REVISTA ODIGOS

Período octubre - enero 2023
Vol. 4, Núm. 3
rodigos@uisrael.edu.ec
https://doi.org/10.35290/ro.v4n3.2023.918 • e-ISSN: 2697-3405

Uso de dispositivos de bajo costo como alternativa para la implementación de IDS en las pymes

Use of low-cost devices as an alternative for the implementation of IDS in PYMEs

Fecha de recepción: 2023-04-24 • Fecha de aceptación: 2023-08-17 • Fecha de publicación: 2023-10-10

Edgar Mauricio Lopez Rojas[1]
Universidad Nacional Abierta y a Distancia & Universidad Americana de Europa, Colombia
Edgar.lopez@unad.edu.co
https://orcid.org/0000-0002-4957-8917

Alexander Larrahondo Núñez[2]
Universidad Nacional Abierta y a Distancia, Colombia
Alexander.larrahondo@unad.edu.co
https://orcid.org/0000-0001-9350-6403

Rosa Gabriela Camero Berrones[3]
Universidad Americana de Europa, México
rosagabriela.camero@aulagrupo.es
https://orcid.org/0000-0003-4438-1645

Anderson Fabian Ferrucho Pérez[4]
Universidad Nacional Abierta y a Distancia, Colombia
afferruchop@unadvirtual.edu.co
https://orcid.org/0000-0002-4660-1886

RESUMEN

Las pequeñas y medianas empresas, comúnmente llamadas pymes, tienen la necesidad de contar con herramientas tecnológicas que apoyen la ciberseguridad en sus procesos brindando un grado de confianza a sus socios comerciales, los cuales las incluyen en su cadena de suministros como elementos claves en el desarrollo de sus productos y servicios. Entre algunos de los problemas que estas tienen se puede mencionar la falta de conciencia en ciberseguridad, falta de presupuesto para realizar inversiones en tecnología y ciberseguridad, lo que las coloca en desventaja frente a las grandes multinacionales que asignan un buen porcentaje de presupuesto a tecnología y ciberseguridad. Es por eso que el uso de sistemas de detección de intrusos basados en código abierto, implementados en dispositivos de bajo costo o de placa simple, se convierte en una excelente alternativa tecnológica, con las mismas características, servicios y ventajas de un sistema de detección de intrusos comercial, reduciendo la desigualdad tecnológica que afecta el desarrollo comercial y económico de las pymes.

PALABRAS CLAVE: dispositivo de seguridad, seguridad, informática y desarrollo, pequeña empresa, red informática

ABSTRACT

Small and medium-sized enterprises, commonly known as SMEs, need to have technological tools that support cybersecurity in their processes, providing a degree of confidence to their business partners, who include them in their supply chain as key elements in the development of their products and services. Among some of the problems they face are the lack of cybersecurity awareness, lack of budget to invest in technology and cybersecurity, which puts them at a disadvantage compared to large multinationals that allocate a good percentage of their budget to technology and cybersecurity. That is why the use of intrusion detection systems based on open source, implemented in low-cost or single-board devices, becomes an excellent technological alternative, with the same features, services and advantages of a commercial intrusion detection system, reducing the technological inequality that affects the commercial and economic development of SMEs.

KEYWORDS: security appliance, security, IT and development, small business, computer networking

Introducción

Según la ANIF (2020) las pymes juegan un papel fundamental en la economía de Colombia, representando el 99% de las empresas del país, generando el 79% del empleado a nivel nacional y aportan el 40% del producto interno bruto. Esto a su vez parte de la cadena de suministros de grandes y multinacionales empresas, desconociendo estas que por su reducido tamaño de operación asumen que no son objetivos de ataques de ciberseguridad (Organización de Estados Americanos, 2018), y, sin quererlo, pueden ser utilizadas por los ciberdelincuentes para llegar a las grandes empresas al formar parte de su cadena de suministros (Marín y Carvajal, 2018; Franco y Urbano, 2019).

Es claro que, para las organizaciones, sin importar su tipo, necesitan tener en cuenta e incluir en sus procesos seguridad informática, ya sea usando herramientas comerciales o de código libre que les permitan mejorar sus posturas de seguridad en todos sus procesos y que les ayuden a identificar posibles amenazas que se pueden convertir en incidentes que a su vez ocasionen afectaciones en las operaciones, finanzas y afectando la credibilidad y el buen nombre de las compañías afectadas.

Al centrarse en las herramientas de código abierto especializadas en seguridad informática y que apoyen la seguridad perimetral de las organizaciones, es posible implementarlas en dispositivo de bajo costo o de placa simple del inglés *Single Board Computers* (SMB), a pesar de que son dispositivos de tamaño reducido cuentan con recursos y características lo suficientemente robustas para permitir su utilización en la implementación de esta clase de herramientas.

Entonces resulta posible el funcionamiento de herramientas especializadas de seguridad informática en entornos tecnológicos, de pequeñas y medianas empresas (Mintic, 2018a), dándoles un nivel de seguridad base y entregándoles visibilidad de los diferentes eventos anormales a los que están expuestas en sus actividades y procesos diarios.

Metodología

Para el desarrollo de la investigación se utilizó el método bibliográfico comparativo, se procedió a consultar literatura sobre el estado actual de la seguridad informática de las pequeñas y medianas empresas –pymes–, como lo son artículos de investigación, encuestas gubernamentales, encuestas del gremio, tesis, entre otros documentos, permitiendo identificar las tendencias de las pymes en sus procesos de tecnología y seguridad informática que apoyan sus procesos misionales y los diferentes incidentes o ataques cibernéticos a los que están expuestas por no contar con adecuadas herramientas o buenas prácticas de seguridad informática.

Basado en esto se orientaron los siguientes pasos o etapas para contemplar todos los aspectos necesarios que se consideran relevantes dentro de la investigación:

- Revisión del estado de la ciberseguridad de las pequeñas y medianas empresas mediante una investigación documental y una recopilación preliminar de datos a partir de encuestas a pymes de Colombia.
- Identificar las arquitecturas tecnológicas más usadas por las pequeñas y medianas empresas en Colombia.
- Analizar los servicios que utilizan y los diferentes problemas de seguridad que pueden causar incidentes de seguridad que posteriormente se vuelvan intrusiones.
- Comparar los diferentes IDS de código abierto que se puedan implementar en un dispositivo Raspberry (Tripathi & Kumar, 2018; Zitta et al., 2017).
- Evaluar y documentar diferentes procedimientos de instalación de sistemas de detección de intrusos, inicialmente en máquinas virtuales implementadas con herramientas de virtualización como VMware player.

2.1 Conceptos generales

Según Vieites (2011) se considera una amenaza a cualquier evento intencional o accidental que resulte en el daño parcial o total de un componente o servicio informático.

Una vulnerabilidad es un fallo, ya sea mal intencionado o no, que tienen los servicios y dispositivos dentro de una infraestructura de TI y el riesgo es la probabilidad que la amenaza explote una vulnerabilidad y logre ocasionar daños en una infraestructura tecnológica, generando alto impacto en la organización.

Para Ortega (2022) un sistema de detección de intrusos es un dispositivo incorporado dentro de una red LAN, cuya función es informar y alertar sobre anomalías internas o externas que pueden afectar el correcto funcionamiento de una infraestructura tecnológica ocasionando serios problemas en su funcionamiento y procesos.

Raspberry son los más conocidos dispositivos de placa simple o de bajo costo que han cambiado el concepto de los computadores, sus usos y aplicaciones, siendo un computador del tamaño de una tarjeta plástica de un banco con grandes capacidades y usos en diferentes campos y especialidades.

Resultados

3.1 Revisión del estado de la ciberseguridad de las pequeñas y medianas empresas mediante una investigación documental y una recopilación preliminar de datos a partir de encuestas a PYMES de Bogotá

Según un informe publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) de Colombia en 2019, el 53% de las pymes en esa Nación habían adoptado tecnologías digitales. Entre las tecnologías más utilizadas estaban el correo electrónico (90%), la página web (44%) y las redes sociales (35%).

Además, en 2020, según un estudio de la Cámara de Comercio de Bogotá, la pandemia de COVID-19 aceleró la adopción de tecnología por parte de las pymes en Colombia. El informe señaló que el 50% de las pymes encuestadas había implementado nuevas herramientas digitales para apoyar sus operaciones y ventas y el 68% había aumentado su presencia en línea.

En términos generales, la ciberseguridad en las pymes colombianas aún se encuentra en una etapa incipiente (Pérez, 2017). Si bien es cierto que existe un mayor grado de conciencia en cuanto a la importancia de proteger los activos digitales de las empresas, la mayoría de ellas todavía carece de una estrategia de ciberseguridad clara y bien definida.

Entre los principales desafíos que enfrentan las pymes colombianas en materia de ciberseguridad se encuentran la falta de recursos y conocimientos especializados, así como la dificultad para identificar y evaluar las amenazas y vulnerabilidades de sus sistemas y redes.

Otro factor que agrava la situación es la falta de regulación y control por parte de las autoridades competentes, lo que puede generar una sensación de impunidad entre los ciberdelincuentes que buscan aprovecharse de las debilidades de las pymes.

A pesar de estos desafíos, es importante destacar que cada vez son más las pymes colombianas que se están interesando por la ciberseguridad y que están adoptando medidas para proteger sus activos digitales. Algunas de estas medidas incluyen la implementación de herramientas de seguridad informática, la formación de su personal en materia de ciberseguridad y la contratación de servicios especializados en esta área.

Según el portal pymas.com.co, dedicado al desarrollo digital de las pymes se indica que el 60% de las pequeñas y medianas empresas en Colombia no pueden sostener sus negocios luego de sufrir un ciberataque o ataque informático, de acuerdo a lo que revela el Informe de Tendencias del Cibercrimen en Colombia (2019-2020). Esto brinda un panorama cercano de la necesidad que tienen las pymes de contar con herramientas de ciberseguridad que les informe cu**á**ndo se esté presentando un evento anormal dentro de sus entornos tecnológicos.

3.2 Identificar las arquitecturas tecnológicas más usadas por las pequeñas y medianas empresas en Colombia

Dentro del manejo que le dan las pymes a la tecnología y ciberseguridad, en la mayoría de los casos se plantea la no necesidad de un área tecnológica y recurren a utilizar estudiantes o pasantes de tecnología, o bien a soportes externos para acciones correctivas sobre los componentes tecnológicos; esto debido a que son procesos no tan pertinentes y necesarios para sus procesos, lo que realmente deja a las pymes en un limbo tecnológico y a la merced de los ciberdelincuentes. Ahora bien, si se tiene en cuenta que las pymes con la pandemia originada por el COVID-19 vieron la necesidad de invertir en tecnología para poder subsistir.

Las pequeñas y medianas empresas (pymes) utilizan una variedad de infraestructuras tecnológicas según sus necesidades y recursos disponibles. Entre estos, algunos de los tipos de infraestructuras tecnológicas comunes utilizadas por las pymes incluyen:

- *Hardware:* utilizan computadores, portátiles, impresoras, servidores, dispositivos móviles, cámaras de seguridad y otros equipos para realizar sus operaciones diarias. También pueden utilizar dispositivos de almacenamiento externos como unidades flash USB y discos duros externos.
- *Software*: dentro de esta variedad pueden manejar sus procesos de negocio como *software* de contabilidad, *software* de recursos humanos, *software* de gestión de proyectos, *software* de facturación y *software* de gestión de inventario.
- Conectividad a Internet: un servicio necesario y primordial. Resulta imprescindible estar conectado a Internet para poder comunicarse con socios comerciales y posibles clientes prospectos. Se utilizan diferentes tipos de conexiones. En Colombia el servicio por excelencia es la fibra óptica, aunque tienden a reducir costos en algunos casos utilizando servicios de Internet residencial en lugar de usar Internet corporativo desconociendo las diferencias en sus características y beneficios (ver Tabla 1).

Tabla 1

Comparación Internet Residencial Versus Internet Empresarial

Característica	Internet residencial	Internet empresarial
Velocidad	Generalmente menor que la de Internet empresarial	Generalmente más rápida que la de Internet residencial
Ancho de banda	Limitado y compartido con otros usuarios en la misma red	Mayor y dedicado exclusivamente a la empresa
Fiabilidad	Puede ser menos confiable debido al uso compartido de la red y la falta de SLA	Mayor confiabilidad y soporte técnico para garantizar la continuidad del negocio
Seguridad	Ofrece una cantidad limitada de medidas de seguridad	Puede incluir medidas de seguridad adicionales, como firewalls y encriptación de datos
Costo	Generalmente más barato que Internet empresarial	Generalmente más caro que Internet residencial debido a la mayor velocidad, ancho de banda y confiabilidad
Soporte técnico	Soporte limitado	Soporte técnico especializado y dedicado a las necesidades de la empresa

- Sistemas de seguridad: utilizados para proteger la información y sus activos informáticos. Principalmente usan antivirus, cámaras de seguridad, en algunos casos sistemas perimetrales como *firewalls* y sistemas de detección de intrusos. Pero, al igual que con la conectividad a Internet para el caso de los antivirus, en ciertas ocasiones tienden a utilizar antivirus no adecuados para los entornos empresariales (ver *Tabla 2*).

Tabla 2

Comparación Antivirus Empresarial Versus Antivirus Corporativo

Característica	Antivirus para hogar	Antivirus empresarial
Funciones de protección	Básicas, enfocadas en la protección contra virus y malware comunes	Avanzadas, con protección contra amenazas específicas para la empresa y la industria
Gestión centralizada	No disponible	Disponible, lo que permite la administración remota de la protección de la red de la empresa
Escalabilidad	Diseñado para cubrir las necesidades de un hogar o un pequeño negocio	Diseñado para adaptarse y crecer con una empresa en constante crecimiento
Personalización	Limitada o no disponible	Totalmente personalizable para adaptarse a las necesidades específicas de la empresa
Soporte técnico	Soporte básico disponible	Soporte técnico dedicado y especializado para las necesidades de la empresa
Precio	Generalmente más barato que los antivirus empresariales	Generalmente más caro que los antivirus para hogar debido a la mayor cantidad de funciones y soporte técnico especializado

- Servicios en la nube: principalmente utilizan servicios de correo, los demás servicios normalmente no son muy utilizados debido a los costos básicos y adicionales que se requieren dentro de sus servicios.

En otras partes del mundo la situación es similar, a pesar de ser entornos más avanzados tecnológicamente y con regulaciones más estrictas, según un estudio realizado por *Ponemon Institute* en 2020 con datos de empresas de los Estados Unidos, Reino Unido y algunas de Europa muestran que el 28% de las pequeñas y medianas empresas (pymes) encuestadas indicaron no tener ninguna solución de seguridad implementada en sus sistemas informáticos. Además, el mismo estudio señaló que solo el 21% de las pymes encuestadas tenía una política formal de seguridad de la información en vigor.

En 2020, otro estudio realizado por Shred-it encontró que el 41% de las pymes encuestadas no tenían un plan de gestión de incidentes de seguridad informática, y el 36% no tenían un plan de continuidad del negocio en caso de una violación de seguridad.

En cuanto a las herramientas de seguridad informática utilizadas por las pymes, casi la mitad de ellas enfrenta problemas para financiar la ciberseguridad. Para Kaspersky (2019) el 57% de las pymes encuestadas utilizaban soluciones de seguridad antivirus en sus sistemas, mientras que el 39% utilizaba soluciones de seguridad de correo electrónico y el 34% utilizaba soluciones de seguridad de red.

En particular, para Latinoamérica la información es igual de preocupante, según la consultora EY, con datos de su encuesta de seguridad de la información 2019-2020, el 70% de empresas en dicha región han sufrido al menos un incidente de ciberseguridad en los últimos doce meses. Sin embargo, solo el 25% de las empresas encuestadas tenían definido un plan de gestión de

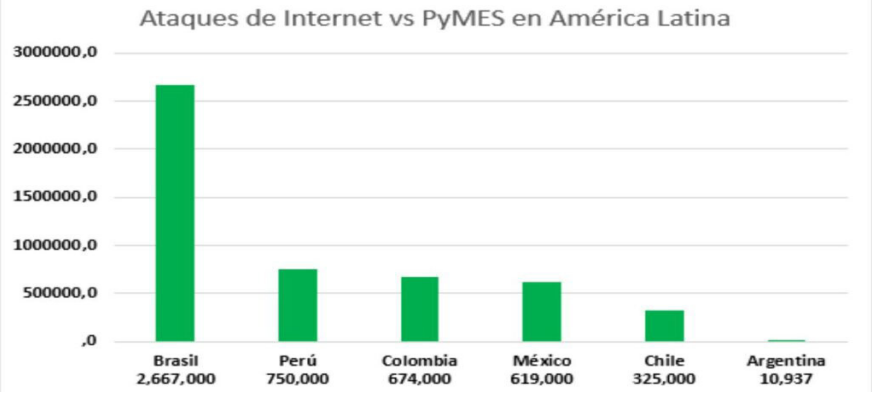
incidentes de seguridad. Fortinet, otro gran fabricante con presencia en todos los continentes en su reporte del estado de la ciberseguridad en Latinoamérica y el Caribe reportó que el 45% de las empresas de la región no tienen una política formal de seguridad informática.

3.3 Analizar los servicios que utilizan y los diferentes problemas de seguridad que pueden causar incidentes de seguridad que a la posta se vuelvan intrusiones

Un estudio realizado por la empresa de tecnología Kaspersky revel**ó** que en el 2022 las pequeñas y medianas empresas en Colombia están en el tercer puesto de ataques cibernéticos en América Latina; gracias a la pandemia muchas de estas han realizado inversión en procesos tecnológicos que les permitan vender y ofrecer sus servicios y productos de manera digital y por las diferentes plataformas de comercio electrónico del mercado digital (ver *Figura 1*).

Figura 1

Ataques de Internet vs Pymes en América Latina



Nota. Prensariotila (s.f)

Las pequeñas y medianas empresas son víctimas a cada momento durante sus operaciones de diferentes ataques basados en infinidad de técnicas para aprovecharse de la ingenuidad, falta de conocimiento, mal uso de los recursos tecnológicos o igual por utilización de servicios no adecuados para una empresa como antivirus para el hogar, *software* comercial no licenciado entre otros factores que ayudan a lograr el objetivo por parte de los ciberdelincuentes.

Dentro de esa infinidad de ataques e incidentes de seguridad a los que están expuestas las pymes es posible detallar los más relevantes en la siguiente *Tabla 3.*

Tabla 3

Principales Ataques a los que se ven Expuestas las Pymes

Tipo de ataque	Descripción	Ejemplo
Phishing	Involucra uno de los servicios más preferidos por los ciberdelincuentes como es el correo electrónico generando correos falsos direccionando a sitios web engañosos que parecen legítimos, diseñados para engañar a los usuarios y hacer que revele información confidencial como contraseñas o información de tarjetas de crédito.	Un correo electrónico falso que parece ser de un banco legítimo que solicita información de inicio de sesión.
Ransomware	Es un tipo de *software* malicioso que cifra archivos importantes del usuario y exige un rescate para recuperarlos.	El *ransomware* WannaCry que infectó a miles de sistemas en todo el mundo en 2017.
Ingeniería social	Se aprovecha de la manipulación psicológica de los usuarios para que revelen información confidencial. Los atacantes pueden hacerse pasar por representantes de una empresa legítima o enviar mensajes engañosos para obtener acceso no autorizado.	Un atacante que llama a un empleado haciéndose pasar por un representante de TI y solicita su contraseña.
Ataques de fuerza bruta	Involucra el uso de *software* automatizado para intentar adivinar contraseñas.	Un atacante que usa *software* para intentar adivinar una contraseña de un empleado en una cuenta de correo electrónico o en una red privada.
Ataques de inyección SQL	Se aprovecha de falencias en el desarrollo y los gestores de bases de datos para la manipulación de una base de datos a través de una entrada de usuario maliciosa.	Un atacante que ingresa código malicioso en un campo de entrada de un sitio web y accede a información confidencial en la base de datos.

Uno de los servicios utilizados por las pymes y el cual fue más utilizado durante la pandemia y pospandemia fue el *Remote Desktop Protocol* por sus siglas RDP o escritorio remoto, como es conocido comúnmente. Normalmente si la pyme tenía el servicio de *Virtual Private Network-VPN*, el cual permite conectar cualquier dispositivo a la red LAN y consumir los servicios internos de la pyme sin importar la ubicación donde se encuentre, se utilizaba el cliente del sistema operativo, pero si no se contaba con el servicio de VPN las pymes recurrían a otras herramientas como TeamViewer, logmein, Anydesk, entre otros, servicios que son muy populares. Sin embargo, respecto de su seguridad informática se han identificado una serie de vulnerabilidades reportadas a portales como CVE donde se registran y codifican las vulnerabilidades de cualquier servicio de tecnología (ver *Tabla 4*).

Tabla 4

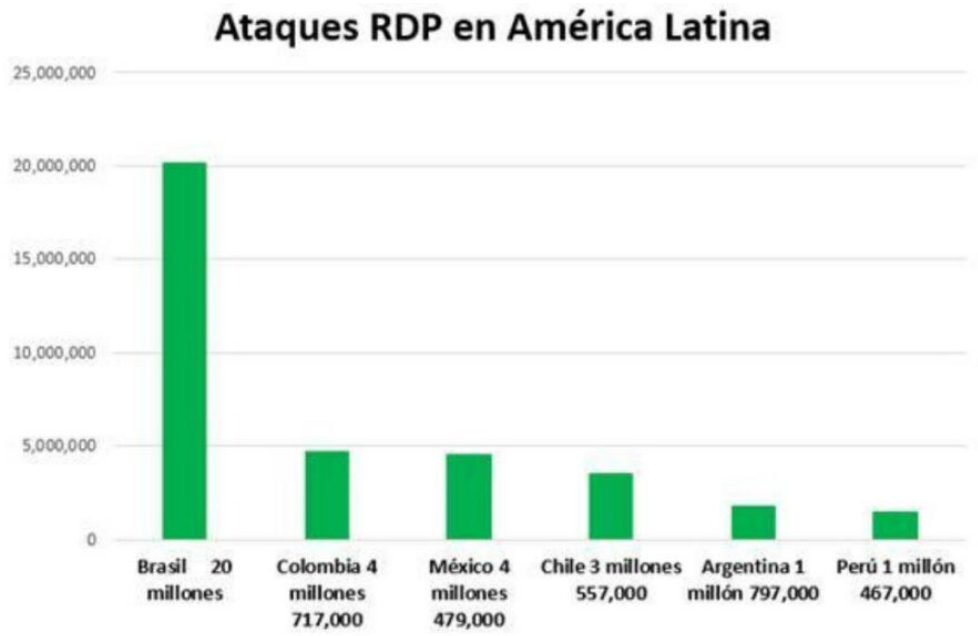
Estadísticas de Ataques a Herramientas RDP Reportadas en CVE-Mitre

Herramienta Acceso Remoto	Vulnerabilidades
Webex	302
Rdp	115
Xrdp	25
Teamviewer	14
Anydesk	9
Logmein	6

Al igual, dentro del informe de Kaspersky se evidencia que en Colombia las pymes sufrieron 4 millones de ataques a herramientas de RDP. En la siguiente Figura 2 se muestra un gráfico relacionado.

Figura 2

Ataques a Herramientas RDP en América Latina a las Pymes



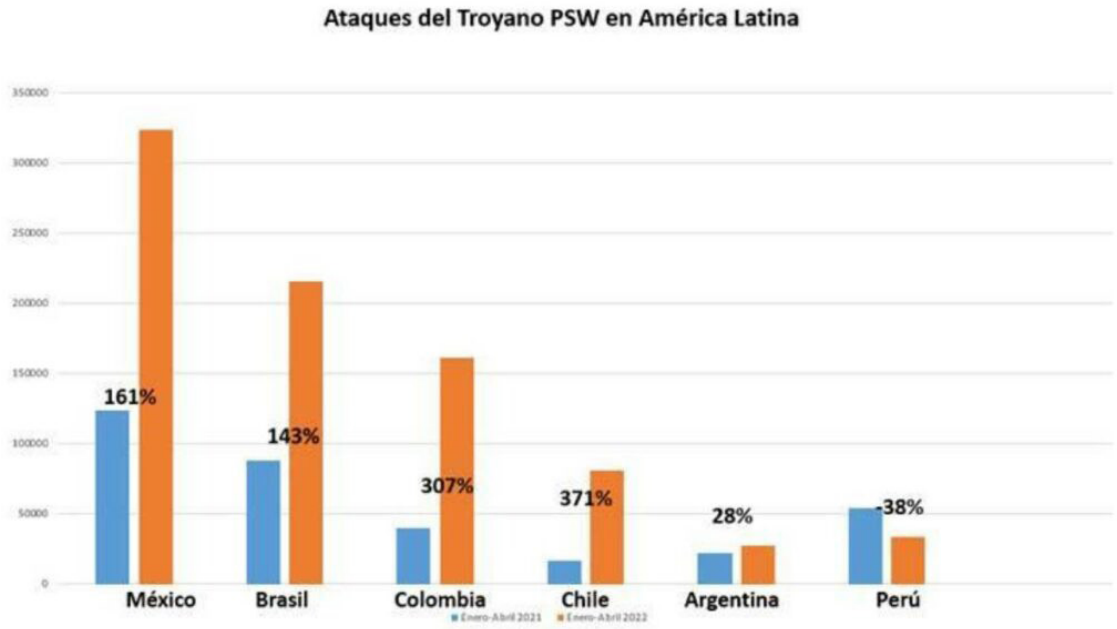
Nota. Prensariotila (s.f)

El troyano *Password Stealing Ware* (PSW) está diseñado para robar información relacionada con los inicios de sesión, como credenciales, buscando dentro de los dispositivos afectados los archivos que almacenan este tipo de datos. Según el informe de Kaspersky del 2022 se puede evidenciar el aumento de ataques 307% en Colombia (Ver *Figura 3*). Dentro de las razones por las que se ven dispositivos afectados con los troyanos se encuentran el mal uso de los servicios y la falta de concientización de los colaboradores, al igual que la mala utilización de servicios de

antivirus no empresariales con características básicas que no protegen igual que un antivirus empresarial, así como también no contar con alguna herramienta que les informe de cualquier anomalía en los servicios de tecnología utilizados por estas.

Figura 3

Ataques de Troyanos en América Latina a las Pymes



Nota. Prensariotila (s.f)

3.4 Comparar los diferentes IDS de código abierto que se puedan implementar en un dispositivo Raspberry

En la *Tabla 5* se presenta una comparación entre los dos sistemas más populares de detección de intrusos basados en código abierto, evidenciando sus características en cuestión de funcionamiento, rendimiento y manejo de reglas.

Tabla 5

Comparativa de los dos Principales Sistemas de Detección de Intrusos Basados en Código Abierto

Características	Snort	Suricata
Desarrollador	Cisco	Open Information Security Foundation
Licencia	GPL	GPL
Soporte Multiplataforma	Sí	Sí
Modos de funcionamiento	Inline y en línea pasiva	Inline y en línea pasiva
Motor de detección	Basado en reglas	Basado en reglas
Motor de detección	Basado en reglas	Basado en reglas
Soporte de reglas	Compatible con reglas de Snort	Compatible con reglas de Snort
Escalabilidad	Escalabilidad vertical limitada	Escalabilidad horizontal y vertical
Rendimiento	Bajo rendimiento en comparación con Suricata	Alto rendimiento
Soporte de protocolos	Soporta una amplia gama de protocolos	Soporta una amplia gama de protocolos
Fácil configuración	Fácil de configurar	Más complejo que Snort
Gestión de eventos	Soporte limitado	Soporte completo
Soporte de salida	Soporte limitado	Soporte completo

En la siguiente *Tabla 6* se presentan las diferentes características más técnicas de los sistemas de detección de intrusos basados en código abierto, permitiendo elegir o decidir en sus respectivas características cuál es la mejor opción para realizar las pruebas iniciales en entornos controlados.

Tabla 6

Comparativa de Características Técnicas de los Sistemas de Detección de Intrusos más usados de Código Abierto

Características	Snort	Suricata
Número de reglas	Más de 11,000	Más de 40,000
Velocidad de procesamiento	5-10 Gbps	10-20 Gbps
Soporte de protocolos	TCP, UDP, ICMP, HTTP, DNS, FTP, SMTP, SSH, SIP, SSL, entre otros.	TCP, UDP, ICMP, HTTP, DNS, FTP, SSH, SIP, SSL, entre otros.
Funcionalidades	Detección de intrusiones, prevención de intrusiones, registro de eventos, captura de paquetes, análisis de tráfico, entre otros.	Detección de intrusiones, prevención de intrusiones, registro de eventos, captura de paquetes, análisis de tráfico, análisis de malware, entre otros.
Lenguajes de reglas	Snort y Emerging Threats open	Suricata y Emerging Threats open
Flexibilidad	Limitada	Mayor
Comunidad	Grande y activa	Grande y activa
Sistema operativo	Linux, Unix, Windows, MacOS	Linux, Unix, Windows, MacOS
Licencia	GPLv2	GPLv2

Debido a que Suricata presenta unas características óptimas para usarlas sobre una Raspberry Pi 4 (ver *Figura 4*), como por ejemplo que la velocidad de procesamiento de Snort (Castro y Moreira, 2018) puede ser de hasta 1 Gbps y en Suricata de hasta 1.5 Gbps, en cuanto al rendimiento Snort puede procesar en promedio entre 100 a 200 Mbps, mientras que Suricata puede procesar entre 200 a 300 Mbps.

Figura 4

Raspberry Pi Versión 4

Nota. Terceravia (2016)

3.5 Evaluar y documentar diferentes procedimientos de instalación de sistemas de detección de intrusos, inicialmente en máquinas virtuales implementadas con herramientas de virtualización como VMware player

Dentro de la evolución de los diferentes procedimientos de instalación sin importar la herramienta, cabe tener en cuenta que lo ideal es instalarlo en un sistema operativo como Linux por su similitud con el sistema operativo de las Raspberry –"Raspberry PI OS"–, que realmente resulta una distribución creada para estos dispositivos. Durante el proceso de evaluación de los diferentes procedimientos se pudo evidenciar que se requieren un sinnúmero de librerías para desarrollo en C, Lua y en Python junto con otros componentes de *software* requerido para su respectivo y correcto funcionamiento.

En la *Tabla 7* se presenta la comparación de los procesos planteados y realizados en entornos controlados.

Tabla 7

Comparativa de los Procedimientos de Instalación de las Simulaciones de Instalación del IDS Suricata

Características	Instalación Completa	Docker
Emulador Vms	Vmware Player 17	Vmware Player 17
Sistema Operativo	Raspberry PI OS	Raspberry PI OS
versión del SO	Released 2023-02-21	Released 2023-02-21
Sistema Detección de Intrusos	Suricata	Suricata
versión del IDS	6.0.11	6.0.11
Pasos de instalación	25	2
Tiempo de Instalación(min)	180	30
Configuración Reglas	60	30
Pruebas y testeo	60	60
Total Proceso en horas	6	2

Dentro de los ejercicios realizados sobre máquinas virtuales apoyado de la herramienta VMware player versión 17 se pudo evidenciar una instalación completa con 25 pasos, incluyendo todos los compontes y librerías que se requieren dentro del proceso. Esto se inicia con la actualización del sistema operativo hasta los testeos iniciales de las reglas, coprocesadores por defecto y la customización de diferentes reglas para identificar qué tanto es el uso de las principales redes sociales en las pymes, para este procedimiento en tiempo se requiere aproximadamente de 4 horas.

Otro procedimiento para implementar un sistema de detección de intrusos es aprovechar las nuevas tecnologías como lo son los Docker utilizando imágenes de sistemas de detección de intrusos desarrolladas en algunos proyectos bajo esta tecnología. Así es posible optimizar el uso de recursos de *hardware* gracias a que con los Docker solo se utilizan los recursos necesarios para que el servicio o herramienta que se está manejando de esta manera.

A continuación, se relaciona el procedimiento de la implementación del sistema de detección de intrusos bajo la tecnología de dockers tomado del proyecto desarrollado por Jason Ish que es un desarrollador perteneciente a *Open Information Security Foundation* (OISF), una organización que promueve la creación de comunidades y respaldar tecnologías de seguridad de código abierto como Suricata.

Como se ha indicado, el procedimiento es muy corto, pero eso no indica que no se deba conocer c**ó**mo es el funcionamiento de Suricata, tanto como el manejo de las reglas, la ubicación de los archivos de configuración y los muy importantes archivos de eventos.

Paso 1: descarga la imagen del Docker utilizando el comando Docker pull jasonish/suricata, este comando lo descarga en el directorio o carpeta donde actualmente se está ubicado dentro del SO como se evidencia en la *Figura 5.*

Figura 5

Paso 1 - Descarga de la Imagen Docker del Repositorio

```
└─# docker pull jasonish/suricata
Using default tag: latest
latest: Pulling from jasonish/suricata
Digest: sha256:ffffa8539dfc197d9a01ad29d177f270fd9b40fa029f9101d1fc184a0236cb9f
Status: Image is up to date for jasonish/suricata:latest
docker.io/jasonish/suricata:latest
```

Paso 2: ejecutar o invocar la imagen con el comando Docker run, teniendo en cuenta que se agregan diferentes parámetros como -v para direccionar la ubicación de los archivos de eventos, al igual que el parámetro -i para indicarle al IDS la tarjeta de red que va a estar analizando. En la *Figura 6* se puede evidenciar el funcionamiento de suricata.

Figura 6

Paso 2 - Ejecución de la Instancia de Suricata versión 6.0.11

```
└─# docker run --rm -it --net=host \
    --cap-add=net_admin --cap-add=net_raw --cap-add=sys_nice \
    -v logs:/var/log/suricata \
        jasonish/suricata:latest -i eth0
Checking for capability sys_nice: yes
Checking for capability net_admin: yes
22/4/2023 -- 16:45:52 - <Notice> - This is Suricata version 6.0.11 RELEASE running in SYSTEM mod
e
22/4/2023 -- 16:46:23 - <Notice> - all 6 packet processing threads, 4 management threads initial
```

Ya en este punto el Suricata está ejecutándose en el Sistema Operativo Raspberry, lo siguiente es proceder a configurar la red interna, la red externa e incluir el archivo personalizado de reglas en el archivo suricata.yaml para que lo reconozca.

Conclusiones

Una vez revisados los contextos locales, regionales y latinoamericanos relacionados con la seguridad de la información, se puede evidenciar que, si bien hay avances en la implementación, tanto de políticas, como de herramientas de seguridad que ayudan a mejorar la postura de seguridad de las pymes; sin embargo, hay mucho trabajo aún por hacer, desde la concientización del eslabón más débil de la cadena de seguridad de la información que es el usuario.

Como la necesidad de la asignación y manejo de un presupuesto para la adquisición de soluciones de seguridad informática no tiene máxima prioridad dentro de las pymes en un entorno pospandemia que es sensible económicamente, el uso de este tipo de soluciones ayuda también desde el punto de vista económico.

Las regulaciones que poco a poco se fortalecen también demandan de las pymes atención en estos temas, que a menudo deben escoger entre sobrevivir o crecer de manera moderada, realizando inversiones en sus procesos misionales del negocio o invertir en tecnología y

soluciones de seguridad informática. Aquí es donde las soluciones basadas en código abierto implementadas en dispositivos de bajo costo pueden ayudar a las pymes a solventar ese problema y ayudarlas a fortalecer sus posturas de seguridad sin necesidad de hacer altas inversiones.

La posibilidad de realizar combinaciones entre diversas soluciones de seguridad informática basadas en código abierto y su implementación en una infraestructura con costos reducidos, que además cuente con un rendimiento adecuado para las necesidades de las pymes, brindan opciones reales para que ellas puedan contar con herramientas que les ayuden a fortalecer sus estrategias de seguridad y a proteger la información que gestionan una inmejorable relación costo/beneficio.

El apoyo a las pymes y el desarrollo de herramientas basadas en código abierto pueden generarse desde la academia con el apoyo de las agremiaciones, como cámaras de comercio e instituciones gubernamentales, buscando con ello mejorar las condiciones de seguridad con el fin de garantizar su subsistencia en un entorno virtual cada vez más extendido, pero también cada vez más peligroso.

Referencias

ANIF. (2020). *Gran encuesta pyme nacional*. https://www.anif.com.co/encuesta-mipyme-de-anif/gran-encuesta-pyme-nacional/

Castro, P., y Moreira, A. (2021). *Desarrollo de un prototipo de un sistema de análisis y monitoreo de una red utilizando la herramienta open source SNORT para identificar las vulnerabilidades de la red y brindar seguridad a las conexiones de los diferentes dispositivos finales con servidor VPN y raspberry PI* (Tesis de grado, Universidad de Guayaquil). http://repositorio.ug.edu.ec/handle/redug/52260

Franco, M., y Urbano, D. (2019). Caracterización de las pymes colombianas y de sus fundadores: un análisis desde dos regiones del país. *Estudios gerenciales*, *35*(150), 81-91. https://doi.org/10.18046/j.estger.2019.150.2968

Kaspersky. (2019). *How businesses are losing money and saving costs amid cyberattacks*. IT security economics in 2019. https://go.kaspersky.com/rs/802-IJN-240/images/GL_Kaspersky_Report-IT-Security-Economics_report_2019.pdf

Marín, A., y Carvajal, O. (2018). *Estudio monográfico sobre los casos más comunes de cibercrimen en las Pymes Colombianas* [Tesis de especialidad, Universidad Nacional Abierta y a Distancia]. https://repository.unad.edu.co/handle/10596/30322

Mintic. (2018a). Caracterización de las MiPyME colombianas y conocimiento de su relación con las TIC. https://colombiatic.mintic.gov.co/679/w3-article-56356.html

Mintic. (2018b). *La economía digital y las mipyme en Colombia*. Ministerio de Tecnologías de la Información y Comunicaciones de Colombia https://mintic.gov.co/portal/vivedigital/612/w3-propertyvalue-7235.html

Organización de Estados Americanos. (2018). *Programa de ciberseguridad*. OEA. https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp

Ortega, S. (2022). *Análisis de sistemas de detección de intrusos con herramientas open source* [Tesis de Maestría, Universidad Israel]. http://repositorio.uisrael.edu.ec/handle/47000/3364

Prensariotila. (s.f). *Kaspersky: las PyMEs de América Latina enfrentan un creciente número de ciberataques*. https://prensariotila.com/kaspersky-las-pymes-de-america-latina-enfrentan-un-creciente-numero-de-ciberataques/

Pérez, Y. (2017). *Importancia de la ciberseguridad en Colombia* [Tesis de especialización, Universidad Piloto de Colombia]. http://repository.unipiloto.edu.co/handle/20.500.12277/2676

Terceravia. (14 de febrero de 2016). Raspberry Pi: El microcomputador educativo de código abierto. https://terceravia.mx/2016/02/raspberry-pi-el-microcomputador-educativo-de-codigo-abierto/

Tripathi, S., & Kumar, R. (2018). Raspberry pi as an intrusion detection system, a honeypot and a packet analyzer. In *2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)* (pp. 80-85). https://doi.org/10.1109/CTEMS.2018.8769135

Vieites, Á. (2011). *Enciclopedia de la seguridad informática*. Grupo Editorial RA-MA.

Zitta, T., Neruda, M., & Vojtech, L. (2017). The security of RFID readers with IDS/IPS solution using Raspberry Pi. In *2017 18th International Carpathian Control Conference (ICCC)* (pp. 316-320). http://dx.doi.org/10.1109/CarpathianCC.2017.7970418.