataques
- Documentos que no se encontraron disponibles en línea
- Artículos o documentos que hayan requerido un pago para su acceso
- Documentación que no se encontrara en un formato digital
- Fuentes no confiables o sin respaldo científico o técnico.

Para el proceso de análisis de los documentos de la investigación, se hizo uso del siguiente documento de apoyo:


Plantilla análisis documental.xlsx

La columna con nombre "¿Por qué es útil el documento?" brinda la explicación acerca de la importancia de cada referencia para la investigación.

3. DESARROLLO DEL TEMA

3.1. Fase 1: Principales Herramientas de Ciberseguridad

En esta fase se revisó la respectiva documentación para entender la ciberseguridad, los tipos de ataques más comunes a pymes y qué herramientas de ciberseguridad comerciales y de código abierto existen para prevenirlos.

3.1.1. ¿Qué es la Ciberseguridad?

Con el fin de profundizar sobre las características de las herramientas de ciberseguridad, debemos tener claro el concepto de ciberseguridad. Fischer (2017) indica que "los componentes y dispositivos de las tecnologías de información y comunicación forman un sistema altamente independiente de redes, infraestructura y datos conocido como ciberespacio". La ciberseguridad es entonces ese conjunto de técnicas, medidas y procesos que se utilizan para proteger el ciberespacio contra cualquier tipo de amenaza que pueda comprometer la confidencialidad, integridad y disponibilidad del mismo. Esta disciplina ha ganado constantemente gran relevancia debido al incremento de la dependencia a las tecnologías de información y comunicación en todas las áreas del mundo moderno.

La ciberseguridad es cada vez más crucial para salvaguardar la información de los usuarios en el entorno digital debido a que la interconectividad de los sistemas informáticos crece de forma acelerada, lo que se traduce a un mayor riesgo de ataques cibernéticos. Tanto en pymes como en instituciones educativas, gubernamentales o multinacionales, es fundamental comprender la importancia de proteger los sistemas que contienen y gestionan los datos de estas organizaciones. Las ciberamenazas son cada vez más frecuentes y evolucionan constantemente. Estas pueden causar graves consecuencias en la privacidad y estabilidad financiera de las empresas independientemente de su tamaño o el sector de actividad.

Actualmente, el uso y adopción de tecnologías en pymes es visto como un indicador positivo de su desarrollo. Sin embargo, también genera un crecimiento en la superficie de ataque para los ciberdelincuentes, lo que aumenta las posibilidades de éxito en sus acciones y de adquirir notoriedad. La implementación de nueva infraestructura, dispositivos móviles y aplicaciones cloud implica nuevos riesgos de seguridad para las compañías (Ponemon Institute, 2016).

Las organizaciones deben tomar medidas preventivas y estar preparadas para hacer frente a los distintos tipos de ataques cibernéticos, los cuáles se pueden clasificar de múltiples formas como por ejemplo según los elementos de los activos informáticos que afecten, la capa de arquitectura

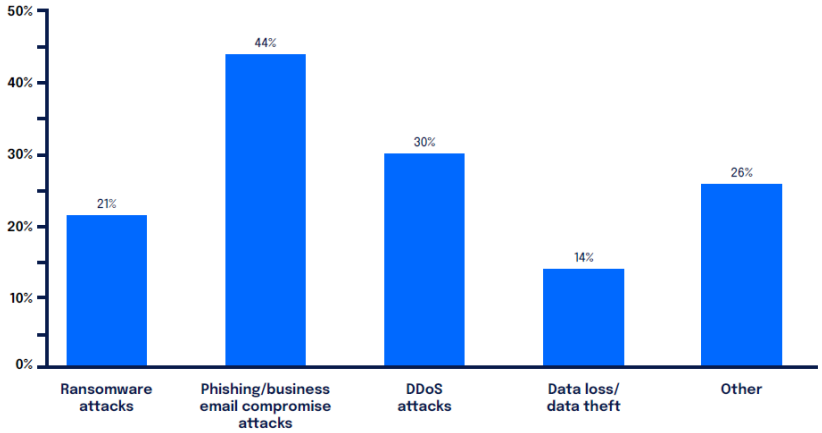
TCP/IP que afecten o según al componente del sistema que se vea impactado (Chinchilla y Sánchez, 2017).

3.1.2. ¿Qué ataques deben prevenir las herramientas de ciberseguridad?

En la Figura 2 se observan las principales brechas de seguridad experimentadas durante el año 2022 acorde a una encuesta realizada por la compañía Digital Ocean (2023) a más de 550 pymes.

Figura 2

Brechas de seguridad experimentadas durante 2022 por pymes



Nota. Tomado de Digital Ocean (2023).

Dentro de estos principales ataques, se encuentran:

- Ransomware: corresponde a un malware que cifra los datos de la organización, o parte de estos volviéndolos inutilizables para que de esta forma los ciberdelincuentes puedan obtener ganancias a través de la extorsión para remover la restricción (O'Kane et. al, 2018).
- Phishing: busca engañar a usuarios a través de técnicas de ingeniería social para adquirir información sensible (usuarios, contraseñas, etc.) tratando de persuadir a las personas mediante el envío de correos electrónicos conteniendo sitios web falsos con el único fin de capturar dicha información (Vayansky y Kumar, 2018).
- Ataques de denegación de servicio distribuidos (DDoS): buscan inhabilitar la continuidad de comunicación de los servicios a través de múltiples peticiones efectuadas al mismo tiempo desde diferentes lugares para así saturar el sistema e incapacitar el uso del mismo (Márquez, 2019).

Los tipos de ciberataques se encuentran en constante evolución. Anteriormente, las categorías utilizadas para catalogar los ataques informáticos eran menos variadas a las existentes en la actualidad. Los ciberdelincuentes han encontrado formas de estandarizar procesos de ataques para explotar las vulnerabilidades de los sistemas informáticos de manera más efectiva, accesible y rentable. Un ejemplo de esta evolución es el malware como servicio (MaaS), el cual permite realizar ataques de malware a gran escala y se compone de tres actores: el desarrollador, el vendedor y el comprador (Dimov, 2017), por lo que es una alternativa atractiva de los atacantes que busquen vulnerar principalmente ambientes corporativos.

3.1.3. Herramientas de Ciberseguridad

En términos generales, se recomienda integrar las medidas de protección prácticas disponibles para asegurar la efectividad de la seguridad informática. Una combinación cuidadosamente diseñada de diferentes herramientas puede generar sinergias que aumenten su eficacia. No obstante, una combinación inadecuada podría resultar contraproducente, puesto que la falla de una medida de protección puede dejar vulnerable a otra. Para una protección adecuada, los sistemas deben defenderse contra todas las formas relevantes de ataque y pueden emplear múltiples medidas de protección para cubrir diferentes tipos de amenazas (Wilson y Kiy, 2014).

Contar con un protocolo básico de ciberseguridad en pymes es igual de importante que para empresas con mayor tamaño. Definir los perfiles de usuarios, crear políticas de privacidad, establecer políticas de acceso a las instalaciones y otros de los procesos que hacen parte de este protocolo son clave para asegurar la información (Bustillos, O. y Rojas). Sin embargo, tener las herramientas adecuadas para la ciberseguridad es también parte importante dentro del proceso de aseguramiento de la información. Con el fin de velar por los sistemas informáticos de cualquier organización empresarial ante ciberamenazas, estas requieren de un sistema de seguridad que permita protegerlas. Este sistema de seguridad, como base, puede ser constatado por las siguientes herramientas: un firewall, un sistema de detección y prevención de intrusos y finalmente una solución de antivirus (Fakiha, 2022). Sin embargo, otras herramientas más avanzadas importantes a considerar son herramientas como Prevención de Pérdida de Datos (DLP), Detección y Respuesta de Endpoints (EDR) y herramientas de Gestión Unificada de Amenazas (UTM). Con base en lo anterior, dentro de los principales tipos de las herramientas de ciberseguridad se encuentran:

3.1.3.1. Firewall. Acorde a Stewart (2013) un firewall, es una herramienta que puede ser hardware o software que se encargue de ofrecer protección en una red para evitar el acceso a la misma de tráfico que no sea un origen autorizado. Estos dispositivos son usualmente posicionados en el borde de las redes para que funcione como una puerta de acceso con el fin de permitir o bloquear el ingreso o la salida del tráfico. La implementación de un firewall dentro de la infraestructura de una red corporativa es importante ya que permite proteger la red de amenazas externas, tener control sobre el tráfico de red, cumplir con regulaciones de seguridad de la información y proteger la privacidad de la organización.

Existen varios tipos de firewall que se encargan de cumplir diferentes objetivos:

- Firewall de host: son programas de seguridad que se ejecutan en un sistema operativo para controlar el tráfico del host específico.
- Firewall de aplicación: son programas que actúan como intermediarios entre una aplicación y el tráfico de red.
- Firewall de estado: monitorizan el estado de las conexiones de red y permiten o deniegan el tráfico dependiendo de la información de estado de la conexión.
- Firewall de próxima generación (NGFW): son firewall que utilizan tecnologías avanzadas de filtrado de paquetes, control de aplicaciones y prevención de intrusos para una

protección más eficaz contra las amenazas. También son llamados UTM (se tratará este concepto más adelante).

3.1.3.2. Sistema de Detección de Intrusos y Sistema de Prevención de Intrusos (IDS/IPS). Un Sistema de Detección de Intrusos (IDS) es un elemento de hardware o software que se encarga de automatizar la detección de intrusiones en sistemas informáticos y en redes. Tiene como principal función monitorizar los eventos que ocurren en sistemas o redes para identificar potenciales infracciones a las políticas de seguridad establecidas. Por el contrario, un Sistema de Prevención de Intrusos (IPS) es una tecnología que combina la detección de actividades o amenazas sospechosas con la toma de medidas preventivas para evitarlas. Este componente aprovecha la información recopilada por el IDS para detener y prevenir ataques de seguridad (Chakraborty, 2013). Por este motivo, ambas tecnologías se complementan entre sí, de esta forma pueden proporcionar una protección más completa para la red de una organización.

3.1.3.3. Antivirus. Un antivirus es un software usado para capturar y notificar código malicioso el cual, al mismo tiempo, dependiendo de la configuración que se haya realizado en este, ejecuta ciertos tipos de funciones que permiten asegurar el sistema tomando medidas preventivas, detectando el código malicioso y finalmente erradicándolo (Patil y Jadhav, 2014). El objetivo principal de un antivirus es la protección ante malware que puede infiltrarse en los sistemas operativos, además también puede incluir otras funciones de seguridad como firewall (para host), protección contra phishing y supervisión de vulnerabilidades. Por este motivo, es necesario que los equipos de una organización cuenten con una solución de antivirus para la protección de la red y la información.

3.1.3.4. Sistema de Prevención de Pérdida de Datos (DLP). Un sistema de prevención de pérdida de información permite analizar, monitorear, llevar trazabilidad, bloquear y proteger un gran rango de información, desde datos de usuarios, registros financieros, propiedad intelectual o cualquier otro tipo de información importante para una organización (Boranbayev et al., 2015). Las soluciones DLP usualmente monitorean el tráfico de red, dispositivos de almacenamiento, correo electrónico, endpoints y muchas otras fuentes de datos con el fin de detectar y prevenir la extracción de información sensible de las organizaciones.

3.1.3.5. Detección y Respuesta de Endpoints (EDR). Acorde al portal Check point (s.f.) el EDR es una integración que permite la protección de endpoints mediante la combinación del análisis de datos y el monitoreo constante en tiempo real para una respuesta automatizada de amenazas basada en reglas preestablecidas. Su función principal es brindar visibilidad y control en tiempo real sobre los diferentes endpoints como portátiles, equipos de escritorio, servidores, dispositivos móviles y otros endpoints para automatizar la detección y respuesta de amenazas. De esta manera, las organizaciones pueden monitorear proactivamente las actividades de los dispositivos finales. Adicionalmente, esta herramienta también tiene la capacidad de realizar análisis de seguridad forense para investigaciones posteriores.

3.1.3.6. Gestión Unificada de Amenazas (UTM). La Gestión Unificada de Amenazas es un conjunto de medidas que combina múltiples soluciones de seguridad en un único dispositivo o plataforma, lo cual permite una gestión centralizada de la ciberseguridad para la protección contra diversas amenazas en la red de una organización. Dentro de las soluciones de seguridad que

combina un UTM se puede incluir el servicio de firewall de red, detección y prevención de intrusiones, antivirus y antimalware, filtrado de contenido, servicio de VPN, anti-spam, servicios de prevención de fuga de datos y otras herramientas.

El portal de Juniper Networks (s.f.) indica que el dispositivo más factible para tener un rol de UTM es un firewall de próxima generación (NGFW) ya que estos tienen la capacidad de proveer múltiples elementos y servicios de seguridad en un solo dispositivo que se encuentre en la red, simplificando así la protección de los usuarios ante amenazas. Una de las ventajas principales de una solución UTM a través de un NGFW es que reduce los costos y la complejidad en comparación con usar múltiples soluciones de seguridad individuales. Adicionalmente, en vista de la centralización de los servicios, se puede tener una mejor visibilidad y control sobre las actividades en la red.

3.1.4. Herramientas de ciberseguridad comerciales

Son diferentes tipos de soluciones que se venden comercialmente a organizaciones y que pueden variar en cuanto a las necesidades que se tengan. Se venden mediante diferentes canales como tiendas en línea, distribuidores, fabricantes y proveedores de servicios de ciberseguridad. Existen múltiples opciones de herramientas de ciberseguridad comerciales en el mercado. La Tabla 1 describe algunas de las soluciones comerciales enfocadas en una línea base de seguridad para una empresa.

Tabla 1
Herramientas de ciberseguridad comerciales en el mercado

Tipo de herramienta	Fabricante	Herramienta
Firewall	Cisco	Adaptive Security Appliance
Firewall	Fortinet	FortiGate
Firewall	Palo Alto Networks	Next-Generation Firewall (NGFW)
Antivirus	Norton LifeLock	Norton Antivirus Plus
Antivirus	McAfee	McAfee Antivirus Plus
Antivirus	Kaspersky	Kaspersky Anti-virus
IDS/IPS	Cisco	Firepower (Módulo de NGFW)
IDS/IPS	McAfee	Network Security Platform
IDS/IPS	Trend Micro	TippingPoint

Nota. Elaboración propia.

Cabe notar que, si bien las herramientas previamente mencionadas pueden ser extremadamente valiosas para la protección de la información, el costo que requieren tiende a ser considerable además del costo adicional por su respectivo licenciamiento de uso. No obstante, el cliente (siendo la organización en este caso) estaría pagando este valor teniendo presente que es una herramienta brindada por una marca confiable que incorpora valor añadido como mayores niveles de seguridad y utilidad, avance continuo y una capacidad más factible de escalabilidad (Singh et al., 2015).

No obstante, en vista de que existen pymes que se encuentran poco a poco invirtiendo en su infraestructura tecnológica, en ocasiones pueden no tener el presupuesto suficiente para invertir en herramientas de ciberseguridad comerciales. Según el estudio previamente mencionado realizado por la compañía Digital Ocean (2023), el 40% de las más de 550 pymes que encuestaron indicaron que el costo de soluciones de ciberseguridad era el principal reto para el aseguramiento de su negocio. La problemática anterior, en conjunto con la subestimación de las amenazas cibernéticas por parte de las pymes puede convertirse en un inconveniente crítico, ya que esto da paso a un aumento en sus vulnerabilidades y riesgos (Alahmari y Duncan, 2020).

3.1.5. Herramientas de ciberseguridad de código abierto

El movimiento de código abierto ha tenido un impacto significativo en la reducción de los costos relacionados a implementaciones en los sistemas de las organizaciones. En la actualidad, ya son muchas las empresas que dependen del software de código abierto para soportar sus sistemas informáticos fundamentales como lo son las bases de datos, servidores web, servidores de correo, entre otros elementos (Coelho y Valente, 2017). Hay muchas herramientas de código abierto que son usadas en la cotidianidad como sistemas operativos (Linux), sistemas de control de versiones (Git), reproductores multimedia (VLC), lenguajes de programación (Python), etc.

En cuanto a la ciberseguridad, también existen múltiples herramientas de código abierto que pueden ser implementadas. A continuación, se dará una descripción y análisis acerca de las principales herramientas de este tipo que pueden ser usadas en infraestructuras de pymes tomando una línea base de ciberseguridad.

3.1.5.1. pfSense (Firewall). Es un firewall de código abierto basado en el sistema operativo FreeBSD. Es basado sobre este sistema operativo por sobre OpenBSD principalmente por su mejoría con tecnologías de redes inalámbricas y de rendimiento. Adicionalmente, este sistema operativo brinda mayor escalabilidad debido a que soporta multiprocesamiento. Además de contar con diferentes servicios útiles para la red (como enrutamiento), su contribución para mejorar la ciberseguridad de una pyme puede definirse en las siguientes funcionalidades:

- Firewall: pfSense tiene un componente de firewall avanzado que puede proteger la red contra tráfico no deseado, incluyendo ataques de hackers, malware, virus y spam. El firewall es altamente configurable y puede bloquear o permitir tráfico basado en una variedad de criterios, como la dirección IP de origen y destino, el puerto utilizado y el protocolo de comunicación.
- VPN: incluye soporte para VPN (redes privadas virtuales), que pueden ser utilizadas para cifrar y proteger el tráfico de red a través de Internet. De esta forma, los trabajadores pueden acceder de manera segura a la red de la empresa desde ubicaciones remotas, lo que es especialmente útil en el contexto de la creciente tendencia de trabajo remoto.
- Túneles seguros: cuenta con la capacidad de comunicar diferentes redes privadas mediante túneles sitio-a-sitio seguros, ideal para la conexión cifrada entre redes ubicadas en diferentes partes del mundo.
- Integraciones: posee la capacidad de fácil integración con otras herramientas de código abierto (IDS/IPS, monitoreo de red, etc.).

- Seguridad de la capa de aplicación: esta herramienta incluye varios servicios de seguridad de la capa de aplicación que pueden ser utilizados para proteger servicios y aplicaciones específicas, como servidores web, proxy inverso, filtrado de contenido, filtro de correo electrónico, control de acceso, prevención de ataques DDoS autenticación y cifrado.

La Tabla 2 describe los tipos de despliegue de la herramienta.

Tabla 2
Tipos de despliegue pfSense

Tipo de despliegue	Descripción
Hardware	Puede instalarse en hardware dedicado exclusivamente para alojar el servicio. La plataforma Netgate maneja múltiples soluciones de pfSense en hardware
Máquina Virtual	Puede implementarse en una máquina virtual como VMWare o VirtualBox descargando la imagen oficial desde el sitio web
Cloud	Se puede implementar en plataformas como AWS, Azure y GCP
Contenedor	Puede implementarse en un contenedor a través de la herramienta Docker

Nota. Elaboración propia.

Esta herramienta cuenta con varias ventajas en su uso para una pyme: es gratuita, por lo que no hay costos de licencias o actualizaciones; es altamente personalizable por lo que se puede ajustar a las necesidades específicas de la organización; tiene gran flexibilidad al poder ser implementada en hardware dedicado, máquinas virtuales o entornos cloud; incluye un conjunto completo de características de seguridad como firewall de red, VPN y protección de contenido web. No obstante, también tiene algunas desventajas que se deben tener en presente: no cuenta con soporte oficial disponible y se depende altamente de la comunidad en línea para resolución de problemas; requiere de conocimientos técnicos para su administración; si bien puede ser ejecutado en hardware dedicado, los requisitos del mismo pueden ser exigentes; puede ser difícil de integrar con ciertos sistemas de terceros en caso de necesitarse en la red.

3.1.5.2. Endian Firewall Community (Firewall). Es un firewall basado en el sistema operativo Linux que requiere de bajos recursos para su funcionamiento, ya que puede trabajar cómo una solución UTM en dispositivos hardware con pocas capacidades de rendimiento. Si bien esta herramienta tiene como objetivo principal brindar una capa de seguridad para redes de hogar, una pequeña organización que no requiera de alta robustez puede hacer uso de la misma ya que provee las siguientes funcionalidades principales:

- Seguridad de correo y web: cuenta con servicios básicos de seguridad web y de correo a través de aplicaciones de código abierto.
- Acceso remoto seguro: mediante la VPN integrada se puede realizar la conexión desde cualquier lugar. Adicionalmente, permite interconectar diferentes sitios mediante un túnel.
- Monitoreo y reporte en tiempo real: permite tener una visualización de la red en tiempo real para gestión de reportes.

- Manejo de eventos: tiene la capacidad de notificar mediante correo electrónico una serie de eventos predefinidos del sistema.
- Firewall de estado: controla el acceso a los recursos dentro de la red.
- Prevención de intrusos: analizar el flujo del tráfico para proteger la red de amenazas internas y externas.

Esta herramienta puede trabajar en sistemas x86 y x64 como portátiles y servidores. Es compatible con Windows, Linux y macOS, por lo que mediante la imagen ISO obtenida del sitio web oficial, se puede hacer la instalación del servicio en hardware o máquinas virtuales con alguno de los sistemas operativos mencionados.

Dentro de las principales ventajas en su uso para una pyme se encuentran: tiene varias funciones de seguridad como filtrado web, protección ante intrusiones, VPN y otros servicios; posee una interfaz web de fácil manejo; ofrece actualizaciones automáticas de seguridad; cuenta con una amplia comunidad de usuarios en línea para soporte de problemas; al ser basada en código abierto, es altamente personalizable. En cuanto a las desventajas principales se encuentran: puede ser complejo de configurar y mantener; su versión gratuita tiene limitaciones en funcionalidades; depende en gran medida de la comunidad para el desarrollo y el soporte técnico.

3.1.5.3. Snort (IDS/IPS). Snort es un sistema de detección y prevención de intrusos de red de código abierto desarrollado por Cisco. Sus principales funcionalidades son realizar análisis de protocolos y registrar paquetes dentro de las redes. Adicionalmente, también tiene la capacidad de búsqueda y matching de contenido, así como detectar diferentes tipos de ataques de red. La detección de intrusiones se ejecuta comparando los patrones en el tráfico de la red mediante una base de datos de reglas previamente definidas. De la misma forma, también cuenta con una serie de reglas establecidas para responder ante cualquier tráfico malicioso y de esta forma prevenir ataques. Esta herramienta ha sido ampliamente usada y gran parte de las otras herramientas de detección y prevención de intrusos usan Snort como su motor base.

Para su implementación dentro de una pyme, esta herramienta puede ser instalada como servicio en sistemas operativos como Linux, Windows, macOS, entre otros. Sin embargo, gran parte de los administradores de red prefieren realizar la instalación en sistemas Linux como Ubuntu, Debian, CentOS o Red Hat debido a que ofrecen una gran estabilidad, seguridad y flexibilidad, además de la fácil integración con estos sistemas. Con base en lo anterior, se debe tener en cuenta que es recomendable instalar esta herramienta en una máquina que cuente con un mínimo de 2 núcleos de CPU y al menos 4GB de memoria RAM, sin embargo, estos valores tendrán que variar dependiendo de la cantidad de tráfico que fluya en la red. Adicionalmente, las consideraciones a nivel de almacenamiento, también deben ser evaluadas con base a la cantidad de logs que se deseen manejar dentro de la organización.

Algunas de las principales ventajas de usar esta herramienta en un ambiente de pyme son: puede detectar una gran variedad de amenazas como ataques DoS, backdoors, escaneos de puertos, etc.; es altamente personalizable y se puede adaptar a las necesidades específicas de las organizaciones; sus reglas son actualizadas regularmente por la comunidad para detectar nuevas amenazas; al ser de código abierto no requiere de una suscripción o pago para su uso; tiene una gran versatilidad en integraciones con otras herramientas de ciberseguridad.

Con respecto a algunas de sus desventajas pueden ser: para su configuración inicial y gestión se requieren los conocimientos técnicos adecuados para su correcto funcionamiento; tiene la posibilidad de generar gran cantidad de alertas falsas aumentando la carga laboral para el personal de seguridad; a pesar de su comunidad activa, no cuenta con un soporte oficial lo que puede limitar las actualizaciones y parches de seguridad; puede presentar dificultades para detectar ataques sofisticados que usen técnicas avanzadas; para su implementación en infraestructuras grandes, requiere de un hardware potente para soportar la carga del procesamiento de análisis de tráfico.

3.1.5.4. Suricata (IDS/IPS). Suricata es una herramienta de detección y prevención de intrusiones de red de código abierto. Esta herramienta fue creada basada en la infraestructura de Snort, ya que gracias a la naturaleza de código abierto de Snort, se permitió el desarrollo de una herramienta IDS/IPS mejorada que tuviera la posibilidad de aprovechar las capacidades computacionales de las máquinas actuales (Fekolkin, 2015). En vista de que previamente se describió el funcionamiento de Snort, a continuación, se describen las principales diferencias entre estas dos herramientas:

- Arquitectura: La arquitectura de Snort es de un solo hilo, por lo que únicamente procesa un paquete a la vez, mientras que Suricata está diseñado para procesar múltiples paquetes de forma simultánea.
- Protocolos: Suricata admite nativamente protocolos cómo HTTP, FTP, SMTP, SSH, entre otros, mientras que Snort se centra en protocolos TCP, UDP e ICMP.
- Rendimiento: Suricata cuenta con mayor capacidad para procesamiento de tráfico y posee más escalabilidad que Snort. Por este mismo motivo, Suricata requiere de mayor disposición de recursos (CPU, RAM, etc.) para su óptimo funcionamiento.

3.1.5.5. ClamAV (Antivirus). Es una herramienta de código abierto que permite la detección de malware en diferentes sistemas operativos. Su funcionamiento se basa en el análisis y comparación de archivos y directorios con una base de datos de firmas actualizadas brindada por Cisco para detectar cualquier malware o amenaza. Esta solución es popularmente usada en servidores de correo electrónico, sistemas de archivos de red y servidores web. Puede ser implementada en sistemas operativos como Ubuntu, Debian, Fedora, CentOS, entre otros. Además, puede ser instalado en sistemas operativos Windows para estaciones de trabajo y servidores.

Para su instalación en una máquina, esta debe contar mínimamente con 4 Gb de memoria RAM, una CPU de 2.0 Ghz y 5 Gb de espacio en disco para los archivos del aplicativo.

En su sitio web, brindan la posibilidad de compartir archivos potencialmente maliciosos que ClamAV no haya detectado en su base de datos y también permiten trabajar con firmas creadas por miembros de la comunidad para expandir la detección conjunta de amenazas. A pesar de no contar con soporte técnico oficial, los creadores proporcionan unas listas de correo gestionadas por la misma comunidad en la que se brinda asistencia a través de cadenas de mensajes mediante la suscripción al correo.

Las ventajas principales de usar esta herramienta dentro de una pyme pueden ser: al ser de código abierto, permite una gran personalización para ser acoplada a las necesidades específicas; es una herramienta gratuita, ideal para presupuestos limitados; gracias a su constante actualización de base de datos de firmas tiene una tasa de detección alta de malware, es compatible con múltiples sistemas operativos; cuenta con una gran capacidad de integración con otras herramientas de seguridad.

Con respecto a las desventajas, se pueden encontrar las siguientes: al ser gratuita, no cuenta con los mismos recursos financieros de herramientas comerciales por lo que no es tan eficiente como una herramienta paga; la protección en tiempo real únicamente es para sistemas basados en Linux; no cuenta con soporte técnico oficial; puede tener altas tasas de falso positivo, identificando archivos inofensivos como malware lo que requiere intervención humana; puede ser difícil de configurar y requiere altos conocimientos técnicos desde su instalación.

3.2. Fase 2: Ventajas y desventajas del uso de herramientas de ciberseguridad de código abierto en comparación con herramientas comerciales

Habiendo definido las principales herramientas de ciberseguridad de código abierto investigadas y sus principales ventajas y desventajas específicas de uso, en la Tabla 3 se presenta una comparativa acerca de las ventajas y desventajas de estas herramientas con respecto a las herramientas comerciales.

Tabla 3
Comparación herramientas de código abierto con herramientas comerciales

Aspecto	**Herramientas de ciberseguridad de código abierto**	**Herramientas de ciberseguridad comerciales**
Costo	Generalmente gratuitas o de bajo costo	Pueden tener costos significativos por licencias y de renovación
Personalización	Altamente personalizables y permiten modificar el código acorde a las necesidades	No siempre es posible personalizar o modificar el software
Soporte	Depende de la comunidad de usuarios, foros y comunidades en línea	Suelen tener soporte dedicado y asistencia técnica especializada
Facilidad de uso	Pueden tener una curva de aprendizaje considerable y requerir habilidades técnicas avanzadas para su uso	Poseen usualmente una interfaz de fácil uso y requerir menos habilidades técnicas específicas para configurar
Compatibilidad	Pueden presentar problemas de compatibilidad con programas o sistemas	Cuenta con alta compatibilidad con una amplia gama de sistemas
Documentación	Tiene una gran variación con respecto a la cantidad y la calidad en la que se encuentra	Presentan documentación detallada y específica

Innovación	Son una fuente de innovación constante con actualizaciones regulares y contribuciones de la comunidad	Pueden ser más lentas para adoptar nuevas tecnologías e innovaciones
Escalabilidad	Pueden ser menos escalables para grandes empresas y entornos robustos	Usualmente son especialmente diseñadas para escalabilidad en entornos empresariales

*Nota***.** Elaboración propia.

3.3. Fase 3: Recomendaciones para la implementación de herramientas de ciberseguridad de código abierto

Acorde a lo mencionado en la metodología de investigación, en esta fase se presentarán algunas recomendaciones o sugerencias para la implementación de herramientas de seguridad de código abierto para pymes en el país de Colombia con base en las herramientas que fueron analizadas en el documento.

3.3.1. Recomendación a nivel de firewall

La consideración principal entre usar la herramienta pfSense o Endian Firewall Community dependerá de la cantidad de usuarios y la robustez de la red de la pyme. La herramienta Endian puede ser más efectiva para pymes con menos cantidad de usuarios y para una configuración más básica, mientas que pfSense puede ser altamente escalable y cuenta con funcionalidades avanzadas adicionales al igual que mayor integración con otras herramientas de código abierto.

3.3.2. Recomendación a nivel de IDS/IPS

Acorde a las principales diferencias mencionadas entre las herramientas de Snort y Suricata, la primera sería más apropiada para un entorno simple, con una carga de red baja y dónde no se tenga la necesidad de implementar configuraciones avanzadas. Aunque Suricata también puede trabajar eficazmente en entornos de baja carga, ofrece un mejor rendimiento para ambientes más densos debido a su capacidad de procesamiento multinúcleo y soporte para más protocolos, por lo que debe tenerse a disposición mayores recursos para su implementación.

3.3.3. Recomendación a nivel de antivirus

En la investigación realizada, ClamAV fue la única herramienta encontrada como antivirus de código abierto que también trabajara en el sistema operativo Windows, siendo el sistema más usado para dispositivos finales corporativos. Esta herramienta aporta un nivel básico de seguridad, sin embargo, siendo complementada con alguna de las herramientas previamente mencionadas, principalmente con un IPS, permitirá detectar y bloquear posibles amenazas a nivel de red. También cuenta con integraciones para seguridad de correo electrónico mediante un sistema de filtrado como Postfix o Sendmail.

3.3.4. Recomendaciones generales para otras herramientas de ciberseguridad de código abierto

En la investigación, se analizaron ciertas herramientas específicas de código abierto acorde a los criterios definidos. Sin embargo, existen muchas otras herramientas que pueden ser implementadas en pymes para aportar a su ciberseguridad. A continuación, se presentan algunas de las recomendaciones generales para la implementación de este tipo de herramientas que pueden ser de gran utilidad:

- La mayoría de herramientas de código abierto requieren de un conocimiento técnico considerable (línea de comandos, sistemas operativos, administración de servidores, conocimientos de red y seguridad, etc.). Por esto, se sugiere contar con personal capacitado (o con la capacidad de aprender) y dedicado a la implementación y administración de las herramientas de código abierto.
- En vista de que existen numerosas herramientas que pueden abarcar el mismo objetivo, se sugiere consultar e indagar en las diferentes opciones para realizar una comparación y así encontrar la que mejor se adapte a las necesidades de la empresa.
- El mantenimiento y supervisión de las herramientas de código abierto no suele ser automático como en muchas de las herramientas comerciales. Por esto, se recomienda estar altamente atentos en mantener las herramientas de ciberseguridad actualizadas y configuradas adecuadamente para garantizar la protección continua de la pyme.

4. CONCLUSIONES

Se puede concluir que la viabilidad en cuanto a la implementación de herramientas de ciberseguridad de código abierto puede ser una opción efectiva para pymes en Colombia que requieran de soluciones tecnológicas que tengan la capacidad de brindar una capa de protección en la infraestructura de forma básica y que no requiera de altos costos para su debida gestión y administración. Estas herramientas son una buena opción para una solución inicial y pueden dar paso al cambio a herramientas comerciales dedicadas a medida que la organización crece.

Cuando se requiere de configuraciones o ajustes específicos que necesite la pyme a nivel de seguridad, es posible que las herramientas comerciales no sean capaces de satisfacer sus necesidades específicas. Por lo tanto, en estos casos, las herramientas de ciberseguridad de código abierto son viables y necesarias, aunque se requiere de un conocimiento técnico especializado para llevar a cabo su implementación.

La oferta de herramientas de ciberseguridad disponibles en el mercado, tanto comerciales como de código abierto es muy variada y amplia. En estas se incluyen los firewalls, antivirus, sistemas de detección y prevención de intrusiones, sistemas de prevención de fuga de datos, sistemas de respuesta ante incidentes, entre otras. Por esta razón, es esencial que las pymes tengan una comprensión clara de los objetivos y del presupuesto que se destina a su ciberseguridad, así como de los tipos de ataques cibernéticos a los que puedan estar más expuestos, para establecer una estrategia y seleccionar las herramientas adecuadas a sus necesidades específicas.

La definición de una línea base en términos de herramientas de ciberseguridad puede variar. No obstante, para una pyme, contar mínimamente con un firewall para la protección perimetral, un antivirus para la protección de equipos de cómputo y un sistema de detección y prevención de intrusos para la protección de la red interna puede ser una sólida estructura.

Las pymes pueden obtener diversos beneficios al utilizar herramientas de ciberseguridad de código abierto. Estas herramientas suelen ser de bajo costo o gratuitas, lo que las hace más asequibles para empresas con presupuestos limitados. Además, son altamente adaptables, lo que permite ajustarlas según las necesidades específicas de cada organización.

Aunque las herramientas de ciberseguridad de código abierto son más económicas que las herramientas comerciales, carecen de algunas de las funcionalidades que ofrecen estas últimas, como brindar soporte especializado por parte de los fabricantes, una interfaz más fácil de usar e intuitiva en muchos casos y una mayor capacidad de escalabilidad para entornos empresariales complejos.

Es crucial considerar ciertos aspectos importantes al implementar tanto las herramientas específicas investigadas (pfSense, Endian, Snort, Suricata y ClamAV) como cualquier otra herramienta de ciberseguridad de código abierto, tales como comparar y evaluar diferentes opciones para elegir la que mejor se adapte a las necesidades de la pyme, y contar con personal capacitado para manejar y administrar adecuadamente estas herramientas.

Luego de realizar el respectivo análisis de las herramientas, se ha determinado que la cantidad de opciones de antivirus de código abierto para sistemas operativos Windows es limitada. Por este motivo, ClamAV se ha presentado como una opción viable y altamente efectiva que puede ser integrada con otras herramientas disponibles.

5. REFERENCIAS

Alahmari, A. y Duncan, B. (15-19 de junio de 2020). *Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence*. 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA), Dublin, Ireland. https://doi.org/10.1109/CyberSA49311.2020.9139638

Boranbayev, A., Mazhitov, M. y Kakhanov, K. (13-15 de abril de 2015). *Implementation of Security Systems for Prevention of Loss of Information at Organizations of Higher Education*. 2015 12th International Conference on Information Technology-New Generations, Las Vegas, NV, USA.

Bustillos, O. y Rojas, O. (2022). Protocolo básico de Ciberseguridad para Pymes. *Interfases, 16*(016), 168-186. https://doi.org/10.26439/interfases2022.n016.6021

Cámara Colombiana de Informática y Telecomunicaciones. (2021). *Tendencias del Cibercrimen 2021-2022 Nuevas Amenazas al Comercio Electrónico.* https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf

Chakraborty, N. (2013). Intrusion Detection System and Intrusion Prevention System: A Comparative Study. *International Journal of Computing and Business Research (IJCBR), 4*(2). http://researchmanuscripts.com/May2013/1.pdf

Check point. (s.f). *¿Qué es la detección y la respuesta de endpoint (EDR)?* https://www.checkpoint.com/es/cyber-hub/what-is-endpoint-detection-and-response/

Chinchilla, E. J. y Sánchez, J. (2017). Riesgos de Ciberseguridad en las Empresas. *Revista Tecnologí@ y desarrollo Revista de Ciencia, Tecnología y Medio Ambiente*, *15*, 1-33. https://revistas.uax.es/index.php/tec_des/article/view/1174/964

Cisco. (s.f). *What Is Cybersecurity?* https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Coelho, J. y Valente, M. T. (21 de agosto de 2017). *Why Modern Open Source Projects Fail*. Proceedings of the 2017 11th Joint meeting on foundations of software engineering, 186-196. doi:https://doi.org/10.1145/3106237.3106246

Digital Ocean. (2023). *Small Businesses and Cybersecurity: How startups and SMBs are viewing security threats in 2023.* https://anchor.digitalocean.com/rs/113-DTN-266/images/Security-Report_DigitalOcean.pdf?mkt_tok=MTEzLURUTi0yNjYAAAGKx5z_ZPYAC-86Rzqj2H8M5CcpHbripszTaynvLi2kXVlcELdKklw7mS0mGPb8wSRtXMcKXZ4Jj6Ji8hZojNgAnDSayB6B7yErQpV8HEyf0k37

Dimov, D. (05 de junio de 2017). *Malware-as-a-service.* Infosec. https://resources.infosecinstitute.com/topic/malware-as-a-service/

Fakiha, B. (2022). Ciberseguridad: análisis y aplicación de la herramienta forense ProDiscover. *Medicina Social*, *15*(3), 142-148. https://www.socialmedicine.info/index.php/medicinasocial/article/view/1369

Fekolkin, R. (6 de enero de 2015). Intrusion Detection and Prevention Systems: Overview of Snort and Suricata. Internet Security, A7011N, Lulea University of Technology, 1. https://www.academia.edu/10341899/Intrusion_Detection_and_Prevention_Systems_Overview_of_Snort_and_Suricata

Fischer, E. (2017). *Cybersecurity Issues and Challenges.* Library of congress Washington dc.

Forbes. (08 de diciembre de 2022). *El 57% de las pymes europeas cierran a causa de los ciberataques.* https://www.forbes.com.mx/el-57-de-las-pymes-europeas-cierran-a-causa-de-los-ciberataques/

Guevara, G., Verdesoto, A. y Castro, N. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas y de investigación-acción). *RECIMUNDO:*

Revista Científica de la Investigación y el Conocimiento, 4(3), 163-173. https://dialnet.unirioja.es/servlet/articulo?codigo=7591592

Juniper Networks. (s.f.). *What is unified threat management?* https://www.juniper.net/us/en/research-topics/what-is-utm.html

Kaspersky. (s.f). *El ransomware: qué es, cómo se lo evita, cómo se elimina*. https://latam.kaspersky.com/resource-center/threats/ransomware

Kaspersky. (2022). *ITSecurity Economics 2022 Executive Summary.* https://go.kaspersky.com/rs/802-IJN-240/images/IT%20Security%20Economics%202022_report.pdf

Lumu. (Diciembre de 2022). *Alerta para organizaciones colombianas: Cómo enfrentar la dura realidad del estado de ransomware del país.* https://lumu.io/wp-content/uploads/2022/12/lumu-alerta-para-organizaciones-colombianas.pdf

Márquez, J. (2019). Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas. *Revista de Bioética y Derecho,* (46), 85-100. https://scielo.isciii.es/scielo.php?script=sci_abstract&pid=S1886-58872019000200006

O'Kane, P., Sezer, S. y Domhnall, C. (2018). Evolution of Ransomware. *IET Networks, 7(5)*, 321-327. https://doi.org/10.1049/iet-net.2017.0207

Patil, B. y Jadhav, R. (2014). Computer Virus and Antivirus Software - A Brief Review. *International Journal of Advances in Management and Economics, 4*(2), 1-4. https://www.managementjournal.info/index.php/IJAME/article/view/408

Ponemon Institute. (2016). *2016 State of Cybersecurity in Small and Medium-sized Businesses.* https://www.keepersecurity.com/assets/pdf/The_2016_State_of_SMB_Cybersecurity_Research_by_Keeper_and_Ponemon.pdf

Rea-Guaman, Á. M., Sánchez-García, I. D., San Feliu Gilabert, T. y Calvo-Manzano, J. A. (21-24 de junio de 2017). *Modelo de maduréz en ciberseguridad: una revisión sistemática.* 12ª Conferencia Ibéricas de Sistemas y Tecnologías de la Información, Lisboa, Portugal.

Singh, A., Bansal, R. y Jha, N. (2015). Open Source Software vs Propietary Software. *International Journal of Computer Applications, 114*(18), 26-31. https://www.ijcaonline.org/archives/volume114/number18/20080-2132

Stewart, J. M. (2013). *Network Security, Firewalls and VPNs.* 2a ed. Jones & Bartlett Publishers.

Vayansky, I., y Kumar, S. (2018). Phishing - challenges and solutions. *Computer Fraud & Security*, (1), 5-20. http://dx.doi.org/10.1016/S1361-3723(18)30007-1

Wang, S. (2019). Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal*, 57. https://doi.org/10.1016/j.pacfin.2019.101173

Wilson, K., y Kiy, M. A. (2014). Some Fundamentals Cybersecurity Concepts. *IEEE access*, *2*, 116-124. https://doi.org/10.1109/ACCESS.2014.2305658