RECOMENDACIONES DE BUENAS PRÁCTICAS DE CIBERSEGURIDAD EN PYMES PARA LA GENERACIÓN DE SOLUCIONES DE DETECCIÓN DE INTRUSOS USANDO SNORT

JHON ALEXANDER MARTÍNEZ ROMERO
LEIDY XIOMARA BLANCO MEDINA

UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
BUCARAMANGA
2020

RECOMENDACIONES DE BUENAS PRÁCTICAS DE CIBERSEGURIDAD EN PYMES PARA LA GENERACIÓN DE SOLUCIONES DE DETECCIÓN DE INTRUSOS USANDO SNORT

JHON ALEXANDER MARTÍNEZ ROMERO
LEIDY XIOMARA BLANCO MEDINA

DIRECTOR: YAMID GABRIEL GAMBA GONZALEZ

UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
BUCARAMANGA
2020

Nota de Aceptación

_____

_____

_____

_____

_____

Firma del jurado

_____

Firma del Jurado

DEDICATORIA

El presente trabajo de grado está dedicado a Dios y a nuestros padres:

A Dios, ya que gracias a él logramos finalizar este ciclo profesional en nuestras vidas, por brindarnos la salud y los recursos necesarios para dar cumplimiento a cada una de las fases y actividades propuestas.

A nuestros padres, por su apoyo incondicional, por haber forjado nuestro camino, por sus consejos y esfuerzos para que pudiéramos llegar hasta esta etapa y por ser el motor principal en nuestras vidas.

AGRADECIMIENTOS

Queremos expresar nuestros agradecimientos a Dios por darnos la sabiduría necesaria para poder finalizar un logro más en nuestra vida profesional la cual nos permitirá seguir creciendo a lo largo de nuestra carrera.

A nuestro director, el Ing. Yamid Gabriel Gamba, por apoyarnos, orientarnos y compartir sus conocimientos a través de cada una de las actividades, retroalimentándonos paso a paso con el fin de comprender y mejorar en cada uno de los procesos que se desarrollaron en este trabajo.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN EJECUTIVO

Introducción: La transformación digital de las empresas se ha convertido en una herramienta esencial, a medida que Internet se convirtió en parte de la vida diaria. El rápido avance de la tecnología no solo brinda facilidad de acceso a la gente común, sino también técnicas sofisticadas a los ciberdelincuentes. Esto conduce a una gran cantidad de ataques cibernéticos tanto a personas como a organizaciones. Los ciberdelincuentes eligen de forma cuidadosa a sus víctimas, aplicando técnicas de reconocimiento como OSINT o fingerprinting buscando conocer el estado y nivel de seguridad de su información, aprender sobres sus negocios, y sus relaciones con sus stakeholders para identificar las posibles vulnerabilidades. Ello conlleva a que las pymes implementen sistemas de detección y prevención de intrusiones las cuales juegan un papel vital en la protección de la información.

Objetivo: Realizar una serie de recomendaciones mediante una valoración objetiva del funcionamiento de la herramienta SNORT en un entorno de detección de intrusos para la prevención de incidentes de ciberseguridad en pequeñas empresas.

Metodología: El proyecto se desarrolló con base a una metodología de investigación aplicada experimental de tipo cualitativo, que mediante el análisis de intrusiones a la infraestructura de pequeñas empresas y mediante un estudio funcional de la herramienta SNORT utilizando un escenario de prueba virtualizado, el cual permitió simular ataques reales y las posibles técnicas de mitigación.

Desarrollo: Para la ejecución del proyecto se buscó información sobre los ataques cibernéticos más comunes a los que están expuestas las pymes para tener un conocimiento de los peligros que asechan a las organizaciones a nivel informático. Una vez obtenida la información esta se analizó teniendo en cuenta los riesgos dados por el OWASP TOP 10 para la clasificación de los incidentes haciendo una réplica de los que se encuentran en las tres primeras posiciones. Para la detección de incidentes e informar a los administradores de los recursos informáticos, se realizó un análisis funcional de la herramienta open source denominada Snort, la cual permite por medio de patrones preestablecidos y configurables reconocer si la organización está siendo víctima de un ciberataque.

Una vez obtenida la información suficiente respecto a los ataques se procedió a la implementación de un entorno controlado el cual buscó simular una red interna de una organización, usando la herramienta de virtualización Virtual box la cual permite simular las maquinas requeridas con diferentes sistemas operativos, tales como: Windows 7, Ubuntu 18.04, Kali Linux 2019.2, así como la aplicación web Badstore. En la implementación del escenario de prueba se usó una máquina de Windows 7 para el papel de IDS Snort y que permite analizar el tráfico de red, detectar los ataques simulados, igualmente, se usó una maquina Ubuntu que cumple con el papel de servidor web y ftp, la máquina de Kali Linux se usó como atacante para la realización de pruebas de intrusión: Sql Injection, xss, i p spoofing y dns spoofing.

Conclusión: La herramienta Snort permite analizar la red y por medio de reglas detectar ataques informáticos; lo cual permite a los encargados de la seguridad informática dentro de la organización actuar rápidamente para evitar la pérdida de información.

PALABRAS CLAVE Intrusion Detection System, Snort Tool, Ciberseguridad, SNORT, IDS, pequeñas empresas, ataques informáticos.

GRUPO DE INVESTIGACIÓN PRISMA.

LÍNEA DE INVESTIGACIÓN Tecnología y sociedad

EXECUTIVE SUMMARY

Abstract: The digital transformation of companies has become an essential tool, as the Internet has become part of everyday life. The rapid advance of technology not only provides easy access for ordinary people, but also sophisticated techniques for cyber-crooks. This leads to a large number of cyber attacks on both individuals and organizations. Cyber-crooks choose their victims carefully, applying reconnaissance techniques such as OSINT or fingerprinting to find out the status and level of security of their information, learn about their business, and their relationships with their stakeholders to identify possible vulnerabilities. This leads to the implementation of intrusion detection and prevention systems by SMEs, which play a vital role in protecting information.

Objective: Make a series of recommendations through an objective assessment of the operation of the SNORT tool in an intrusion detection environment for the prevention of cybersecurity incidents in small companies..

Methodology: The project was developed based on a qualitative applied research methodology, which through the analysis of intrusions into the infrastructure of small businesses and through a functional study of the SNORT tool using a virtualized test scenario, which allowed the simulation of real attacks and possible mitigation techniques.

Development: For the execution of the project, information was sought on the most common cyber attacks to which SMEs are exposed in order to gain an understanding of the dangers that beset organizations on an IT level. Once the information was obtained, it was analyzed taking into account the risks given by the OWASP TOP 10 for the classification of incidents, making a replica of those in the first three positions. In order to detect incidents and inform IT resource managers, a functional analysis of the open source tool called Snort was carried out, which uses pre-established and configurable patterns to recognize if the organization is being victimized by a cyber attack.

Once sufficient information about the attacks was obtained, a controlled environment was implemented to simulate an organization's internal network, using the Virtual box virtualization tool, which simulates the required machines with different operating systems, such as Windows 7, Ubuntu 18.04, Kali Linux 2019.2, and the Badstore web application. In the implementation of the test scenario, a Windows 7 machine was used for the role of IDS Snort, which allows the analysis of network traffic and the detection of simulated attacks. Likewise, an Ubuntu machine was used to play the role of web and ftp server, and the Kali Linux machine was used as an attacker to carry out intrusion tests: Sql Injection, xss, ip spoofing and dns spoofing.

Conclusion: The Snort tool allows us to analyze the network and by means of rules detect anomalies and possible computer attacks; which allows those in charge of computer security within the organization to act quickly to avoid the loss of information.

KEYWORDS Intrusion Detection System, Snort Tool, Cybersecurity, SNORT, IDS, small companies, computer attacks.

INVESTIGATION GROUP PRISMA.

LINE OF RESEARCH Technology and society

1. PROBLEMÁTICA Y ÁRBOL DE PROBLEMA

1.1 PLANTEAMIENTO DE LA PROBLEMÁTICA

La actual era digital entre otras cosas, ha generado un gran impulso en el desarrollo de la tecnología y la infraestructura informática con cambios que hasta hace muy poco eran únicamente posibles en la ciencia ficción, llevando a mejoras significativas de diversas organizaciones sin importar su tamaño u objetivo de negocio. Al mismo tiempo y con la misma contundencia estos grandes avances han motivado una serie de brechas de seguridad que también afectan a dichas organizaciones. Ello conlleva a que los ciberatacantes diseñen nuevos vectores de ataque que ejecutan mediante herramientas cada vez más sofisticadas, complejas y peligrosas, (Cosimo, Ahsan, Morabito, & Hussain, 2020).

Este nuevo escenario, aún desconocido para la mayoría de las pequeñas y medianas empresas favorece una serie de problemas críticos para la infraestructura de las tecnologías de la información, conllevando a que estén expuestos a incidentes informáticos casi a diario como por ejemplo la destrucción, secuestro o robo de información, estos últimos usados por los ciberatacantes con fines delictivos como el chantaje o el tráfico y venta en la Deep web con fines lucrativos por fuertes sumas de cripto monedas. Los ataques más evidentes son los que se presentan en la infraestructura de red que interconecta a los sistemas informáticos de las organizaciones que se usan a diario, generando un gran desafío a nivel de ciberseguridad para la pequeña y mediana empresa Pymes (ITCL, 2018). Las cuales según un estudio realizado a nivel global por el Ponemon Institute, refleja que este tipo de ataques va en creciente aumento como se muestra en la Figura 1 donde se evidencia el tipo de ataques que han sufrido las Pymes para el año 2018, así como su varianza con respecto a 2017, ataques que en su gran mayoría repercuten directamente en el rendimiento de las infraestructuras informáticas de pymes afectando sus procesos misionales, objetivos de negocio y procesos de apoyo como por ejemplo los sistemas de contabilidad y facturación, y las comunicaciones, internas y externas.

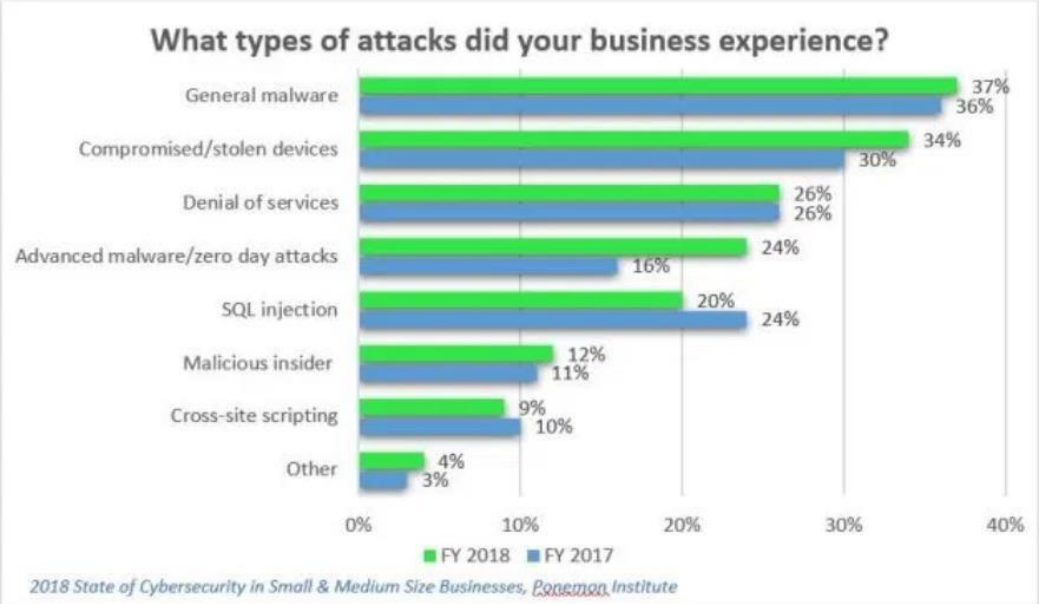

Figura 1 Tipos de ataques en pymes en 2018. Fuente: Reporte anual de ciberseguridad (Tenable, 2018)

En este contexto Colombia no es la excepción, según datos del Informe de tendencias del cibercrimen, Colombia es un país altamente vulnerable a diversos tipos de ataques cibernéticos debido a que la población y las compañías no tienen ni la educación ni la cultura suficiente para autoprotegerse, convirtiéndose casi de forma automática en víctimas de dichos delitos, permitiendo el acceso a personas indeseadas a toda su información personal y a la información financiera y bases de datos de las empresas (VICTOR ANTONIO HOYOS BUITRON, 2015) (Ver Figura 2)

Figura 2 Cifras denuncias ataques cibernéticos 2015 – 2019. Fuente: Informe de tendencias del cibercrimen en Colombia *(Nacional Policia, CCIT, 2019)*

En 2019 los incidentes cibernéticos en el país tuvieron un incremento del 54 % con respecto al 2018, según registros de las autoridades SIEDCO Policía, SPOA Fiscalía. Además, de los 28.827 casos reportados, 15.948 fueron denunciados como infracciones a la ley 1273 de 2009, que tipifica los delitos informáticos en Colombia. El 80 % de los ataques a empresas

fue de correos fraudulentos, seguido del 60 % con la suplantación de identidad, el 53 % con el enmascaramiento de correos y el 37 % con la infección de sitios web (Nacional Policia, CCIT, 2019). (Ver Figura 3)

Figura 3 Incremento en incidentes para 2018. Fuente: (Informe de tendencias del cibercrimen en Colombia (2019-2020)).

Estas estimaciones demuestran grandes pérdidas económicas para las pymes donde los ataques cibernéticos han costado cerca de 1,3 millones de dólares por empresa en promedio. Ello conlleva que las PYME, el coste medio de la recuperación ascienda a 117.000 dólares. Incluyendo tanto los costos de negocio perdido, las mejoras de software y sistemas y los gastos extra en personal interno y en asesoramiento experto (Kaspersky Lab y B2B International).

En la Figura 4, se evidencia la cantidad de delitos informáticos discriminado por ciudades en Colombia, donde el factor de desarrollo económico ha influenciado sobre los objetivos de los cibercriminales, quienes se han enfocado en ejecutar acciones constantes contra las pymes, entidades financieras y grandes compañías con asiento varias de estas ciudades.

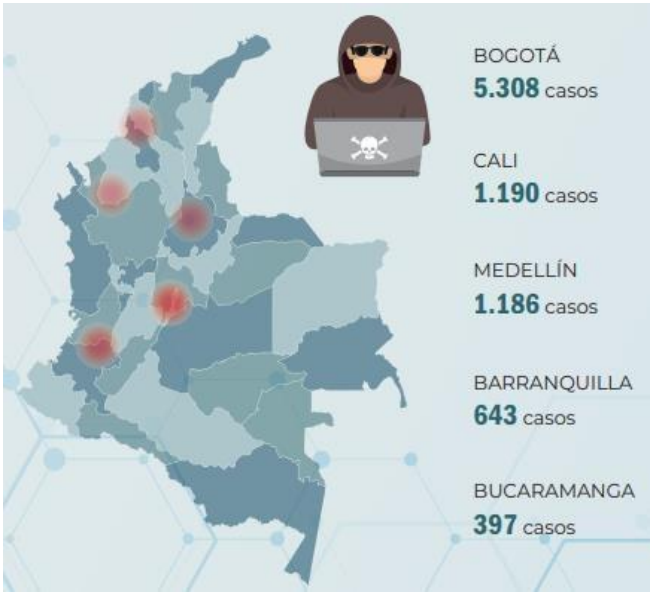

Figura 4 Número de delitos informáticos por ciudades. Fuente: (Nacional Policia, CCIT, 2019).

Según el estudio de las Tendencias del Cibercrimen en Colombia para 2019, los ataques por malware tipo ransomware aumentaron en más de 612%, con montos pagados por concepto rescate de información entre los 32 millones y los 160 millones de pesos, haciendo que Colombia sea uno de los países que recibió el mayor número de ataques en Latinoamérica con un total de 252, cerca del 30%, seguido de Perú (16%), México (14%), Brasil (11%) y Argentina (9%) y donde las pymes fueron el blanco preferido por los ciberatacantes, pues conocen que los niveles de seguridad suelen ser más bajos en este tipo de compañías ya que como se muestra en la Figura 5, según el mismo estudio el 83% de las pymes carecen de protocolos de respuesta a incidentes de seguridad (Nacional Policia, CCIT, 2019)

Figura 5 Porcentaje de empresas que carecen de protocolos de respuesta a violación en seguridad. Fuente: (Nacional Policia, CCIT, 2019))

1.2 ÁRBOL DE PROBLEMA

Para darle una rigurosidad a la problemática planteada se usó la técnica de árbol de problema

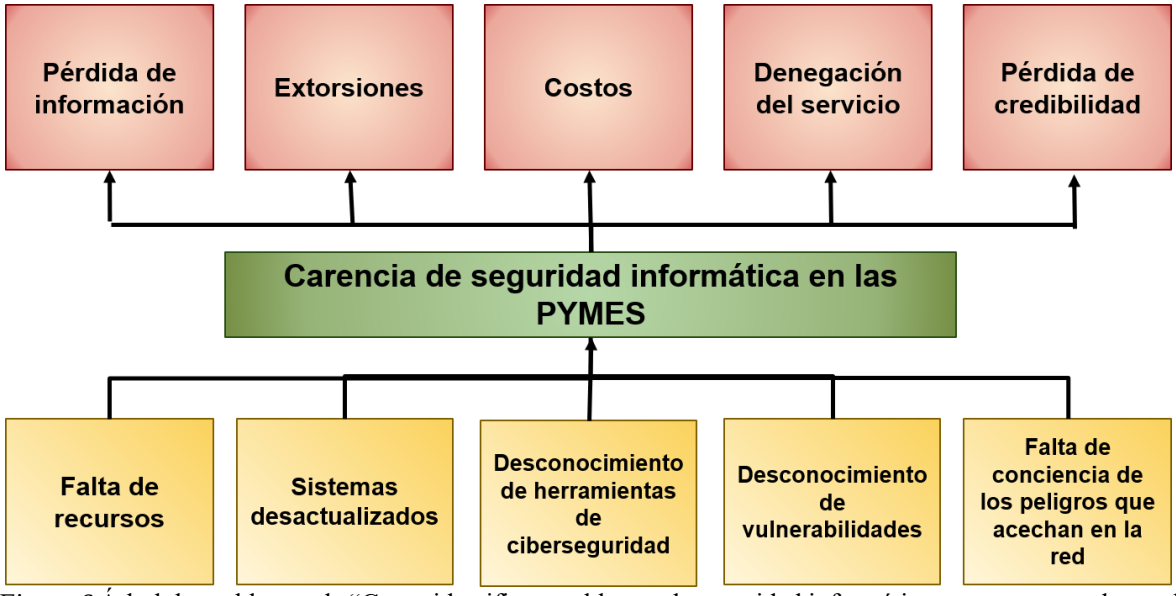

Figura 6 Árbol de problemas de "Como identificar problemas de seguridad informática en pymes usando una herramienta IDS". Fuente: (Romero Castro, Figueroa Moràn, & Vera Navarrete, INTRODUCCIÓN A LA SEGURIDAD, 2018)

2. **JUSTIFICACIÓN**

En la actualidad el 53 por ciento de la población mundial está conectada a internet. Ello implica un riesgo muy alto para particulares y empresarios que deben velar por el tema de la ciberseguridad; (informe “Digital in 2018”, elaborado por We Are Social y Hootsuite), el asegurar las bases de datos internas y de clientes y realizar transacciones son unos de los hitos más importantes es por esto que la penetración rápida y constante de internet obliga a las organizaciones a adoptar políticas digitales en el corto plazo (John Galindo, CEO de Digiware, 2018).

> “Lamentablemente, la explotación de vulnerabilidades por virus, gusanos y redes robot puede propagarse muy rápidamente por las redes y, en pocos segundos, éstas pueden verse considerablemente afectadas” (ITU X.1209, 2010).

Las organizaciones deben darse cuenta de que su valor más importante en el sistema es la información, incluidos los datos sobre sus sistemas de producción, organizaciones, productos, inversiones, exportaciones, importaciones y datos de clientes. En otras palabras, todo lo que rodea a la organización puede ser fácilmente robado o manipulado por terceros con fines delictivos (ITCL, 2018)

Es por esto que la relevancia que tiene la seguridad informática es fundamental para el logro de los objetivos de cualquier entidad y ha traído consigo el desarrollo de herramientas con el propósito de crear mecanismos de seguridad tanto para la prevención como la detección de intrusos, una de estas herramientas es el IDS SNORT, el cual implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, análisis de protocolos y todo esto en tiempo real (MAESTROS DEL WEB, 2020)

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar una serie de recomendaciones mediante una valoración objetiva del funcionamiento de la herramienta SNORT en un entorno de detección de intrusos para la prevención de incidentes de ciberseguridad en pequeñas empresas.

3.2 OBJETIVOS ESPECÍFICOS

- Reconocer los tipos de vulnerabilidades e intrusiones más comunes mediante la descripción de los vectores de ataque en el ámbito de ciberseguridad en pymes con base a los resultados obtenidos de la búsqueda sistemática de información.
- Identificar la funcionalidad de la herramienta SNORT mediante la revisión de la documentación oficial y la comprensión de las guías de la comunidad.
- Implementar un escenario controlado para la prueba de intrusiones en una red prototipo, utilizando las configuraciones propuestas, mediante la herramienta SNORT en un entorno virtualizado.
- Proponer recomendaciones de buenas prácticas para la mitigación de los riesgos de ciberseguridad en pymes con base a los resultados obtenidos y la evidencia científica.

4. **ANTECEDENTES**

Tabla 1
Antecedentes al proyecto

TÍTULO	DESCRIPCIÓN	AUTORES
DISEÑO DE RED BAYESIANA PARA LA PREDICCIÓN DE ATAQUES INFORMÁTICOS DE TIPO RANSOMWARE	Este proyecto presenta el diseño de una estrategia basada en el teorema de Bayes para la predicción de ataques de Ransomware, específicamente WannaCry buscando que las pymes tomen decisiones predictivas con base en niveles de seguridad de TI.	(GÓMEZ BAUTISTA & REY SEPULVEDA, 2019)
PROPUESTA PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE DETECCION DE INTRUSOS (IDS) EN LA DIRECCION GENERAL SEDE CENTRAL DEL INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO INPEC "PIDSINPEC"	Este proyecto propone la implementación de un IDS, en la red de comunicaciones de la Sede Central del INPEC, haciendo la caracterización de los IDS más populares. Como resultado obtienen un sistema que permite monitorizar de manera eficiente los eventos y violaciones a sus políticas de seguridad.	(GARZON PADILLA, 2015)
IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN DE INTRUSOS EN LA RED INTERNA DE LA ALCALDIA DE MONTERIA USANDO SOFTWARE LIBRE	Este proyecto presenta Gracias a los sistemas de detección de intrusos es posible contener ataques a la infraestructura tecnológica de una entidad, para el caso de la alcaldía de Montería siendo de carácter gubernamental, se siempre velar por preservar la seguridad e integridad de la información. Para esto se quiere Implementar un sistema de detección de intrusos en la red interna de la Alcaldía de Montería, a través de la implementación de diversas herramientas de seguridad Informática.	(QUINTERO HERRERA, 2018)

Fuente: Autores

5. ESTADO DEL ARTE

5.1 PROCESO DE BÚSQUEDA

Teniendo como punto de partida la pregunta de investigación establecida: ¿Cómo identificar problemas de seguridad informática en pymes usando una herramienta IDS?; y de conformidad con problema planteado: Incremento de ataques cibernéticos en las empresas durante los últimos años, los cuales generan pérdidas millonarias por destrucción o robo de información, además falta de conocimiento por parte de las organizaciones de las herramientas de ciberseguridad existentes; se desarrolló el proceso de revisión sistemática el cual aporta el soporte científico a la propuesta de proyecto: recomendaciones de buenas prácticas de ciberseguridad en pymes para la generación de soluciones de detección de intrusos usando snort.

Dicha búsqueda sistemática de evidencia disponible se llevó a cabo por los dos proponentes del proyecto, en las bases de datos: *Google académico*, *ACM*, *IEEE*, *Scopus*, donde se utilizan las palabras claves en inglés y español: Intrusion Detection System, *Snort Tool Ciberseguridad, SNORT, IDS, pequeñas empresas, ataques informáticos.*

A partir de las palabras claves se inició el proceso de búsqueda en las bases de datos propuestas. Una vez se cumple con esta etapa, se aplica un primer filtro de selección a partir del establecimiento de criterios de inclusión manteniendo únicamente las evidencias que cumplan con: La evidencia debe corresponder a documentos completos; El idioma debe ser en inglés y/o español; La fecha de publicación debe ser entre 2012 y 2020; El tipo debe corresponder con artículos de revistas, y artículos de conferencias. La temática debe estar relacionada con Detención de intrusos, ataques de red, ataques informáticos a pymes, ciberseguridad.

Una vez depurada la evidencia la siguiente etapa corresponde a un nuevo filtro de refinación a partir de la revisión específica y el análisis minucioso del título, las palabras claves, el resumen y el contenido, excluyendo, además los documentos repetidos, para a su utilización y aplicación en el proyecto. En la figura 7 se muestra un diagrama de flujo en detalle de la metodología del proceso de búsqueda, el cual se describe en el siguiente apartado.

5.2 PROCEDIMIENTO PARA LA SELECCIÓN DE ESTUDIOS

El proceso inició con el establecimiento de los parámetros de búsqueda y las palabras claves, a partir de los cuales los dos investigadores se dividieron la búsqueda por temáticas en las bases de datos propuestas:

Paso 1: Inicia el proceso de búsqueda escogiendo las bases de datos.

Paso 2: En cada base de datos se incluyeron las palabras claves establecidas teniendo en cuenta el conector AND, y que las palabras se encuentren en título y resumen.

Paso 3: Depurar la información de manera exhaustiva mediante filtros específicos, de conformidad con la temática del proyecto, evaluando los resúmenes de cada artículo teniendo en cuenta los criterios establecidos en el protocolo de búsqueda.

Paso 4: Analizar la información de los artículos seleccionados según el resumen.

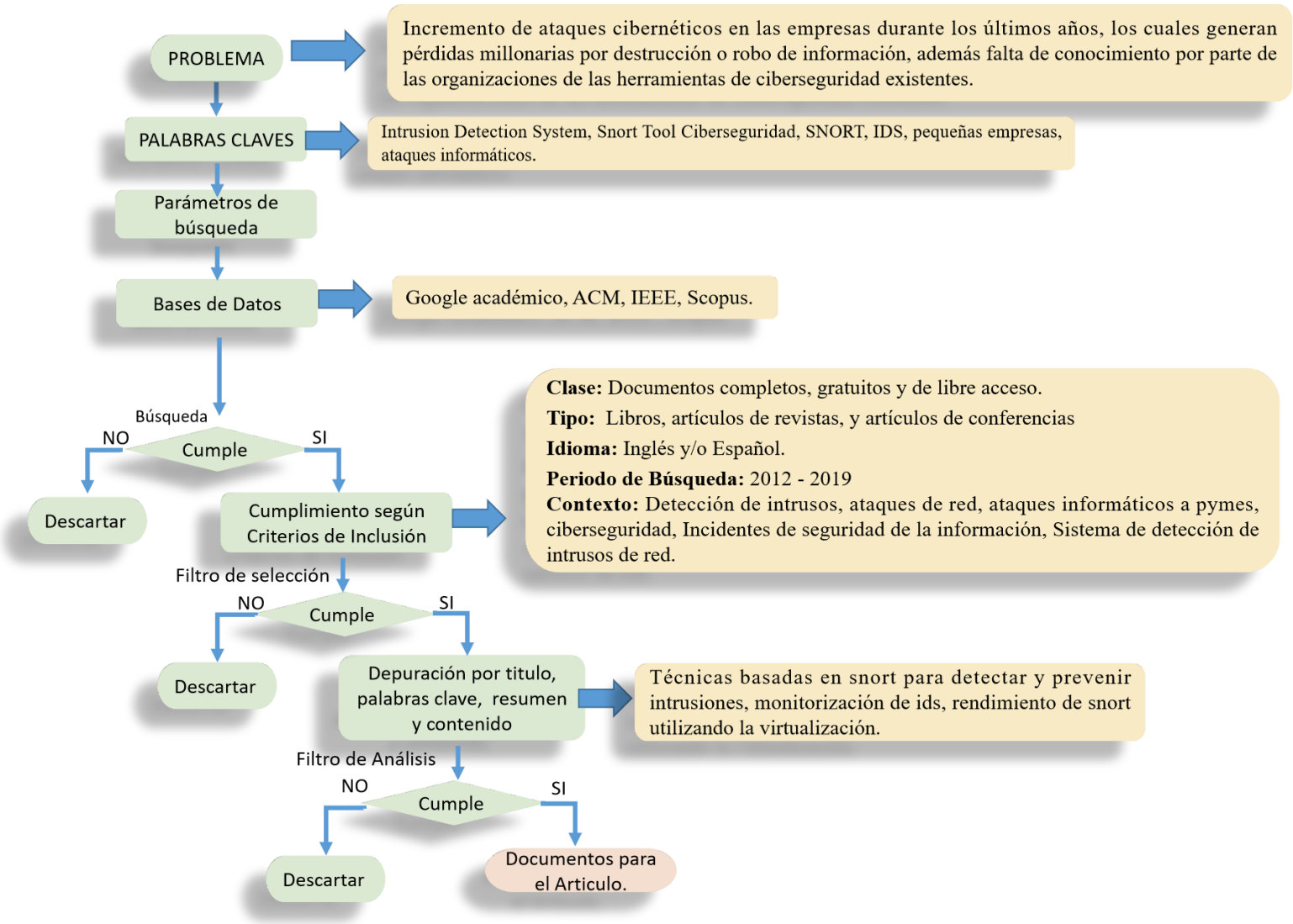

Figura 7 Diagrama de Flujo del Proceso de Búsqueda. Fuente [Autores]

En la base de datos *Google Académico*, se buscaron las palabras claves: Intrusion Detection System, Snort Tool, Ciberseguridad, SNORT, IDS, pequeñas empresas, ataques informáticos, donde se obtuvieron como resultado inicial 1.900 documentos. Se aplicaron los filtros correspondientes a los criterios de inclusión: Texto Completo, fecha de 2012 a 2019, idioma inglés y español quedando 368 documentos. Se aplican filtros por título y resumen y obtienen 61 documentos para luego de una revisión específica y exhaustiva según la temática se incluyen 3 documentos:

1. **Implementación de un sistema de detección y prevención de intrusos (IDS/IPS), basado en la norma ISO 27001, para el monitoreo perimetral de la seguridad informática, en la red de la Universidad Peruana Unión.** El documento muestra la revisión de los componentes de Snort y todas las funcionalidades que nos puede brindar, además crean máquinas virtuales las cuales ayudan a simular el monitoreo del tráfico así como algunos ataques, configuran Snort en modo IDS/IPS, y pasan a crear reglas que ayudan a detectar los ataques y monitorizar el tráfico que se realizan y finalmente se comprueba la eficacia de su detección y prevención, para poder tener un buen control de la red incluyen la norma ISO 27001 la cual ayuda a conocer los métodos de evaluación del tráfico mediante las etapas que esta brinda (Coyla Jarita, Implementación de un sistema de detección y prevención de intrusos (IDS/IPS), basado en la norma ISO 27001, para el monitoreo perimetral de la seguridad informática, en la red de la Universidad Peruana Unión – Filial Juliaca, 2019)

2. **Análisis de la eficiencia de los IDS Open Source Suricata y Snort en las pymes.** Este artículo analiza la eficiencia de dos IDS, Snort y Suricata, dentro de una infraestructura virtualizada con una configuración que organiza el tráfico de paquetes para su mejor análisis y dispositivos de almacenamiento que minimicen la latencia de escritura y lectura de datos, de manera que se puede determinar que IDS en condiciones de altas cargas de trabajo es más eficiente y de esta forma ver como una empresa puede tomar la decisión más compatible con sus objetivos estratégicos (Pacheco, Zambrano B., & Guailacela, ANÁLISIS DE LA EFICIENCIA DE LOS IDS OPEN SOURCE SURICATA Y SNORT EN LAS PYMES., 2019).

3. **Diseño de un sistema de detección de intrusos snort y un sistema trampas tipo honeypots de baja interacción en la red.** Este documento analiza la red con el propósito de identificar cuáles son los protocolos y puertos de tienen mayor tráfico en los servidores, con el objetivo de proponer algunas reglas que sirvan como base para la validación del diseño del sistema de detección de intrusos que se plantea para una subred. Además, se propone el diseño de un sistema de trampas de baja interacción o Honeypots, con el fin de atraer a los posibles atacantes que se están conectando a través de una red interna con el propósito de realizar ataques a algunos de los equipos de la red o a los servidores (MARTÍNEZ FLÓREZ, 2014)

En la base de datos IEEE, se buscaron las palabras claves: Intrusion Detection System, Snort Tool, Ciberseguridad, SNORT, IDS, pequeñas empresas, ataques informáticos, donde se obtuvieron como resultado inicial 483 documentos. Se aplicaron los filtros correspondientes a los criterios de inclusión: Texto Completo, fecha de 2012 a 2019, idioma inglés y español quedando 153 documentos. Se aplican filtros por título y resumen y obtienen 32 documentos para luego de una revisión específica y exhaustiva según la temática se incluyen 4 documentos:

1. **An analysis of various snort based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in Kali Linux environment** El artículo muestra la definición de la herramienta IDS SNORT además presenta su funcionalidad, las ventajas y desventajas que tiene cada paso de la herramienta. Además, se muestra la discusión de varias técnicas que ofrece una visión consolidada de los trabajos de investigación en varios aspectos del rendimiento, como la precisión de detección, la escalabilidad y la capacidad de detectar ataques desconocidos. Nos proporciona un diseño incremental con unas características específicas con una tasa de detección más precisa, además nos describe que el funcionamiento de cada capa (Gaddam & M. Nandhini, 2017)

2. **Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM*)*** El documento presenta como las auditorías de Tecnología de la Información (TI) y Seguridad de la Información (InfoSec) que fueron eficientes en el pasado, están tratando de converger en auditorías de ciberseguridad para abordar las amenazas cibernéticas, los riesgos cibernéticos y los ataques cibernéticos que evolucionan en un agresivo ciber panorama, sin embargo, ante el notorio aumento de ataques informáticos se pone en evidencia la necesidad de un nuevo modelo de auditoria como lo es el Modelo de Auditoría de Seguridad Cibernética (CSAM) evalúa y valida los controles de auditoría, preventivos, forenses y detectives para todas las áreas funcionales de la organización. (Sabillon, Serra-Ruiz, Cavaller, & Cano, 2018)

3. **Detecting SQL Injection attacks using SNORT IDS** Este documento muestra el ataque de inyección SQL y el aumento continuo de fallas encontradas en las aplicaciones web, por lo cual es importante tomar medidas para garantizar la seguridad de los datos utilizando el ids snort el cual por medio de una serie de reglas propuestas y con algunas palabras de firmas logran detectar dicho ataque (Alnabulsi, Islam, & Mamun, 2014)

4. **Automatic SNORT IDS rule generation based on honeypot log** En este articulo integran IDS y honeypot para generar y activar automáticamente reglas de snort por medio del envió de datos del servidor, esta técnica recopila datos los envía al IDS y el IDS los evalúa para generar automáticamente la regla necesaria, una vez esta se activa puede filtrar los paquetes enviados por el usuario en la red, finalmente hace una comparación de la regla generada automáticamente con las reglas predeterminadas por Snort (Sagala, 2015)

En la base de datos *Scopus*, se buscaron las palabras claves: Intrusion Detection System, Snort Tool, Ciberseguridad, SNORT, IDS, pequeñas empresas, ataques informáticos, donde se obtuvieron como resultado inicial 742 documentos. Se aplicaron los filtros correspondientes a los criterios de inclusión: Texto Completo, fecha de 2012 a 2019, idioma inglés y español quedando 416 documentos. Se aplican filtros por título y resumen y obtienen 86 documentos para luego de una revisión específica y exhaustiva según la temática se incluyen 3 documentos:

1. **An intrusion prevention scheme for malicious network traffic based on SDN**. Este documento presenta el sistema de prevención de intrusiones que posee las características de detección y protección de intrusos, el cual es uno de los métodos más importantes para garantizar la seguridad de la red SDN. Además, proponen un esquema de prevención de intrusiones basado en SDN para la seguridad. Este esquema utiliza la capacidad de programación de SDN para crear cuatro módulos en el plano de aplicación del controlador, incluido el módulo de monitoreo de red, el módulo de detección de dirección IP, la detección de paquetes destructivos y el módulo de enlace Snort. (Xiaofeng, Jiahao, & Yifang, 2020)

2. **Implementación del sistema de detección de intrusos** Este articulo aborda los problemas de seguridad relacionados con la intrusión en una red y se centra en la configuración de un Sistema de detección de intrusiones (IDS) en una VLAN y en la detección de varios tipos de ataques en la VLAN. Además, describe varios enfoques para detectar y prevenir los ataques con diferentes técnicas, como la coincidencia de patrones, la decodificación de protocolos, la definición de reglas y firmas. También proponen una arquitectura segura para una LAN con la colocación del sistema de detección de intrusiones utilizando Snort, como kit de herramientas de código abierto en la plataforma Linux. (Siva Kumar, Nanduri, Ashok Kumar, & Sujatha, V., 2020)

3. **Performance evaluation of Snort and Suricata intrusion detection systems on Ubuntu server.** En este documento, se comparan experimentalmente a Snort y Suricata a través de una serie de pruebas para identificar los IDS más escalables y confiables al poner los sistemas bajo mucho tráfico. Los resultados indicaron que Snort tenía una sobrecarga del sistema más baja que Suricata y utilizaba solo un procesador en un entorno multinúcleo. Sin embargo, Suricata utilizó de manera uniforme todos los elementos de procesamiento del entorno multinúcleo y proporcionó una mayor tasa de análisis de paquetes. Para el tráfico malicioso, tanto Snort como Suricata descartaron paquetes con Snort en el lado superior para una velocidad y tamaño de tráfico bajos (Gupta, Alka & Sharma, Lalit Sen, 2019)**.**

Tabla 2
Revisión de la Literatura

Revisión de la literatura	
Palabras Clave	Intrusion Detection System, Snort Tool, Ciberseguridad, SNORT, IDS, pequeñas empresas, ataques informáticos

Bases de datos consultadas	Google Académico, IEEE, Scopus
Cantidad de Referencias Recuperadas	8
Criterios de Búsqueda	Rango de Fecha de la Búsqueda: Entre 2012-2019
	Documentos en inglés, Actas de conferencia

Fuente: Autores

Tabla 3
Antecedentes al Proyecto

TÍTULO	APORTES AL PROYECTO	AUTORES
Análisis de la eficiencia de los IDS Open Source Suricata y Snort en las pymes.	• La implementación de Snort el uso de expresiones regulares y predecesores permite que se puedan generar y agregar reglas para ampliar su funcionalidad. • Pasos de configuración de redes virtualizadas. • Caracterización de Ataques: DOS, Registro de botnet por malware, e inyección SQL.	(Zambrano & Guailacela, 2019)
Un análisis de varias técnicas basadas en snort para detectar y prevenir intrusiones en la propuesta de redes con la herramienta de snort de refactorización de código en el entorno Kali Linux	• Tipos de IDS, sus ventajas y/o desventajas. • Conceptos de Snort • Técnicas de detección de intrusos basadas en Snort	(Gaddam & M. Nandhini, 2017)
Implementación del sistema de detección de intrusos	• Fallos de seguridad en Redes. • Tipos de intrusiones a la red.	(Siva Kumar, Nanduri, Ashok Kumar, & Sujatha, V., 2020)

Fuente: Autores

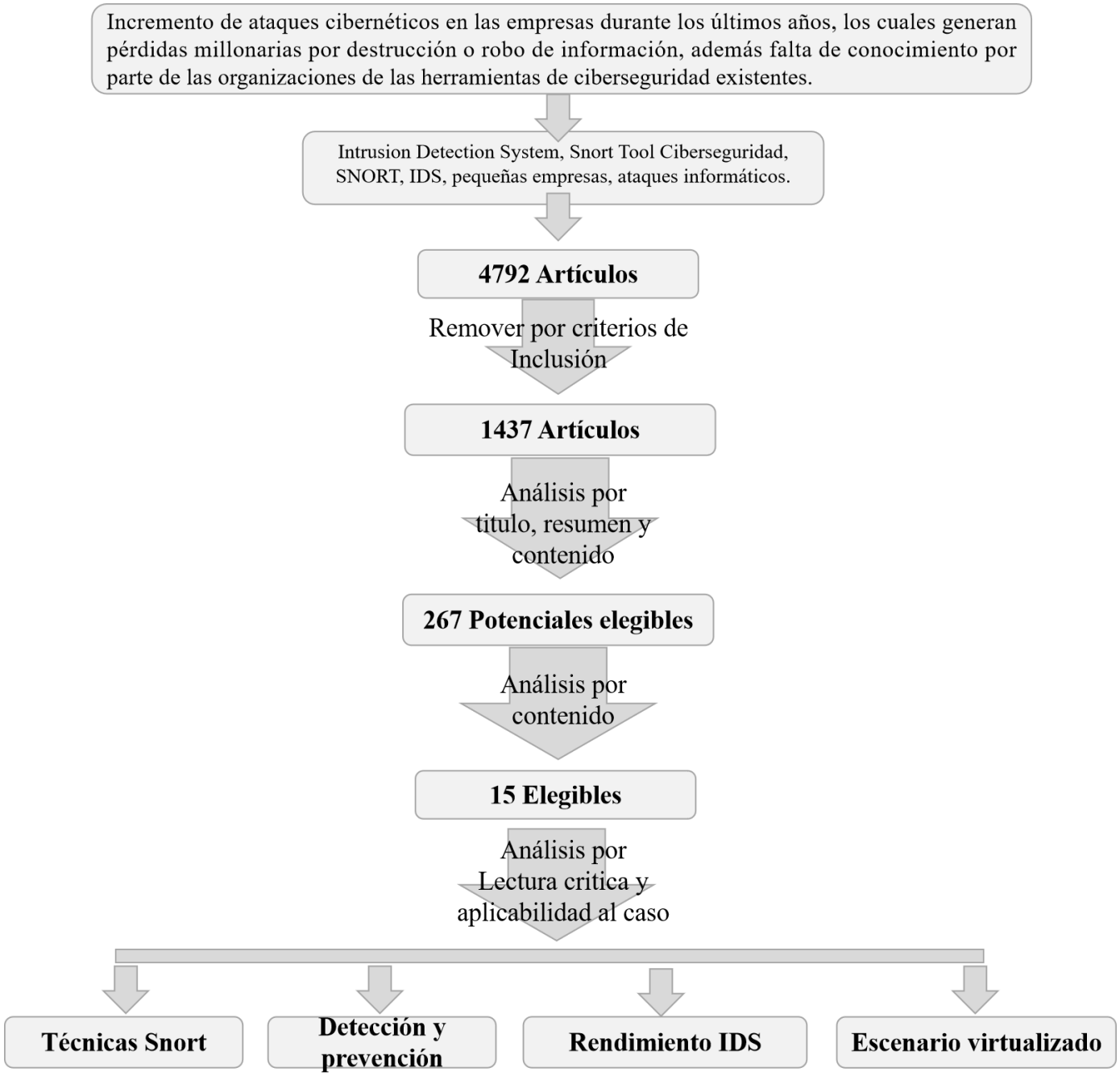

Figura 8 Selección proceso de búsqueda. Fuente [Autores]

6 MARCO REFERENCIAL

6.1 MARCO CONCEPTUALSeguridad de la información

"Preservación de la confidencialidad, la integridad y la disponibilidad de la información, como uno de los activos más valiosos para una organización, independientemente de su formato" (NORMA TECNICA COLOMBIANA 27001, 2013).

6.1.2 Política de seguridad

"Conjunto de directrices o lineamientos, estándares y procedimientos instrucciones que orientan el trabajo definiendo los criterios de seguridad que deben ser adoptados a nivel institucional, con el objeto de establecer, estandarizar y regular la seguridad de los recursos humano y tecnológico." (Clavijo & Ciro Antonio, 2006)

"Conjunto de reglas que define y restringe los tipos de actividades de entidades y partes implicadas en la seguridad" (UIT-R, 2012).

6.1.3 Vulnerabilidades

"Fallas en los sistemas, no diseñadas deliberadamente, sino producto de errores de diseño, configuración o implementación, y que generan oportunidades de ataque haciendo viable una amenaza". (Romero Castro, Figueroa Moràn, & Vera Navarrete, INTRODUCCIÓN A LA SEGURIDAD INFORMATICA Y EL ANÁLISIS DE VULNERABILIDADES, 2018)

6.1.4 Amenazas

"Eventos que pueden dañar o entorpecer programas y/o recursos. Algunas son difícilmente controlables como los desastres naturales o errores humanos, pero que deben ser tenidas en cuenta a la hora de calcular riesgos" (Romero Castro, Figueroa Moràn, & Vera Navarrete, INTRODUCCIÓN A LA SEGURIDAD INFORMATICA Y EL ANÁLISIS DE VULNERABILIDADES, 2018)

6.1.5 Ataque informático

"Consiste en aprovechar una vulnerabilidad en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático, con la finalidad de obtener un beneficio, causando un efecto negativo en la seguridad del sistema, que repercute directamente en los activos de la organización" (Mieres, 2009).

6.1.6 Ciberseguridad

"Conjunto de herramientas, políticas, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno" (ITU-X 1205, 2008).

6.1.7 Detección de intrusión

"Consisten en una estrategia de seguridad que se incorpora mediante un servidor anfitrión en una red local para manifestar intrusiones o accesos no autorizados, buscando advertir a los administradores de red la posibilidad de un incidente que ponga en peligro la infraestructura computacional de una organización". (ITU-X 1205, 2008)

6.2 MARCO TEÓRICO

6.2.1 SISTEMA DE DETECCIÓN DE INTRUSOS

Un sistemas de detección de intrusos o IDS por sus siglas en inglés (Intrusion Detection System), hace referencia a la implementación de un software específico que permite la detección de intrusos como parte esencial de las tecnologías de seguridad de red (Yang et al., 2010). El IDS se basa en un sniffer, el cual actúa como núcleo, que mediante sensores virtuales obtiene el tráfico externo que incide directamente en la red local sea sospechoso o no, para que de esta manera el IDS ayude a reducir el riesgo de intrusión en dicha red. (Yang et al, 2010) En la Figura siguiente se puede observar dos de las opciones de ubicación en una red local.

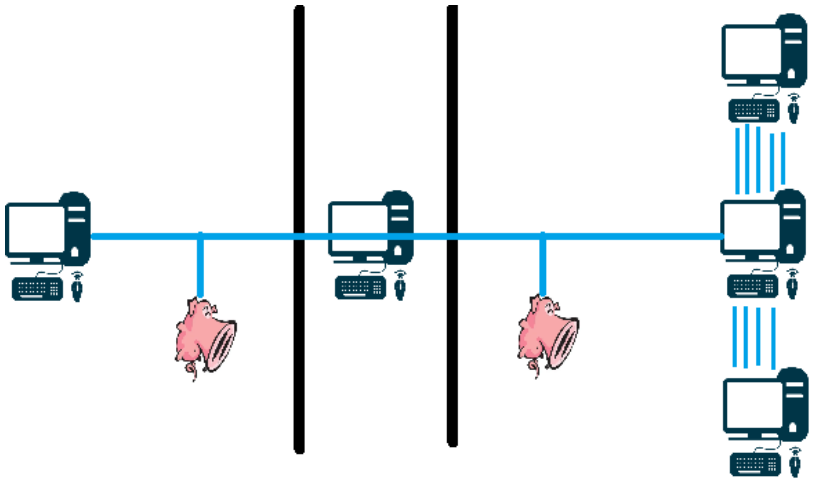

Figura 9 Implementación de IDS. Fuente. Adaptado de (Presente y futuro de los IDS, Departamento de Inteligencia Artificial Barrera García- Orea, Alejandro).

6.2.1.1 Funcionamiento

Un IDS basa su funcionamiento en un barrido completo del tráfico de red o host, analizando los contenidos y comportamientos sospechosos, y comparándolos con respecto a las firmas de ataques conocidos, escáner de puertos abiertos, o paquetes maliciosos, etc. Un IDS se puede integrar junto con un dispositivo que actúe como puerta de enlace o firewall, esto se debe a que un IDS por sí solo no es capaz de detener un ataque. Esta estructura se integra junto con el análisis inteligente del IDS con el poder de bloqueo del firewall, logrando forzar a que los paquetes sean bloqueando para identificar los agentes maliciosos antes de ingresar

a la red o al host donde están instalados.

6.2.1.2 Tipos de IDS

Los IDS se pueden clasificar de acuerdo al ámbito de instalación y al tipo de tráfico que monitorean como: HIDS o NIDS. Algunos ejemplos de estos son: Ossec, Wazuh, Samhain y Snort, Suricata, Bro, Kismet respectivamente.

HIDS (HostIDS):

> **"**Sistema de detección de intrusiones en el host, su principio se fundamenta en el monitoreo de los registros de las actividades de una maquina mientras una sesión se encuentra activa en busca de intrusiones sospechosas por parte de agentes externos o producto de mal uso de recursos por usuarios internos" (Yang et al., 2010).

NIDS (NetworkIDS):

> "Sistema de detección de intrusiones de red, su principio se fundamenta en el monitoreo del tráfico de los paquetes y segmentos de la red buscando coincidencias entre los rastros generados por una intrusión y una serie de patrones previamente definidos como sospechosos". (Cheng-yu et al, 2009)

6.2.2 SNORT

Es un sistema de prevención de intrusos de código abierto (IPS / IDS) capaz de hacer análisis de tráfico en tiempo real y registro de paquetes (SNORT, 2020).

Snort está formado por varios componentes, cada uno de ellos es el encargado de llevar a cabo una tarea específica. En el momento en que circula un paquete por la red, este es capturado por el módulo DAQ, que lo reenvía posteriormente a Snort. A partir de aquí, recorre cada componente de Snort en el siguiente orden:

1. Packet Decode Engine (motor de descodificación de paquetes o simplemente descodificador de paquetes): Una vez que el módulo DAQ envía el paquete a Snort, este pasa por el descodificador de paquetes (Packet Decoder), que se encarga de almacenar toda la información de cada paquete que llegue de la red, como por ejemplo protocolos, IPs de origen y destino, etc., en una estructura de datos para su posterior procesamiento (Zhang, Wei, Yang, & Song, 2020)

2. Preprocessor (preprocesador): Una vez que se descodifica el paquete, se ejecutan los preprocesadores, que pueden analizar e incluso modificar el paquete en cuestión, dependiendo del objetivo de cada preprocesador. También, pueden lanzar alertas, clasificar o descartar un paquete antes de enviarlo al motor de detección (Detection Engine), que cuenta con un alto coste computacional (Zhang, Wei, Yang, & Song, 2020).

3. Detection Engine (Motor de detección): Este componente es considerado como el

corazón de Snort. Toma información del Packet Decoder y de los preprocesadores e inspecciona el contenido del paquete para compararlo a través de su módulo, o plug-in, de detección (Detection) con los patrones de la base de firmas (Zhang, Wei, Yang, & Song, 2020).

4. Output (Salida de Snort): Cuando se ha detectado un paquete sospechoso, ya sea porque un preprocesador lo ha decidido o porque cumple con una regla concreta, este módulo de salida genera una alerta, en el formato que se especifique en el archivo de configuración de Snort (Zhang, Wei, Yang, & Song, 2020).

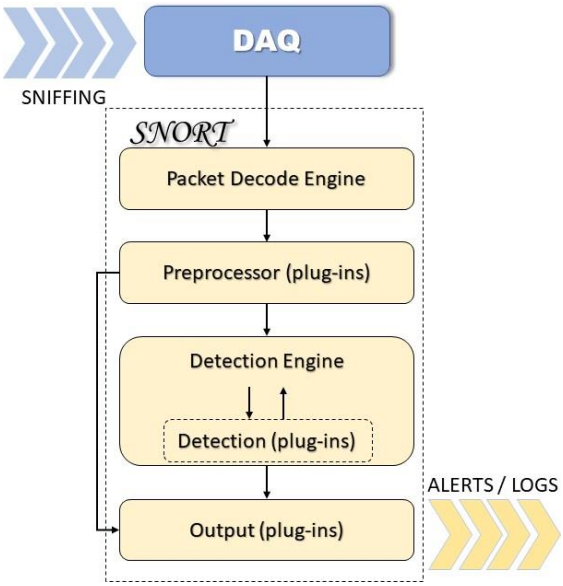

Figura 10 DAQ y Componentes de Snort. Flujo de datos desde la capa de enlace de datos hasta la salida de Snort.

Fuente. Adaptado de (bibing, 2020)

Todos y cada uno de los componentes de Snort juegan un papel importante e imprescindible en el correcto y eficiente funcionamiento de la aplicación. No obstante, no hay que olvidar que el objetivo principal de Snort es detectar posibles ataques. Por tanto, el motor de detección es considerado el componente central del IDS sobre el que girarán el resto de componentes.

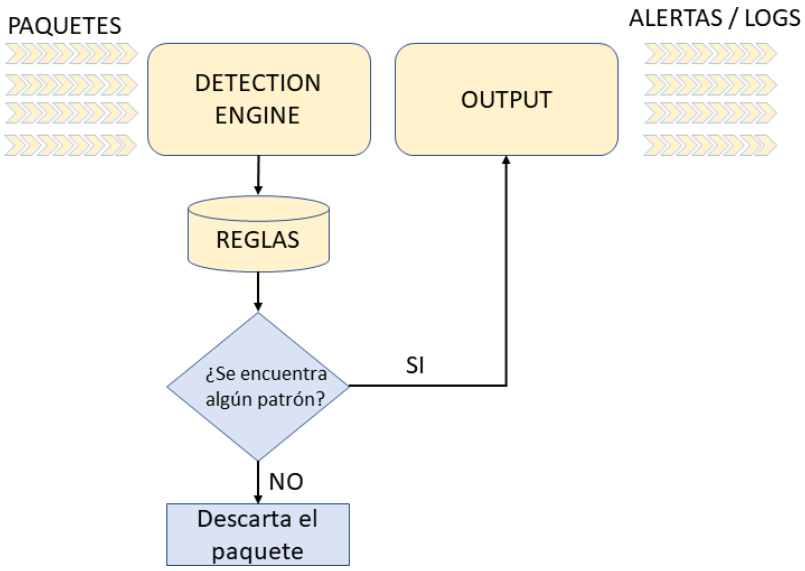

Figura 11 Funcionamiento del motor de detección. Fuente. Adaptado de (Anonimo, 2020).

6.2.3 Firewall

Un firewall es una pieza de software o hardware que verifica cada paquete entrante o saliente entre la computadora, red doméstica o red de compañía para así decidir si acepta o rechaza el paquete. (Bagheri & Shameli-Sendi, 2020)

> "Los firewalls han constituido una primera línea de defensa en seguridad de la red durante más de 25 años. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet. Un firewall puede ser hardware, software o ambos". (CISCO, 2020)

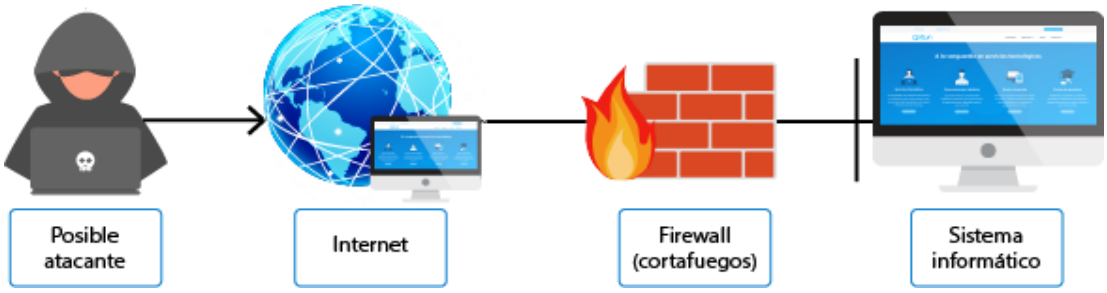

Figura 12 Firewall, Diseño de red con cortafuegos. Fuente. Tomado de (Anonimo, 2020).

Las empresas manejan grandes cantidades de datos, desde información de clientes hasta datos de ventas, acuerdos comerciales, información de empleados, entre otras. Algunos de estos pueden ser datos muy confidenciales, por lo que deben protegerse. Por tanto, debe existir un mecanismo de seguridad informática. (Antiun, 2020)

6.2.4 EDR

Es una tecnología de ciberseguridad que aborda la necesidad de una supervisión en tiempo real, de centrarse en los análisis de seguridad y en la respuesta al incidente de los endpoints corporativos. Ofrece una visibilidad completa de extremo a extremo sobre la actividad de cada equipo de la infraestructura corporativa, administrada desde una única consola, junto con una valiosa inteligencia de seguridad que podría usar un experto de seguridad informático para una investigación y respuesta mayores. (AO Kaspersky Lab, 2020)

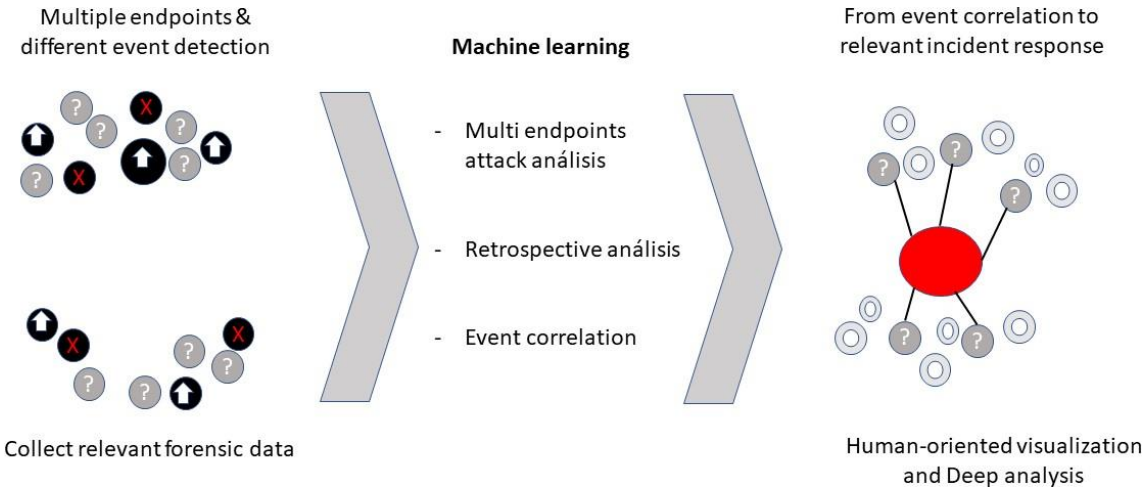

Figura 13 EDR Tecnología de ciberseguridad.

Fuente. Adaptado de (AO Kaspersky Lab, 2020)

Para defenderse de manera eficaz y confiable contra amenazas avanzadas, EPP y EDR deben cooperar, porque EPP controla las amenazas conocidas, mientras que EDR se ocupa de las amenazas desconocidas más complejas. Una plataforma EDR es una herramienta para que se analicen e investiguen y por ende mejoren sus capacidades de defensa, no solo a responder al daño causado por amenazas avanzadas que la protección de endpoints tradicional podría pasar por alto.

6.2.5 Tecnologías de ciberseguridad

Tabla 4
Tecnologías de ciberseguridad

Tecnologías de ciberseguridad			
Técnicas	**Categoría**	**Tecnología**	**Objetivo**
Integridad del sistema	Antivirus	Métodos de firma	Utiliza firmas de código para proteger contra códigos informáticos maliciosos, como los virus y gusanos.
		Métodos de comportamiento	Verifica que los programas que se ejecutan no tengan un comportamiento no autorizado

Tecnologías de ciberseguridad			
Técnicas	**Categoría**	**Tecnología**	**Objetivo**
	Integridad	Detección de intrusión	Puede utilizarse para advertir a los administradores de red de la posibilidad de que ocurra un incidente de seguridad, como la puesta en peligro de archivos en un servidor
Auditoria y supervisión	Detección	Detección de intrusión	Compara el tráfico de red y los registros cronológicos de entrada, del anfitrión para encontrar firmas de datos indicativos de piratas
	Prevención	Prevención de intrusión	Detecta ataques en una red y toma las medidas especificadas por la organización para contrarrestar los ataques. Las actividades sospechosas disparan las alarmas del administrador, así como otras respuestas configurables
	Registro cronológico	Herramientas de registro cronológico	Supervisa y compara el tráfico de red y los registros cronológicos de entrada del anfitrión para encontrar firmas de datos y perfiles de dirección

Tecnologías de ciberseguridad			
Técnicas	**Categoría**	**Tecnología**	**Objetivo**
			de anfitrión indicativos de piratas
Gestión	Gestión de red	Gestión de configuración	Permite el control y la configuración de las redes y la gestión de fallos
		Gestión de parches	Instala las últimas actualizaciones y arreglos de dispositivos de red
	Política	Observancia	Permite a los administradores supervisar e imponer las políticas de seguridad

Recuperado de SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD (ITU-X 1205, 2008)

6.3 MARCO LEGAL Y NORMATIVO

Según el marco normativo y legal nacional e internacional el proyecto desarrollado se reglamenta bajo las siguientes leyes, normas y/o estándares:

6.3.1 Ley 1581 de 2012

La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada. (Normativa, 2012)

Está Ley es importante en el contexto del proyecto ya que para el registro de los usuarios se deben aplicar estrategias que permitan garantizar su cumpliméntenlo para un óptimo manejo de los datos personales de los usuarios.

6.3.2 Ley 1273 de 2009

“Por medio de la cual se modifica el código penal, y se crea un nuevo bien jurídico de la protección de la información y de los datos - y se preservan integralmente los sistemas que

utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones, cuyo objetivo es sancionar todo comportamiento ilícito frente a la comisión de los delitos informáticos en el país.” (MINTIC, 2009)

6.3.3 Ley 11723: "Ley de Propiedad Intelectual" o también como "Ley de Propiedad Científica, Literaria y Artística".

“Esta ley regula todo lo referente a derecho de propiedad de las obras científicas, literarias y artísticas las cuales comprenden los escritos de toda naturaleza y extensión, entre ellos los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales. Además, establece sanciones tanto pecuniarias (multa) como privativas de la libertad (prisión) a quienes violen sus normas.” (Ley De Software Libre En Colombia, 2020)

6.3.4 Política de gobierno digital:

“Promueve el uso y aprovechamiento de las Tecnologías de la Información y la Comunicación para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores que promuevan desarrollo social, garantía de los derechos, satisfacción de necesidades y prestación de servicios de calidad; gobernanza desde la participación y la legitimidad, en un entorno de confianza digital.” (Risaralda, 2019)

Esta política es importante en el contexto del proyecto ya que obliga a las empresas del estado y sugiere a las del sector privado a buscar estrategias que propendan en la protección de la información que almacenan, procesan y trasmiten en sus infraestructuras informáticas.

6.3.5 Estrategia GEL:

“Gobierno en Línea es una estrategia definida por el Gobierno Nacional mediante el Decreto 1151 de 2008. Esta estrategia pretende contribuir a mejorar la eficiencia y transparencia del Estado Colombiano a través de la construcción gradual de un gobierno electrónico.” (MinTIC, 2019)

Esta estrategia de gobierno digital es importante en el contexto del proyecto ya que plantea que las empresas del estado deben incorporar la seguridad de la información para la protección de la información que almacenan, procesan y trasmiten en sus infraestructuras informáticas.

6.3.6 Norma ISO/IEC 27000:2013

“Familia de estándares donde especifica claramente los parámetros sobre seguridad de la información, para desarrollar, implementar y mantener los sistemas de gestión de seguridad de la información.” (Perafán Ruiz & Caicedo Cuchimba, 2014)

“La 27001 Define los requisitos para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información).” (Perafán Ruiz & Caicedo Cuchimba, 2014)

La 27002 “Es una guía de buenas prácticas, describe los controles a seguir dentro del marco de la seguridad de la información; enmarcados en 11 dominios, 39 objetivos de control y 133 controles.” (Perafán Ruiz & Caicedo Cuchimba, 2014)

La 27005 “Suministra directrices para la gestión del riesgo en la seguridad de la información.” (Perafán Ruiz & Caicedo Cuchimba, 2014)

Esta familia de normas es importante en el contexto del proyecto ya que permite a las empresas contar con una guía de buenas prácticas para la gestión de un sistema de seguridad de la información SGSI.

6.3.7 ISO 31000

Recoge una serie de buenas prácticas internacionales que proporcionarán la eficiente gestión de los riesgos a todos los niveles, especialmente a nivel operativo, de gobierno y, muy importante, a nivel de la confianza de las partes interesadas. Por tanto, sirve de complemento perfecto para el resto de nuevas normas publicadas, aportando no sólo el enfoque basado en riesgos, sino un incremento en la seguridad (31000, 2018)

7 DESARROLLO METODOLÓGICO

El proyecto se desarrolló con base a la metodología de investigación aplicada experimental de tipo cualitativo por medio del análisis de intrusiones a la infraestructura de red de pequeñas empresas y teniendo en cuenta el uso de la herramienta SNORT. las intrusiones se implementaron mediante un escenario virtualizado que permitió simular y validar tipos de ataques reales y posibles técnicas de evasión. Para ello se tuvieron en cuenta cuatro fases:

Figura 14 Fases de la investigación de tipo cualitativo.

Fuente. Adaptado de (Monje Álvarez, 2011)

7.1 FASE PREPARATORIA

En esta etapa, se pueden distinguir dos fases principales, a saber: la etapa de reflexión y la etapa de diseño. En la primera fase, se utilizaron las habilidades adquiridas en el semillero de seguridad informática, y la búsqueda sistemática de información buscando establecer un marco teórico-conceptual que permitiera dar inicio a la investigación desde este marco. En la fase de diseño, se generaron las actividades a ser ejecutadas en fases posteriores. (Monje Álvarez, 2011)

7.1.1 Actividades realizadas en esta fase:

Se definió una búsqueda de información en las bases de datos IEEE, Scopus, ACM, Google académico de conformidad a un protocolo de búsqueda que se define en el apartado 5, con él se logró obtener un recurso de información importante que luego fue depurada para ser tomada como insumo del proceso contextual del proyecto. Igualmente se consultó y recopilo la información necesaria sobre la herramienta Snort en los repositorios oficiales buscando comprender su funcionalidad y así realizar las actividades pertinentes para el proyecto.

7.2 FASE DE TRABAJO DE CAMPO

Durante esta fase de investigación del proyecto se desarrolló cada uno de los pasos, la verificación y el contraste de los datos.

> "La investigación se hace paso a paso, los datos se contrastan una y otra vez, se verifican, se comprueban; las dudas surgen y la confusión es preciso superarla. El investigador ha de ser meticuloso, cuidando cualquier detalle. Sobre todo, en lo que se refiere a la recogida de información, su archivo y organización." (Monje Álvarez, 2011)

7.2.1 Actividades realizadas en esta fase

Se realizó el diseño de un escenario controlado para poder simular una red interna en la cual se realizaron pruebas de ataques seleccionados teniendo en cuenta la información obtenida de la revisión de la literatura y se probó el rendimiento de la herramienta a la hora de detectar dichos ataques con algunas reglas ya establecidas.

7.3 FASE ANALITICA

Se realiza después de terminar el trabajo de campo, para analizar detalladamente los datos recogidos en el campo. Es difícil hablar de una estrategia o procedimiento para el análisis de los datos. No obstante, es posible establecer unas tareas que constituyen el proceso analítico básico. A) Reducción de datos. B) Disposición y transformación de datos. C) Obtención de resultados y verificación de conclusiones.

7.3.1 Actividades realizadas en esta fase

Teniendo en cuenta las pruebas realizadas se observó un buen rendimiento por parte de la herramienta Snort detectando los ataques en tiempo real y mostrando una alerta en tiempo eficaz.

7.4 FASE INFORMATIVA

El proceso de investigación culminó con la presentación y difusión de resultados. De esta manera, los investigadores no solo tienen una comprensión más profunda del fenómeno en estudio, sino que también comparten esta comprensión con otros. El informe debe ser un argumento persuasivo, proporcionar sistemáticamente datos para respaldar el caso del investigador y refutar otras explicaciones. (Monje Álvarez, 2011)

Se definió unas recomendaciones de seguridad informática para las pymes teniendo en cuenta los resultados obtenidos de la herramienta Snort y la revisión bibliográfica, resaltando controles, procedimientos y buenas prácticas que las empresas deberían realizar para evitar ser víctimas de ataques y robo de información.

8 CONTEXTO DE CIBERSEGURIDAD EN PYMES

8.1 INTRUSIONES DE SEGURIDAD EN PYMES

La nueva realidad que representa el acceso a tecnologías de la información y comunicación TIC ha brindado múltiples beneficios para las pequeñas y medianas empresas (pymes), sin embargo, también ha generado un escenario propicio para que se trasladen a su infraestructura tecnológica, sistemas informáticos y redes diversos tipos ataques. Según Kaspersky actualmente ninguna organización está a salvo de ser víctima de un ciberataque. (Kaspersky, 2020). Esta nueva problemática conlleva a que las pymes sean más vulnerables no solo por su falta de estrategias y recursos a nivel del cómo se gestiona la seguridad de la información, sino además por la falta de concienciación y conocimiento llevándolas a ser más vulnerables. (Martínez Cortes, 2015) Ello conlleva a que sea de vital importancia explorar los diferentes aspectos que conforman el contexto de ciberseguridad, mediante el reconocimiento de los tipos de vulnerabilidades, así como los vectores de ataque más comunes, que permiten la generación de riesgos e intrusiones que se materializan en incidentes de seguridad informática.

8.1.1 ERRORES COMUNES DE LAS PYMES EN RELACIÓN A LA SEGURIDAD DE LA INFORMACIÓN

Con el arribo a de las organizaciones al ciberespacio sin importar su tamaño se han incrementado los riesgos dejándolas expuestas a diversos tipos de amenazas donde los ciberdelincuentes, han aprovechado no solo la falta capacitación sino la falta de conciencia de usuarios de los sistemas informáticos facilitándoles su trabajo (TICbeat, 2014). Dentro de las malas prácticas más habituales en pymes se encuentran las que se describen a continuación:

- El exceso de confianza: Los usuarios desprevenidos generalmente suelen confiar en los enlaces que se encuentran en sus redes sociales, correo electrónico o motores de búsqueda, lo cual le lleva a abrir archivos desconocidos si percatarse que su contenido puede ser malicioso. Generalmente los empleados de las pymes usan las redes sociales o correos electrónicos para comunicarse con clientes, proveedores o compañeros de trabajo, sin tener en cuenta que estas plataformas pueden estar corrompidas con algún tipo de software malicioso haciendo que sean presa fácil de los atacantes (Gao & Zhu, 2015).
- Una misma clave para todo: Los usuarios suelen utilizar indistintamente las mismas credenciales, usuario y contraseña sin importan el ámbito donde se encuentran ya sea personal o empresarial. Igualmente, la fortaleza de dichas contraseñas no es lo suficientemente robusta, o es conocida por agentes externos a la organización como familiares o parejas o las suelen anotar comúnmente en una agenda, libreta o incluso en un papel en su escritorio o debajo del teclado. (Bachmann, 2014)

- Configuraciones por default, software ilegal o desactualizado: Los usuarios generalmente usan las configuraciones básicas para sus dispositivos de cómputo, o usan sistemas operativos piratas que no les permiten hacer sus actualizaciones pertinentes, por lo que no se tienen en cuenta las correcciones de seguridad o parches a vulnerabilidades por parte del fabricante. (Yusuf et al., 2017) (Sabetghadam et al., 2009)
- Utilizar dispositivos personales con información empresarial: Los usuarios usan sus equipos de cómputo o dispositivos móviles personales, así como sus correos personales con información propia de la empresa la cual es confidencial, y se pone constantemente en riesgo ya que los niveles de seguridad de dichos entornos personales son generalmente insuficientes. (Asghar et al., 2008).

8.2 VULNERABILIDADES EN ENTORNOS WEB

La arquitectura de un sitio web está compuesta por diversos componentes, los cuales realizan tareas muy precisas y especificas aumentando su complejidad y por ende sus vulnerabilidades, por lo que están comúnmente sujetos a múltiples ataques. A continuación, en la siguiente tabla se presentan algunas de las vulnerabilidades más típicas.

Tabla 5
Vulnerabilidades web

VULNERABILIDAD	DETALLE
Clickjacking	El secuestro de clics suele estar relacionado con scripts maliciosos que se encuentran embebidos en sitios web que comúnmente son consultados por usuarios desprevenidos, para redireccionarlos a un sitio web malicioso. Este se aprovecha de las capas de transparencia o marcas de agua para que se dé clic en un botón o enlace oculto. (Sivaraman & Khanna, 2016)
Cross Site Scripting (XSS)	La inserción de código en sitios cruzados o XSS permite insertar código malicioso en un sitio web, para evitar el acceso al sitio o realizar suplantación de identidad. Existen varios tipos de XSS: que se basa en DOM XSS, No XSS, XSS persistente, DOM XSS, y XSS No persistente. (Pranathi et al., 2018)
Falsificación de solicitudes entre sitios / CSRF	CSRF se basa en la confianza del usuario en el navegador seleccionado en lugar de un sitio específico, haciendo que envíen solicitudes maliciosas, desde sitios reales que no cierran sesiones abiertas en el navegador exponiendo la identidad y privilegios de la víctima forzándolo a realizar operaciones que normalmente no realizaría (Farah et al., 2016)

VULNERABILIDAD	DETALLE
Ejecución remota de código	Consiste en la ejecución de scripts de forma remota para conocer los fallos en un sitio web con el fin de explotar vulnerabilidades a nivel web, insertar malware o abrir puertas traseras obteniendo acceso y control del sistema. (Mohammad & Pourdavar, 2010)
Inclusión de archivos locales (LFI) y remotos (RFI)	La inclusión de archivos se produce cuando se utilizan variables controladas en una aplicación web para obtener una ruta al código logrando controlarlo en tiempo real de ejecución (A. Begum, MM Hassan, 2016)
Inyección SQL	Permite la inyección de scripts con sentencias SQL en un sitio o aplicación web que tiene conexión con bases de datos para la manipulación de su comportamiento y la obtención de privilegios de administrador mediante consultas con parámetros no deseados. (Kara & Aydos, 2019)
Redirección de URL	Toma parámetros específicos que no son verificados redirigiendo a los usuarios de un sitio web, por ejemplo mediante un phishing donde las víctimas se redireccionan a un sitio web malicioso (Liu & Zhang, 2019)

Fuente: Adaptado por los autores

8.2.1 VULNERABILIDADES EN HERRAMIENTAS DE ADMINISTRACION DE CONTENIDOS

Dos de las herramientas más populares en las Pymes para la gestión de contenidos por su facilidad y bajo costo de implementación, así como su robustez son WordPress y Joomla. Sin embargo, gracias a estas mismas cualidades y a las diversas vulnerabilidades que tienen implícitas, estas plataformas son muy apetecidas por los atacantes.

8.2.1.1 VULNERABILIDADES EN WORDPRESS

Según W3Techs WordPress es una de las plataformas de gestión de contenidos más populares con una cuota en el mercado de cerca del 63%. (Koskinen, Ihantola, & Karavirta, 2012) Esto lo hace muy apetecido por las pymes, pero gracias a su alto uso, también lo son por los atacantes en búsqueda de vulnerabilidades para atacar. A continuación, en la siguiente tabla se presentan algunas de las vulnerabilidades más típicas en los plugin de WordPress.

Tabla 6
Vulnerabilidad en WordPress

PLUGIN	VULNERABILIDAD	VALORACIÓN ESCALA CVSSv3
Page Layer: Proporciona soporte en el desarrollo de sitios web mediante un editor que permite arrastrar y soltar. (pagelayer & WordPress, s.f.)	Se presentan brechas para la falsificación de solicitudes entre sitios (CSRF), lo que permite enviar solicitudes de actualización para configuraciones de un plugin. (Popescu & Cernica, 2019)	8.8 (Security, 2020)
	Se causa por acciones AJAX desprotegidas, para inyectar código JavaScript que permite crear cuentas de administrador falsas para redirigir a los usuarios a sitios maliciosos. (Petrică, Axinte, & Bacivarov, 2017)	7.4 (Security, 2020)
Elementor Pro: Versión premium de "Elementor Page Builder", permite la creación de sitios web automáticamente. (WordPress.org, 2020)	Permite un control completo del sitio web, suplantando un usuario registrado para cargar archivos para una ejecución remota de código (Hills, 2016)	9.9 (Security, 2020)

Fuente: Adaptado por los autores

8.2.1.2 VULNERABILIDADES EN JOOMLA

Junto a WordPress Joomla es otra de las herramientas para la gestión de contenidos más populares por su versatilidad en la implementación de sitios web dinámicos de manera fácil y rápida, esto lo hace altamente apetecido también por los atacantes. A continuación, en la siguiente tabla se presentan algunas de las vulnerabilidades más típicas en los plugin de Joomla.

Tabla 7
Vulnerabilidades en Joomla

PLUGIN	VULNERABILIDAD	VALORACIÓN ESCALA CVSSv3
CVE-2020-10243	La conversión de variables SQL no se ejecuta de manera correcta, haciendo que se puedan realizar ataques de inyección SQL. (Patel, Rathod, & Parikh, 2011)	9,8 (Vulnerabilidades en Joomla y Drupal, 2020)
CVE-2020-10239	Una incorrecta gestión del control de acceso para el campo com_fields en SQL que permite privilegios de usuarios administradores a usuarios básicos. (Patel, Rathod, & Parikh, 2011)	8.8 (Vulnerabilidades en Joomla y Drupal, 2020)
CVE-2020-10238	Versiones anteriores a 3.9.16. permiten que en com_templates no se hagan comprobaciones de ACL, ocasionando un alto impacto en la confidencialidad. (Vulnerabilidades en Joomla y Drupal, 2020)	7.5 (Vulnerabilidades en Joomla y Drupal, 2020)

Fuente: Adaptado por los autores de (Vulnerabilidades en Joomla y Drupal, 2020).

83 VULNERABILIDADES EN BASES DE DATOS

Un gran número de pymes no cuentan con bases de datos lo suficientemente robustas en cuanto a su seguridad, no implementan buenas prácticas de desarrollo o codificación segura para evitar ataques limitándose únicamente a la gestión de su usabilidad, lo cual que las hace altamente vulnerables a ataques informáticos con el fin de acceder, robar o modificar la información allí contenida. (Ciberseguridad, 2019) A continuación, en la siguiente tabla se presentan algunas de las vulnerabilidades más comunes en bases de datos mal diseñadas o gestionadas.

Tabla 8
Vulnerabilidades en base de datos

VULNERABILIDAD	DESCRIPCIÓN
Software desactualizado	Generalmente las aplicaciones de código abierto usadas en gestión de bases de datos son muy vulnerables, dado que sus desarrolladores no publican regularmente parches de seguridad lo que incide en un riesgo inherente alto. (Ciberseguridad, 2019)

VULNERABILIDAD	DESCRIPCIÓN
Inyección SQL / NoSQL	Implica la ejecución de sentencias SQL o no SQL arbitrarias en las diferentes consultas que se gestionan por la base de datos las cuales pueden ser generadas por aplicaciones web o encabezados HTTP. (Katsunuma, y otros, 2006)
Desbordamiento de búfer	Cuando no se les da un tamaño adecuado a los tipos de variables o datos en los bloques de almacenamiento de tamaño fijo se sobre escribe el buffer de memora produciendo un desbordamiento, que además puede almacenar datos en direcciones de memoria contiguos como base para lanzar ataques más sofisticados. (Grechko, Babenko, & Myrutenko, Secure Software Developing Recommendations, 2019)
No filtrado de peticiones	Se inyectan múltiples solicitudes a la base de datos haciendo que, no pueda responder las solicitudes legítimas volviéndose inestable ocasionando una Denegación de servicio. (Zhang, Bi, Bai, & Li, 2018)
No restringir conexiones o dispositivos a través de sesiones o permisos	Se puede contaminar la base de datos con software malicioso a través de cualquier dispositivo terminal conectado a la red de la base de datos que no esté restringido. (Samantray, Tripathy, & Das, 2019)

Fuente: Apadtado por los autores.

8.4 VULNERABILIDADES EN ENTORNOS DE RED

La infraestructura de red de una organización está compuesta por diversos dispositivos e interfaces, los cuales realizan tareas muy específicas, lo cual aumenta su complejidad y por consiguiente sus vulnerabilidades, llevándolas a estar expuestas continuamente a múltiples ataques. A continuación, en los siguientes apartados se presentan algunas de las vulnerabilidades más comunes a nivel de entornos inalámbricos, dispositivos de red e IoT.

8.4.1 VULNERABILIDADES EN MIKROTIK

Tabla 9
Vulnerabilidades en Mikrotik

VULNERABILIDAD	DESCRIPCIÓN
Recorrido de ruta relativo en NPK	Las versiones inferiores a RouterOS 6.44.5 permiten la creación de directorios actualizando el campo de nombre del paquete, donde si un cliente instala un script malicioso podrá tener Shell de desarrollador. (Ceron, Scholten, Pras, & Santanna, 2020)

VULNERABILIDAD	DESCRIPCIÓN
Validación insuficiente del origen de actualización	El RouterOS 6.44.5 no comprueba el origen del paquete de actualización en el modo automático, lo que permite engañarlo para actualice una versión anterior y restablecer todos los nombres de usuario y contraseñas. (Ceron, Scholten, Pras, & Santanna, 2020)
Protección de solicitudes de DNS / caché Insuficiente	Las versiones inferiores a RouterOS 6.44.5 permiten consultas remotas de DNS a través del puerto 8291 a atacantes no autenticados, donde las respuestas de DNS son almacenadas en el caché llevando a un envenenamiento de caché. (Ceron, Scholten, Pras, & Santanna, 2020)
Manejo inadecuado de la respuesta de DNS	Las versiones inferiores a RouterOS 6.44.5 son vulnerables a ataques de datos no relacionados con DNS, permitiendo agregar todos los registros y envenenar el caché DNS con registros incorrectos. (Ceron, Scholten, Pras, & Santanna, 2020)

Fuente: (Ceron, Scholten, Pras, & Santanna, 2020)

8.4.2 VULNERABILIDADES EN SSH

Tabla 10
Vulnerabilidades en Ssh

VULNERABILIDAD	DESCRIPCIÓN
CVE-2018-10933	Vulnerabilidad en librería libssh, que permite conectarse a un servidor sin necesidad de contraseña. (Albrecht, Paterson, & Watson, 2009)
CVE-2018-15473	En varias funciones de autenticación en OpenSSH, no se genera una lista de usuarios válidos, lo que permite adivinar los nombres de usuario. (Albrecht, Paterson, & Watson, 2009)

Nota: información tomada de (Albrecht, Paterson, & Watson, 2009)

8.5 VULNERABILIDADES EN ENTORNOS WIFI

En la actualidad las redes inalámbricas son una solución que ha permitido a las pymes una mayor versatilidad en sus entornos de red por lo cual su implementación es muy popular. Sin embargo, este tipo de entornos está expuesto a múltiples vulnerabilidades. A continuación, en la siguiente tabla se presentan algunas de las vulnerabilidades más representativas.

Tabla 11
Vulnerabilidades Wi-Fi

PROTOCOLO	DEFINICIÓN	VULNERABILIDAD
WEP	Pretende brindar la misma seguridad de una red cableada, implementando un vector de inicialización, un mecanismo de detección de errores CRC32 y el criptosistema simétrico RC4 para la generación de claves. (Lashkari, Towhidi, & Hosseini, 2009)	Al usar el mismo vector de inicialización para cada paquete de datos se pueden generar respuestas con suficientes vectores de inicialización desde el punto de acceso lo que permite que mediante análisis estadísticos se pueda encontrar la clave. (Sandirigama & Idamekorala, 2009)
WPA	Utiliza el mecanismo TKIP para encriptar mensajes, a diferencia del vector IV, genera una diferente para cada paquete de cada mensaje. digital (Potter, 2003)	Al implementar WPS se simplifica el esquema de conexión de los clientes de la red, el cual mediante un mecanismo de 8 bits que debe coincidir entre los dispositivos permite la conexión. El tamaño de 8 bits no es suficiente y lo hace inseguro ante ataques de fuerza bruta. (Liu, Jin, & Wang, 2010)
WPA2	Cambia el mecanismo TKIP por el algoritmo AES. Implementa un handshake de 4 vias *(4 way handshake)* para la conexión entre el host y el anfitrión (Adnan, Abdirazak, & Sad, 2015)	Al negociar la clave utilizar cifrado en el paso 3, pero no notifica al punto de acceso cuando el cliente recibe la clave haciendo que se envié repetitivamente, exponiéndose a ataques de hombre del medio y suplantación de cliente para capturar la clave y crackearla por fuerza bruta o diccionario (Fehér & Sandor, 2018)
WPA3	Busca prevenir ataques de crackeo de contraseñas gracias a la implementación del protocolo de autenticación SAE (Autenticación Igualitaria Simultánea) (Vanhoef & Ronen, 2020)	Vulnerable en el uso del algoritmo de curvas elípticas (CVE-2019-13377), el cual es la base del cifrado en WPA3, permitiendo generar un canal auxiliar para determinar el tiempo e información de cifrado

PROTOCOLO	DEFINICIÓN	VULNERABILIDAD
		para forzar el uso de contraseñas. (Vanhoef & Ronen, Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd, 2020)
RADIUS	Se basa en el uso de UDP sobre el puerto 1812 para el establecimiento de la conexión y autenticación de red entre clientes y puntos de acceso en un esquema cliente-servidor. (Feng, 2009)	Vulnerable en el algoritmo de autenticación extensible EAP-pwd, (CVE-2019-13456) que permite un ataque de canal lateral para obtener contraseñas y acceder a la información necesaria para las redes cifradas. (Feng, Analysis, Implementation and Extensions of RADIUS Protocol, 2009)

Fuente: Adaptado por los autores.

8.5.1 TPLINK

Uno de los dispositivos inalámbricos comerciales que más usan las pymes por sus altas tasas de transmisión permitiendo mayores capacidades y rendimiento es TPlink. A continuación, en la siguiente tabla se presentan algunas de las vulnerabilidades más representativas.

Tabla 12
Vulnerabilidades en TPLINK

VULNERABILIDAD	DETALLES	VALORACIÓN ESCALA CVSSv3
CVE-2019-15060	El Traceroute en la referencia TL-WR840N v4 con de firmware 0.9.1 3.16 permite la ejecución de código remoto mediante una carga útil que se ubica en el campo de entrada de la dirección IP.	6.5
CVE-2019-13614	CMD_SET_CONFIG_COUNTR Y junto a las versiones anteriores del depurador del Archer C1200 1.0.0 Build 20180502 rel.45702 permiten desbordamiento de búfer	7,5

VULNERABILIDAD	DETALLES	VALORACIÓN ESCALA CVSSv3
	basado en la pila, dando lugar al envío de payloads para ejecutar código malicioso o DoS.	
CVE-2019-13613	versiones anteriores de CMD_FTEST_CONFIG en Archer 1.0.0 Build 20180502 rel.45702 (EU) junto a las versiones anteriores del depurador permiten desbordamiento de búfer basado en apilamiento, dando lugar al envío de payloads para ejecutar código malicioso o DoS.	7,5
CVE-2019-13268	Reenvió de solicitudes ARP entre clientes y punto de acceso, como parte de los paquetes de transmisión, haciendo que la filtración actúe como canal para que el remitente envié solicitudes a otros clientes en la red.	5,8
CVE-2019-13267	En la transferencia desde la red de host a la de invitados, un cliente dejará el grupo IGMP, allí se usa la IP general de la red para crear un paquete de consulta IGMP y reenviarlo a la red de invitados donde se transmiten datos en el campo IP que es de control absoluto del remitente.	5,8

Fuente: Apadtado por los autores de (DETAILS, 2020)

8.6 VULNERABILIDADES EN IOT

Las diversas funciones de los dispositivos inteligentes en IoT proporcionan múltiples formas de mejorar la industria o los ambientes cotidianos. Aunque IoT representa un beneficio en general, sus dispositivos también pueden introducir puntos de acceso y riesgos a las infraestructuras de red. A continuación, en la siguiente tabla se presentan algunas de las vulnerabilidades más representativas.

Tabla 13
Vulnerabilidades en IoT

VULNERABILIDAD	DETALLE
Seguridad física deficiente	Debido a su autonomía y ubicación física en entornos no

VULNERABILIDAD	DETALLE
	supervisados los dispositivos IoT pueden ser accedidos fácilmente permitiendo daños físicos, o accesos a su esquema de cifrado, a copias de firmware o a agregar nuevo hardware que destruya o corrompa su control.
Energía insuficiente	La energía limitada y la falta de fuentes o mecanismos de renovación automatizados en los dispositivos IoT permiten generar mensajes legítimos que se pueden corromper cuando se agota la energía almacenada haciendo que no se puedan utilizar por los usuarios y/o procesos.
Autenticación inadecuada	La capacidad y potencia informática limitadas en el paradigma de IoT, no permiten la generación de mecanismos de autenticación robustos, permitiendo que se agreguen funciones para agregar nodos maliciosos que logran afectar los dispositivos y las comunicaciones IoT, así como la integridad de los datos.
Cifrado inadecuado	La limitada capacidad de procesamiento y recursos de memoria de los dispositivos IoT, hacen que haya una baja solidez en cuanto al diseño e implementación de algoritmos o estrategias para encriptar afectando la solidez, y efectividad de los algoritmos llevando a que se puedan eludir fácilmente.
Puertos abiertos innecesarios	Los dispositivos IoT suelen tener puertos abiertos por default, generar sockets cuando se ejecutan servicios innecesarios que pueden ser vulnerables, permitiendo ser un puente o punto de conexión para el reconocimiento y acceso a los sistemas.
Gestión de acceso insuficiente	La baja implementación de mecanismos de gestión de credenciales y controlar el acceso no autorizado en los dispositivos de IoT permiten el uso de contraseñas débiles o predeterminadas de fabrica que no requieren cambiarse periódicamente, esto sumado a que no se cuenta con un esquema de gestión de permisos de usuario permiten ganar acceso no autorizado con perfil de usuario administrador.
Inadecuada administración de parches	Muchos dispositivos IoT no cuentan con parches de seguridad o mecanismos de actualización automático del firmware, y cuando los tienen no garantizan la integridad de las actualizaciones, siendo vulnerables a modificaciones o malware que aumentan el vector de ataque.
Malas prácticas de programación	Los hábitos de programación en dispositivos IoT son seguros, que usan al root como punto de acceso principal, sumados a la falta de un mecanismo TLS como capa de conexión segura, hacen que el riesgo en los componentes de

VULNERABILIDAD	DETALLE
	seguridad de los numerosos firmwares aumente para la generación de puertas traseras, desbordamientos de búfer, o accesos no autorizados.
Mecanismos de auditoría insuficientes	Los dispositivos de IoT no cuentan con mecanismos de auditoria o procedimientos de registro lo cual permite que puedan ocultarse actividades maliciosas sin que haya un control oportuno.

Fuente: Apadtado por los autores de (Neshenko et al., 2019)

8.6.1 HERRAMIENTA SHODAN

Como parte del contexto de vulnerabilidades en entornos de red e IoT se revisa la herramienta Shodan, la cual consiste en un motor de búsqueda en línea que permite encontrar información detallada sobre dispositivos como de red o IoT conectados a Internet, permitiendo encontrar dispositivos vulnerables por ejemplo en cámaras, sensores, routers, servidores entre otros que los usuarios o administradores no securizan por malas prácticas de configuración como configuraciones de fabrica exponiéndose públicamente a agentes maliciosos con tan solo tener la dirección IP de la organización (Albataineh & Alsmadi, 2019).

Alguna de la información que Shodan devuelve, consiste en datos generales de ubicación del servidor IP, el proveedor de servicios de Internet, la última fecha de actualización, el nombre de host y el ASN, las tecnologías web como jQuery, MySQL, PHP, Bootstrap, Yoast SEO, WooCommerce, recaptcha, los puertos abiertos y los protocolos y servicios usados como ftp, tcp, udp, dns y http, junto a la información de usuarios anónimos, tipo de privacidad y comandos que se puede reconocer en el sitio. También en muchos casos se muestra el certificado digital, con versión, fecha de vencimiento, algoritmo de firma, identificador de clave de autorización, política de certificado real y método para acceder a la información de autorización entre otros datos. (NetCloud Engineering, 2019)

8.7 VECTORES DE ATAQUE

Una vez identificado el contexto con los tipos de vulnerabilidades e intrusiones más comunes en el ámbito de ciberseguridad en pymes, se hace un resumen con la descripción de los vectores de ataque más representativos.

Tabla 14
Vectores de ataque

TIPO DE INCIDENTE	DESCRIPCIÓN	IMPLEMENTACIÓN
Inyección de código SQL	Se inserta código SQL en un campo de texto para su ejecución aprovechando que el Server SQL ejecuta las consultas válidas que se reciben. (Su & Wang, 2018)	La inserción de código SQL permite enviar código directamente en variables especificadas por un agente externo haciendo que se puedan concatenar y se ejecutan comandos SQL para la manipulación de bases de datos que el motor reconoce y ejecuta como consultas SQL validas logrando falsificar identidades, obtener y divulgar información como contraseñas o información relevante, eliminar total o parcialmente la base de datos, cambiar el nombre de las tablas, generar o anular transacciones, llevando incluso ser administrador. (Micosoft, 2017)
SQL Injection por error	Permite de manera sencilla obtener cualquier tipo de acción sobre la base de datos referente a su estructura, tablas, nombres de campos y los datos (H1RD SECURITY, 2017)	La generación de consultas SQL en un campo de texto de la aplicación o sitio web de front-end por ejemplo mediante la sentencia SQL: " ' or 1=1 – " , entre otras hace que se puedan realizar consultas sobre la base de datos para tener acceso a los datos que gestiona el back-end y realizar acciones de gestión no autorizada sobre su estructura (H1RD SECURITY, 2017).
SQL Injection por unión	Permiten extraer de información de la base de datos cuando las dos consultas tienen una misma estructura mediante el operador unión el cual puede ser utilizado para generar un select que simule una consulta original, necesitando únicamente conocer el nombre de la tabla, su cantidad de columnas y el tipo de datos (Martinez, 2017)	Se busca que la aplicación o sitio web en su front-end devuelvan un resultado donde se pueda agregar el resultado de otra consulta SQL al resultado original para la obtención de los usuarios y contraseñas del back-end que se muestran en la página de resultados (H1RD SECURITY, 2017)
SQL Injection ciego	Es una opción cuando no se puede inyectar código por error o por unión. Este se puede realizar de dos maneras, una basada en contenido donde se muestra si existe el resultado correcto y la otra basada en tiempo donde se tiene un delay de 5 segundos para mostrar los resultados. (Ping, 2017)	Se busca generar consultas SQL en la aplicación o sitio web en su front-end buscando obtener únicamente respuestas desde el back-end que muestren resultados false o true. (Ping, 2017)
Phishing	Esta estrategia busca engañar a usuarios incautos para obtener información privilegiada como contraseñas o información bancaria de tarjetas de crédito. (A.A. & K, 2020)	Se aplican técnicas de ingeniería social, donde el phisher suplanta personas o sitios web de empresas mediante alguna comunicación como un correo electrónico, mensaje de texto SMS/MMS o de mensajería instantánea, redes sociales, para engañar a un usuario buscando que este de clic en algún enlace o agregue información privilegiada en un sitio malicioso. (McRae & Vaughn, 2007)
IP Spoofing	El enmascaramiento de direcciones IP busca suplantar la identidad de una red o un host dentro de la misma donde se busca crear paquetes con direcciones de origen falsificadas para engañar al sistema mismo o a otras redes que permitan conexión, sin que se pueda identificar al origen (Lema, Simba, & Ally, 2018)	Se modifica la cabecera de los paquetes IP que son enviados hacia un sistema informático haciéndole creer que su origen es un dispositivo diferente que esta legítimamente autorizado y que ha sido suplantado. (Santhosh & Fancy, 2017)
DNS Spoofing	La falsificación de DNS busca direccionar de manera errónea a los equipos que hacen las consultas al DNS. (Hussain, Jin, Hussien, & Abduljabbar, 2016)	Se debe hacer que el servidor DNS legítimo acepte y utilice información incorrecta mediante una traducción de los nombres de dominio que redirecciona a los usuarios a direcciones IP de sitios web falsos permitiendo además interceptar mensajes de email. (Hussain, Jin, Hussien, & Abduljabbar, 2016)

TIPO DE INCIDENTE	DESCRIPCIÓN	IMPLEMENTACIÓN
Ransomware	Este tipo de malware bloquea el acceso por parte de usuarios legítimos a los documentos y archivos dentro de un sistema encriptándolos para solicitar una remuneración económica. (Almashhadani, Kaiiali, Sezer, & O'Kane, 2019)	Se busca infectar un computador o red a través de una memoria o dispositivo USB infectados, también mediante un archivo adjunto o enlace que se incluyen en mensajes de correo o sitios web maliciosos que mediante técnicas de phishing, o descargas troyanizadas que ocultan el script malicioso, una vez en el equipo el malware se autoejecuta y encripta los datos usando un algoritmo de cifrado que usa una clave que se auto genera y que se puede guardar o no en un servidor externo (Saxena & Soni, 2018)
Keylogger	Este tipo de malware se puede implementar a nivel de software o de hardware para registrar las pulsaciones que un usuario de un sistema informático realiza en el teclado, también puede capturar los clics de un mouse, para inclusive guardar capturas de pantalla o videos. (Sagiroglu & Canbek, 2009)	Se busca infectar un computador a través de una memoria o dispositivo USB infectados, también mediante un archivo adjunto o enlace que se incluyen en mensajes de correo o sitios web maliciosos, o descargas troyanizadas que ocultan el script malicioso, una vez en el equipo el malware se autoejecuta para capturar las pulsaciones del teclado, los clics de un mouse, capturas de pantalla o cortos de video con las actividades del usuario del equipo infectado para posteriormente enviarlos a un correo o servidor vía email o ftp. En el caso de los keyloggers de hardware se conecta un teclado o un conversor USB que contienen internamente un microcontrolador y una memoria para controlar todo el tráfico binario con las pulsaciones correspondientes a lo que el usuario digita. (Sagiroglu & Canbek, 2009)
Spyware	Este tipo de malware busca registrar información manteniéndose oculto para hacer un seguimiento a las actividades en línea oculto en computadores y dispositivos móviles. (Wazid, Katal, & Goudar, A framework for detection and prevention of novel keylogger spyware attacks, 2013)	Se busca infectar un computador a través de un archivo adjunto o enlace de descarga en sitios web maliciosos que ocultan el script malicioso, una vez en el equipo el malware se autoejecuta para supervisar y copiar las actividades en línea. (Mallikarajunan, Preethi, Selvalakshmi, & Nithish, 2019)
Adware	Este tipo de malware busca mostrar publicidad y recopilar datos comerciales redirigiendo las peticiones y búsquedas a sitios web de publicidad (como los tipos de sitios web que a menudo se visitan) para mostrar avisos personalizados. (Erturk, 2012)	Se busca infectar un computador a través de un archivo adjunto o enlace de descarga en algunos programas freeware o shareware, una vez en el equipo el malware se autoejecuta para llenar de publicidad las cargas en el navegador. (Ideses & Neuberger, 2014)
DDoS	La denegación de servicio distribuido busca realizar múltiples peticiones sobre un mismo servidor, haciéndolo colapsar hasta que se bloquea. (Saleh & Manaf, 2014)	Mediante el uso de botnets, que consisten en un grupo de equipos que ha sido previamente infectado con malvare tipo troyano o gusano genera múltiples peticiones hacia el mismo servidor hasta que quede fuera de línea sin que los usuarios se percaten de que sus máquinas están siendo usadas en un ataque. (Nagpal, Sharma, Chauhan, & Panesar, 2015)

Fuente: Apadtado por los autores.

9 FUNCIONALIDAD DE LA HERRAMIENTA SNORT

La herramienta Snort consiste en capturador de tráfico o sniffer de red, que permite hacer un comparativo mediante una serie de reglas configurables de los eventos que se registran en la misma contra los patrones que tiene guardados previamente en su configuración, generando un archivo con las coincidencias encontradas, lo que le permite detectar diversos tipos de intrusiones(Hernán & Medina, 2016). La estructura de esta herramienta se basa en un decodificador de paquetes el cual permite las capturas de tráfico, un preprocesador el cual analiza los paquetes que el decodificador entrega, un motor de detección el cual busca y compara los patrones de ataque según las firmas en la herramienta y un sistema de alarmas e informes que guarda e imprime en pantalla las alarmas generadas (Gaddam & Nandhini, 2017). En el esquema de la figura 15 se muestra la arquitectura general del IDS Snort.

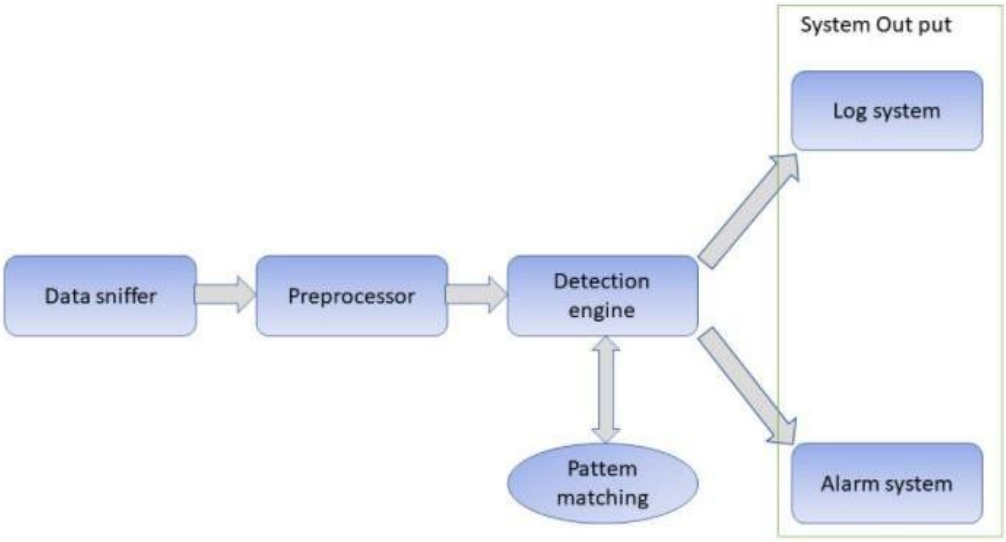

Figura 15 Arquitectura de Snort. Fuente. Adaptado de: (Gaddam & Nandhini, 2017)

9.1 DONDE INSTALAR EL IDS

Una de las características más representativas de los IDS es su ubicación, por lo que es sumamente importante que antes de definirla se verifiquen las opciones en donde se debe ubicar, (Para conocer más sobre el concepto y características de un IDS ver apartado 6.2.1). Por consiguiente, para definir la ubicación, es vital tener en cuenta el tipo de red considerando si el tipo de tráfico que se desea capturar es entrante o saliente. Dependiendo de ello se define si su ubicación del IDS como antes o después del firewall. Es importante recalcar que sin importar cual sea dicha ubicación se debe garantizar el acople y funcionamiento con respecto a los demás elementos de la red, buscando que haya una coexistencia que le permita capturar y compartir la información de routers, switches, firewalls y demás elementos de red. A continuación, en los siguientes apartados se describen las posibles ubicaciones para instalar Snort.

9.1.1 Delante del Firewall

Esta ubicación que se muestra en la figura siguiente, permite analizar todo el tráfico que entra y sale de la red mostrando una gran cantidad de información almacenada en el log, sin embargo, también se generan muchos falsos positivos por ataques. (Jayner, 2018).

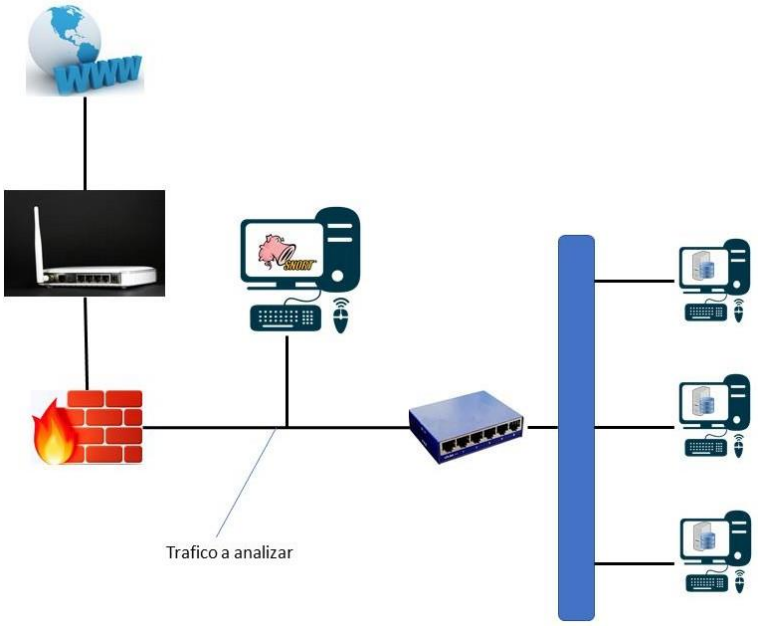

Figura 16 IDS delante del Firewall.Fuente: Adaptado de: (Jayner, 2018).

9.1.2 Detrás del Firewall

Esta ubicación que se muestra en la figura siguiente, ubica el IDS detrás del firewall para escanear y analizar directamente en su totalidad el tráfico entrante que cruza firewall y que este no ha filtrado sumando a snort como un filtro adicional y haciendo que se obtengan menos falsos positivos que en la configuración de apartado anterior. (Jayner, 2018)

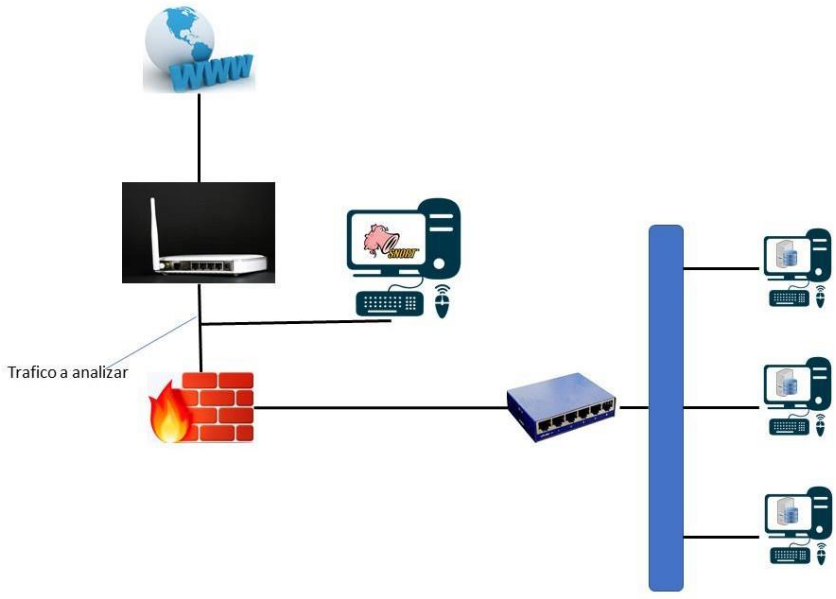

Figura 17 IDS detrás del Firewall. Fuente: Adaptado de: (Jayner, 2018).

9.1.3 Combinación delante y detrás del Firewall

Esta ubicación que se muestra en la figura siguiente, en ella se ubica el IDS en ambas ubicaciones requiriendo dos equipos anfitriones para conseguir un control de los ataques más efectivo, ya que de esta manera se captura todo lo trata de ingresar y que cruza el firewall, logrando hacer detecciones de paquetes sin que ingresen al firewall y también de paquetes cuando el firewall los deja pasar. (Jayner, 2018).

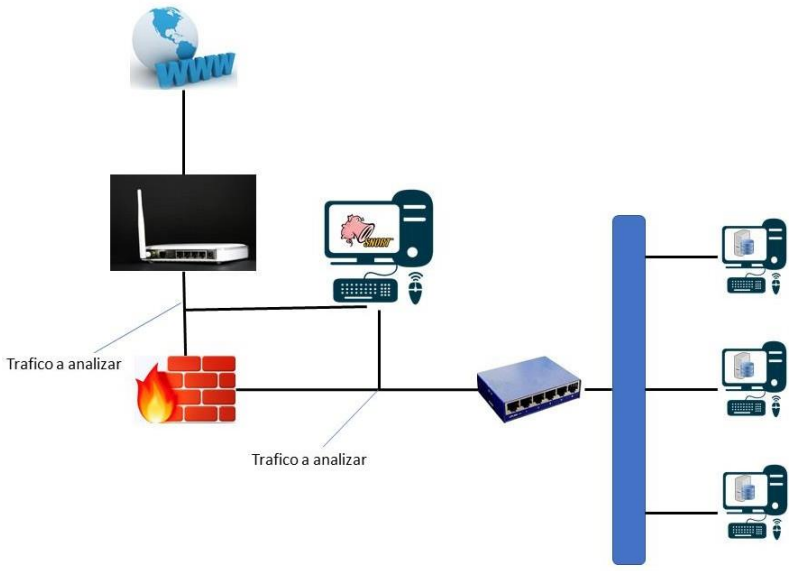

Figura 18 Combinación de los dos casos. Fuente: Adaptado de: (Jayner, 2018).

9.1.4 Firewall/NIDS

Esta ubicación que se muestra en la figura siguiente, donde se busca que un mismo equipo cumpla con las funciones de firewall y de IDS. (Jayner, 2018)

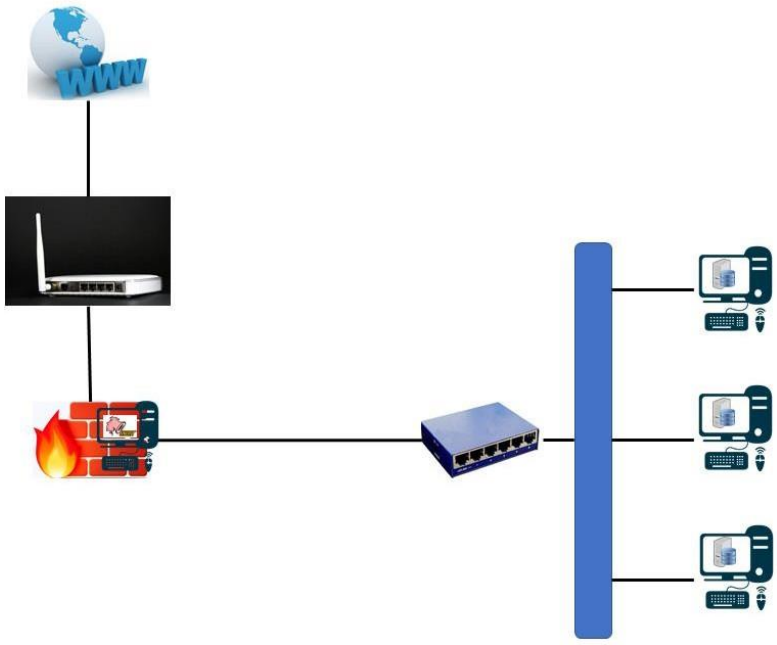

Figura 19 Firewall/NIDS. Fuente: Adaptado de: (Jayner, 2018).

9.2 INSTALACIÓN Y CONFIGURACIÓN DE SNORT

Una de las características más interesantes de Snort es que es multiplataforma, lo que le permite ser utilizado en diferentes entornos sin importar si el sistema operativo es Linux, Windows, o MacOS, entre otros.

9.2.1 Proceso de Instalación de Snort

Dentro del proceso de reconocimiento de la funcionalidad de la herramienta Snort se definió que era importante para lograr su adherencia por parte de los encargados de administrar la red y los oficiales de seguridad en Pymes reconocer el uso de Snort desde el proceso mismo de instalación. Esto motivo al diseño de procedimientos básicos de instalación de la herramienta en los dos sistemas operativos más representativos: Windows que es el mayormente usado en las pymes y Kali Linux que es un sistema operativo que se fundamenta en la distribución debían, ampliamente usado por los analistas y auditores de seguridad informática.

La instalación de Snort requiere de un equipo anfitrión ya sea físico o virtualizado que cuente con un sistema operativo que lo soporte y un mínimo de 2gb de memora RAM. La descarga del archivo de instalación se hace directamente de la página oficial www.snort.org, donde se selecciona la versión: Windows, o Linux, según su distro Debian, CentOS, o Fedora. Una vez finalizada la instalación Snort permite descargar paquetes de reglas definidas por la comunidad mediante un registro. Para conocer el paso a paso del proceso de instalación de Snort en los sistemas operativos Windows y Kali Linux (Ver Anexo: Procedimientos), donde se presentan los pasos de virtualización de las maquinas Windows y Kali Linux dándole a los encargados en las pymes una base desde cero de los procedimientos y conocimientos requeridos para la puesta a punto de Snort.

9.3 DEFINICIÓN GENERACION DE REGLAS

Una de las características más interesantes de la herramienta Snort es el esquema de definición de reglas y patrones de firmas con respaldo de la comunidad brindándole a las pymes una excelente opción, si no tienen los recursos para adquirir la versión paga. Esta estructura de reglas permite usar el motor de detección de Snort mediante la creación de sentencias propias o ajustadas según las necesidades por categorías de reglas completas que se configuran y gestionan al agregarlas o eliminarlas en el /etc./snort/snort.conf. a continuación, en los siguientes apartados se muestran los parámetros requeridos en la definición de reglas, así como algunos ejemplos de las reglas más comunes de la comunidad y ejemplos de su construcción.

9.3.1 Parámetros de Snort

La definición de los parámetros o modificadores que se requieren en la definición de reglas en Snort se describen en la siguiente tabla.

Tabla 15
Parámetros Snort

Parámetros	Descripción
-v	Mostrar la totalidad de paquetes por consola con las cabeceras TCP/IP
-d	Mostrar datos de aplicación.
-e	Mostrar las cabeceras de enlace (nivel 2).
-q	Modo silencioso. No muestra ni la información previa ni las estadísticas.
-l log	Especificar el directorio donde guardar los paquetes capturados (por defecto /var/log/snort).
-b	Guardar los paquetes en modo binario.
-r packets.log	Analizar los paquetes previamente guardados en el fichero de log especificado.
-c snort.conf	Archivo de configuración de alertas: /etc/snort/snort.conf
-A **-fast** **- full** **- unsock** **- none** **- console** **- cmg**	Modo de presentación de las alertas - Timestamp + mensaje + IP/Port origen y destino - Modo por defecto. A "fast" le añade la cabecera. - Lo envía a un socket - Desactiva las alertas - Modo "fast" enviado a consola Lo mismo que full y el contenido del paquete.
-i eth0	Selección de interfaz de donde capturar

Fuente: (Suarez, 2018)

9.3.2 Estructura de una regla

Pese a que las reglas integradas en Snort y definidas de manera estándar permiten detectar y securizar de manera eficaz ataques conocidos, la variación de los escenarios y vectores de ataque suele requerir de la redefinición de estas o de la creación de reglas específicas para brindar un mejor rendimiento a Snort minimizando además la tasa de falsos positivos. A continuación, se presenta la estructura general de una regla en Snort y el uso de los modificadores definidos en el apartado anterior.

De acuerdo con su estructura una regla se divide en dos secciones: un encabezado y la sección de opciones. El encabezado contiene la operación de la regla, el protocolo IP, la máscara de red, el puerto de origen y el puerto de destino del paquete o de operación. Mientras que en las opciones se generan mensajes para la toma de decisiones, mediante 4 opciones distintas.

- **Metadata**. Muestra información adicional sobre las reglas, que no son usados en la fase de descubrimiento.
- **Payload**. Busca firmas el payload del paquete.
- **Non-Payload**. Busca patrones en campos que no hacen parte de la carga útil del paquete como puede ser la cabecera.
- **Post-detection**. Habilita las reglas específicas que se deben ejecutar después de una

regla previa.

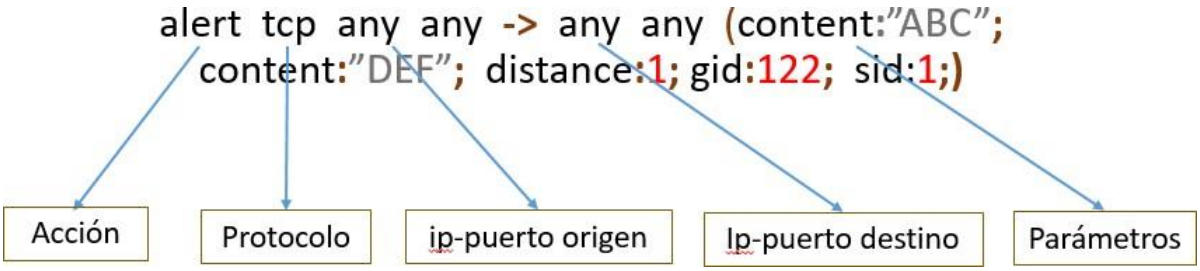

Figura 20 Estructura de una regla. Fuente: adaptado por los autores

9.3.3 Atributos de una regla

Tabla 16
Atributos de reglas

Parámetro:	Descripción:
msg:<message text>	Mensaje que se muestra de la alerta
gid:<generator id>	Identificador de un grupo de reglas relacionadas
sid:<snort rules>	Identificador único de la regla (gid+sid) – Los valores hasta 1,000,000 están reservados. – Para reglas de carácter general, no es necesario el gid (se pone por defecto el 1)
rev:<rev id>	Identificador de revisión (cambio) de la regla – Cada actualización o modificación de regla es una revisión. – Este parámetro no tiene sentido sin un sid previo a él.

Fuente: (Suarez, 2018)

9.3.4 Ejemplos de reglas estándar

A continuación, se presentan algunas reglas definidas de manera estándar que permiten detectar ataques conocidos.

9.3.4.1 Reglas que identifican Malware-Backdoor

Tabla 17
Reglas Malware-Backdoor

Reglas	Descripción
# alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"MALWARE-BACKDOOR Unix.Backdoor.Cdorked backdoor command attempt"; flow:to_server,established; content:"SECID="; fast_pattern:only;	Permite generar la detección de una actividad relacionada con malware con Impacto: grave. Posible existencia de malware en el host de destino. Detalles: esta actividad es indicativa de actividad de malware en un host. En este caso,

Reglas	Descripción
content:"SECID="; depth:6; http_cookie; content:"POST"; http_method; pcre:"/^Cookie\x3a\s?SECID=[^\x3b]+?$/mD"; pcre:"/\?[a-f0-9]{4}$/miU"; metadata:impact_flag red, policy max-detect-ips drop, service http; reference:url,blog.sucuri.net/2013/04/apache-binary-backdoors-on-cpanel-based-servers.html; reference:url,virustotal.com/en/file/7b3cd8c1bd0249df458084f28d91648ad14e1baf455fdd53b174481d540070c6/analysis/; classtype:trojan-activity; sid:26529; rev:5;)	se detectó el intento de comando de puerta trasera MALWARE-BACKDOOR Unix.Backdoor.Cdorked. Facilidad de ataque: simple. Esto puede ser un indicio de una infestación de malware.
# alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-BACKDOOR Backdoor.Win32.Neshgai.A runtime detection"; flow:to_server,established; content:".asp?"; nocase; http_uri; content:"SystemInfo-"; fast_pattern:only; http_uri; content:"hostid="; nocase; http_uri; content:"hostname="; nocase; http_uri; content:"hostip="; nocase; http_uri; content:"filename="; nocase; http_uri; content:"filetext="; nocase; http_uri; metadata:impact_flag red, policy max-detect-ips drop, policy security-ips drop, service http; reference:url,www.virustotal.com/file/fdbae1ccf6aa82e601584e09b4098dc3874d40d858654e9903628d55c98b07b9/analysis; classtype:trojan-activity; sid:26823; rev:3;)	Permite generar la detección de una actividad relacionada con malware. Impacto: grave. Posible existencia de malware en el host de destino. Detalles: esta actividad es indicativa de actividad de malware en un host. En este caso, se detectó la detección en tiempo de ejecución de MALWARE-BACKDOOR Backdoor.Win32.Neshgai.A. Facilidad de ataque: simple. Esto puede ser un indicio de una infestación de malware.

Reglas	Descripción
# alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-BACKDOOR Trojan.Midwgif.A runtime detection"; flow:to_server,established; content:"loginmid="; fast_pattern; nocase; http_client_body; content:"&nickid="; distance:0; nocase; http_client_body; pcre:"/loginmid=[0-9a-f]{24}&nickid=[^&]+&s=/iP"; metadata:impact_flag red, policy max-detect-ips drop, policy security-ips drop, service http; reference:url,www.virustotal.com/file/2c7b0b235c04f9f9392418ebced21b7efeb19550f5e29aee5a13d9f884a31da9/analysis/; classtype:trojan-activity; sid:26773; rev:2;)	Permite generar la detección de una actividad relacionada con malware. Impacto: grave. Posible existencia de malware en el host de destino. Detalles: esta actividad es indicativa de actividad de malware en un host. En este caso, se detectó la detección en tiempo de ejecución de MALWARE-BACKDOOR Trojan.Midwgif.A. Facilidad de ataque: simple. Esto puede ser un indicio de una infestación de malware.

Fuente: Comunidad Snort (SNORT, 2020)

9.3.4.2 Reglas que identifican Protocolo DNS

Tabla 18

Reglas protocolo DNS

Reglas	Descripción
# alert udp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"PROTOCOL-DNS DNS root query traffic amplification attempt"; flow:to_server,no_stream; content:"|00 01|"; depth:2; offset:4; content:"|00 00 02 00 01|"; within:5; distance:6; detection_filter:track by_src, count 5, seconds 30; metadata:policy max-detect- ips drop, service dns; reference:url,isc.sans.org/diary.html?storyid=5713; classtype:misc-activity; sid:15259; rev:7;)	Este evento se genera cuando se detecta una consulta de raíz de DNS en la red. Impacto: detalles de la denegación de servicio (DoS): este tráfico indica que puede haber un ataque DDoS en curso. Un ataque de amplificación de DNS que simplemente consulta a los servidores de nombres para el "." El dominio hará que se genere este evento. El dominio consultado es el dominio del servidor raíz, por lo que la respuesta será grande. Este tráfico de respuesta está dirigido a un punto final que no es la fuente real de la consulta, la intención es causar una DoS en la fuente falsificada. Facilidad de ataque: simple.

Reglas	Descripción
# alert tcp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"PROTOCOL-DNS dns zone transfer vía TCP detected"; flow:to_server,established; content:"|00 01 00 00 00 00 00 00|"; depth:8; offset:6; byte_test:1,!&,0xF8,4; content:"|00 00 FC 00 01|"; fast_pattern; isdataat:!1,relative; metadata:policy max-detect-ips drop, ruleset community, service dns; reference:cve,1999-0532; reference:nessus,10595; classtype:attempted - recon; sid:255; rev:24;)	Se ha solicitado una transferencia de zona de registros en el servidor DNS. Una transferencia de zona exitosa puede brindar un reconocimiento valioso sobre los nombres de host y las direcciones IP del dominio. Impacto: fuga de información, reconocimiento. Un usuario malintencionado puede obtener información valiosa sobre la red. Detalles: las transferencias de zona se utilizan normalmente para replicar información de zona entre servidores DNS maestro y esclavo. Si las transferencias de zona no se han restringido solo a servidores esclavos autorizados, los usuarios malintencionados pueden intentar realizar un reconocimiento de la red. El contenido | 00 00 FC | busca el final de una consulta de DNS y un tipo de DNS de 252 que significa una transferencia de zona DNS. Facilidad de ataque: fácil de realizar utilizando herramientas como nslookup, dig y host.
# alert udp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"PROTOCOL-DNS dns zone transfer vía UDP detected"; flow:to_server; content:"|00 01 00 00 00 00 00 00|"; depth:8; offset:4; byte_test:1,!&,0xF8,2; content:"|00 00 FC 00 01|"; fast_pattern; isdataat:!1,relative; metadata:policy max-detect-ips drop, ruleset community, service dns; reference:cve,1999-0532; reference:nessus,10595; classtype:attempted- recon; sid:1948; rev:20;)	Se ha solicitado una transferencia de zona de registros en el servidor DNS. Una transferencia de zona exitosa puede brindar un reconocimiento valioso sobre los nombres de host y las direcciones IP del dominio. Impacto: fuga de información, reconocimiento. Un usuario malintencionado puede obtener información valiosa sobre la red. Detalles: las transferencias de zona se utilizan normalmente para replicar información de zona entre servidores DNS maestro y esclavo. Si las transferencias de zona no se han restringido solo a servidores esclavos autorizados, los usuarios malintencionados pueden intentar realizar un reconocimiento de la red. El contenido | 00 00 FC | busca el final de una consulta de DNS y un tipo de DNS de 252 que significa una transferencia de zona DNS. Facilidad de ataque: fácil de realizar utilizando herramientas como nslookup, dig y host.

Fuente: Comunidad Snort (SNORT, 2020)

9.3.4.3 Reglas que identifican Protocolo ICMP

Tabla 19

Reglas protocolo ICMP

Reglas	Descripción
# alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"PROTOCOL-ICMP invalid ICMPv6 header attempt"; dsize:32; content:"|3A 01 66 0D 66 0D 66 0D 66 0D 00 00 00 00 00 00|"; depth:16; content:"|80 00|"; within:2; content:"|DE AD BE EF|"; within:4; distance:2; metadata:policy max-detect-ips drop; reference:url,thc.org/thc-ipv6/; classtype:misc-activity; sid:24305; rev:3;)	PROTOCOL-ICMP - Snort alerta sobre el tráfico del Protocolo de mensajes de control de Internet (ICMP), que permite a los hosts enviar mensajes de error sobre interrupciones en el tráfico. Los administradores pueden usar ICMP para realizar diagnósticos y resolución de problemas, pero los atacantes también pueden usar el protocolo para obtener información en una red. Este protocolo es vulnerable a varios ataques y muchos administradores lo bloquean por completo o bloquean mensajes selectivos.
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"PROTOCOL-ICMP webtrends scanner"; icode:0; itype:8; content:"|00 00 00 00|EEEEEEEEEEEE"; fast_pattern:only; metadata:ruleset community; classtype:attempted-recon; sid:476; rev:10;)	Este evento se genera cuando Webtrends Security Scanner genera un mensaje de solicitud de eco ICMP. Impacto: las solicitudes de eco ICMP se utilizan para determinar si un host se está ejecutando en una dirección IP específica. Un atacante remoto puede escanear una amplia gama de hosts utilizando solicitudes de eco ICMP para determinar qué hosts están operativos en la red. Detalles: Webtrends Security Scanner genera un mensaje de solicitud de eco ICMP que contiene la siguiente firma hexadecimal: | 00000000454545454545454545454545 | Al buscar esta cadena en un paquete, es posible determinar el tipo de host que generó la solicitud. Facilidad de ataque: simple. El comando "ping" esta presente en casi todos los sistemas operativos y puede generar este tipo de mensajes ICMP.
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"PROTOCOL-ICMP Router Selection"; icode:0; itype:10; metadata:ruleset community; classtype:misc-activity; sid:443; rev:9;)	Este evento se genera cuando se encuentra un mensaje de selección de enrutador ICMP en la red. Impacto: Detalles: Las solicitudes de máscara de dirección ICMP se definen en RFC 950 como el tercer método que los hosts pueden admitir para determinar la máscara de dirección correspondiente a su dirección IP. En la mayoría de las implementaciones, este método no es compatible y no debería ser tráfico normal en la mayoría de las redes. Facilidad de ataque: numerosas herramientas y scripts pueden generar solicitudes de máscara de dirección ICMP.

Fuente: Comunidad Snort (SNORT, 2020)

9.3.4.4 Ejemplos de reglas propuestas por los autores

Partiendo de la estructura expuesta en los apartados anteriores y con base en la literatura se proponen las reglas descritas en la siguiente tabla.

Tabla 20
Reglas creadas por autores

Reglas	Descripción
# alert tcp any any -> 192.168.1.21 80 (content:"GET pass.html"; msg:" Ataque HTTP Detectado";)	Esta regla lanza una alerta con un mensaje: Ataque HTTP Detectado, cuando detecta el patrón GET pass.html dentro de la parte de datos en los paquetes dirigidos através del puerto 80 a un servidor http.
# alert tcp any any -> 192.168.1.21 80 (content:"pass.html";offset: 4;Depth: 257; msg:" Intento de acceso a pass.html Detectado";)	Esta regla lanza una alerta con un mensaje: Intento de acceso a pass.html Detectado, cuando busca la cadena pass.html entre los caracteres 5 y 261 de la parte de datos de todos los paquetes HTTP enviados al servidor web por el puerto 80.
# alert tcp $HOME_NET any -> $EXTERNAL_NET [21,110] (content:"PASS"; msg:" Uso de contraseñas en texto claro detectado";)	Esta regla lanza una alerta con un mensaje: Uso de contraseñas en texto claro detectado, cuando detecta el envío desde la red local de contraseñas en texto plano (PASS) para la conexión de servicios o consulta de correo a través de los protocolos FTP y POP3.
# alert tcp $HOME_NET any -> $EXTERNAL_NET [21,110] (content:"PASS"; noncase; pcre:"/^PASS\s[^\n]*?%[^\n]*?%/smi"; msg:"Detectado el uso de contraseñas en claro";)	Esta regla es una alternativa a la regla anteriormente descrita y lanza una alerta con un mensaje: Uso de contraseñas en texto claro detectado, cuando detecta el envío desde la red local de contraseñas en texto plano (PASS) para la conexión de servicios o consulta de correo a través de los protocolos FTP y POP3, usando expresiones regulares. Para la construcción de la contraseña detectada.

Fuente: Autores, literatura Snort

10 ESCENARIO DE PRUEBAS EN ENTORNO VIRTUALIZADO

Tomando como punto de partida la información brindada por el contexto de seguridad generado en el apartado 8, y con base en la búsqueda sistemática de información y la evidencia identificada, se diseñó un escenario de prueba prototipo, el cual está conformado por tres equipos: dos de los cuales están conectados a la misma red LAN, uno de los cuales funciona como cliente, otro que trabaja como IDS, y uno que es externo y hace el papel de atacante. (Ver figura 21).

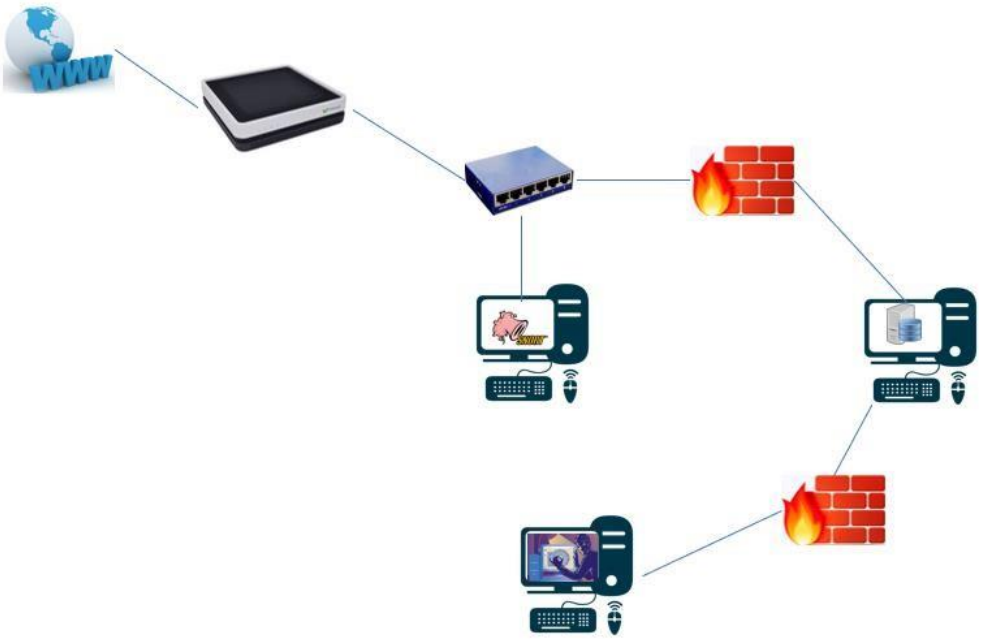

Figura 21 Escenario de pruebas. Fuente: Los autores

10.1 DISEÑO DE ENTORNO WEB

Buscando emular un entorno web real de una Pyme promedio se utilizaron maquinas virtualizadas en la plataforma VirtualBox, donde la máquina que se presenta como servidor web fue implementada usando el sistema operativo Ubuntu 1804. En dicha maquina se instalaron los servicios web de apache con php, el servicio de bases de datos con el motor de MySQL, y servicio ftp. (Ver Anexo: Procedimientos)

10.2 DESCRIPCION DE LAS PRUEBAS, SUS VECTORES DE ATAQUE Y CONTRAMEDIDAS

A continuación, en los subsiguientes aparatados se describen algunos de los ataques más comunes, haciendo una descripción de sus características, vectores de ataque, resultados y contramedidas. (Ver Anexo: Procedimientos).

10.2.1 ATAQUE DE SQL INJECTION

10.2.1.1 Vector de ataque

En un ataque de inyección de código SQL, se explota un sistema vulnerable para realizar consultas SQL sobre una base de datos en el back-end de una aplicación web. El primer paso es realizar una petición con un nombre de usuario y su contraseña en un campo de login, usando operadores lógicos como "0 OR 1=1", o enviando sus propias peticiones mediante sentencias de SQL para que de esta forma, se logre un acceso a las propiedades de gestión de la base de datos para crear, leer, actualizar, modificar o incluso eliminar los datos de misma (Academy, 2020). Durante un ataque de inyección de código SQL cualquier fuente de datos internas o externas pueden ser un posible vector de inyección, lo que representa diferentes tipos de este ataque. (Minero Guardado, 2011)

10.2.1.2 Vector de Ataque Sql Injection, basada en errores

Este ataque se realiza para obtener información de la estructura de la base de datos mediante comillas simples (') y/o de comillas dobles ("), donde específicamente se busca obtener los nombres de las tablas, los tipos de datos y la mayor cantidad de información de la aplicación web.

10.2.1.3 Vector de Ataque Sql Injection, basada en booleanos

Este ataque busca sobrescribir de manera lógica las condiciones de una consulta SQL en esquemas de autenticación mediante operadores AND/OR, buscando que la base de datos asuma los permisos y credenciales de usuarios administrativos correctos durante la consulta para obtener resultados TRUE o FALSE.

10.2.1.4 Vector de Ataque Sql Injection, basada en formularios

Este ataque se basa en errores posteriores, donde se ejecutan sentencias SQL en un formulario de login en una aplicación web directamente sobre los campos de texto de usuario y contraseña para robar sesiones en el servidor.

10.2.1.5 Vector de Ataque Sql Injection, basada en Order by

Este ataque busca identificar la cantidad de columnas de la base de datos mediante el uso de la cláusula order by con la cual se pretende organizar los resultados de estas columnas ordenándolas de manera ascendente o descendente.

10.2.1.6 Vector de Ataque Sql Injection, basada en unión

En este ataque se utiliza el operador UNION SQL en declaraciones SELECT para extraer de la base la información deseada, llegando a obtener datos de las tablas que tengan un mismo número de columnas o tipo de datos.

10.2.1.7 Resultados

- Se pudo evidenciar que hay páginas vulnerables a los ataques de SQL Injection, que puede comprometer información de la base de datos asociada a una aplicación web en una pyme.
- Se observo que la herramienta Snort permite detectar y dar aviso a sobre este ataque

en curso para realizar las acciones pertinentes antes de que la consecuencia del ataque sea grave.

- Se pudo ver que los diferentes tipos de inyección Sql se pueden hacer de varias formas tanto codificada o sin codificar y que con la ayuda de la herramienta y agregando las reglas pertinentes se puede hacer la detección de estos ataques a la aplicación con estas vulnerabilidades.

10.2.1.8 Contramedidas

- Instalar y configurar la herramienta Snort para detectar este ataque y mejorando los esquemas de protección y la seguridad de la red, aplicación y equipos de la organización. A continuación, se presentan dos tipos de reglas definidas para detectar este tipo de ataques.

  #alert tcp 192.168.1.1/24 any -> any 80 (msg:"Error basado en SQL Injection ' ' detectado"; content:"%27"; sid:10000003;)

Figura 22 Alerta generada al inyectar código Sql con comillas simples. Fuente Autores

#alert tcp 192.168.1.1/24 any -> any 80 (msg:"Error basado en SQL Injection " " detectado"; content:"%22"; sid:10000004;)

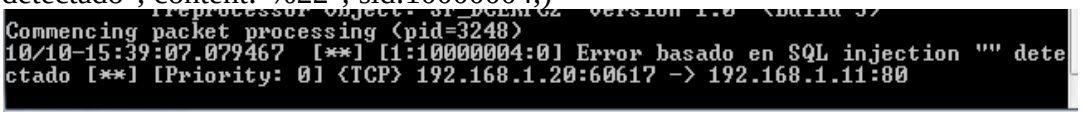

Figura 23 Alerta generada al inyectar código Sql con comillas simples. Fuente Autores

- No permitir campos de login o de texto en las aplicaciones web con caracteres especiales que se usan en las consultas SQL como las comillas simples (‘), comillas dobles (“), como buena práctica al momento de desarrollar dichas aplicaciones, ya que también son utilizadas en ataques de inyección. Igualmente, se debe evitar consultas corrompibles añadiendo un contra slash o barra invertida (\) al final de la cadena en dichas consultas de SQL. El uso de la función **mysql_real_scape_string ()** por ejemplo en PHP permite bloquear este tipo de caracteres (HOSTALIA, 2013), el uso de las funciones **escape ()** y **unescape** en JavaScript también ayudar a evitar este tipo de consultas. (Codigo, 2009)
- Una buena práctica en la gestión de bases de datos es delimitar cualquier tipo de consulta usando comillas simples para hacer más difícil la inyección de consultas. Por ejemplo, no se debe usar la consulta: SELECT Name FROM users WHERE id_user = $id, siendo más recomendable usar la consulta: SELECT name FROM users WHERE id_user = ‘$id’. (HOSTALIA, 2013)
- Verificar los tipos de datos que se permiten en la consulta es otra buena práctica por ejemplo si se está esperando un entero, no confiarse en que sea así, para esto es

recomendable tomar medidas como en el caso de PHP, el cual ofrece funciones como pueden ctype_digit() para validar si se trata de un número, también la función ctype_alpha () permite validar cuando es un string o cadena de texto.

- El uso de captchas en los esquemas de autenticación hace posible la validación de cualquier tipo de peticiones de usuario, detectando si se trata de una persona o de un boot para peticiones maliciosas.

10.2.2 FTP

10.2.2.1 Vector de ataque

El servicio FTP se usa ampliamente en las transferencias de archivos por ejemplo los archivos alojados en un servidor web en un hosting, donde los clientes suben y bajan archivos a los sitios o aplicaciones web, o donde los administradores realizan de copias de respaldo o backup (Avila, 2018). Esta funcionalidad hace que este servicio siempre se encuentre de cara a Internet haciendo que se busque explotar las vulnerabilidades en el protocolo para acceder de manera no autorizada al servidor donde está instalado, para obtener acceso al servidor junto a los demás dispositivos la red a la cual pertenecen, y/o privilegios de root mediante un ataque a las contraseñas por fuerza bruta o diccionario, aprovechando que los administradores dejan la configuración anónima, o usan el usuario root con contraseñas débiles o por default (Bin, 2015)

10.2.2.2 Vector de Ataque FTP Anonymous

La configuración del servicio FTP anónimo suele ser una configuración rápida para transferencia de archivos, sin embargo, es altamente vulnerable. En este ataque se busca obtener acceso mediante el identificador "anónimo", que generalmente no requiere de contraseña, o usa la contraseña por default "Invitado", obteniendo acceso rápido a la información registrada en el servidor y dando la opción de agregar software malicioso para escalar privilegios.

10.2.2.3 Resultados

- Se pudo observar que, el momento de configurar el servidor se establece que para el ingreso se deban usar credenciales de usuario para que en cada ingreso los usuarios tengan que identificarse, llevando a que se puedan revisar los logs del servidor para saber quién accede al servicio.
- Se pudo evidenciar que configurar el servidor de forma anónima, no permite validar el ingreso y los registros logs únicamente informaran las fechas y horas de ingreso.
- Se pudo comprobar que configurar la herramienta Snort con las reglas adecuadas permite detectar los ingresos y enviar alarmas para avisar que se está accediendo al servidor de forma anónima.

10.2.2.4 Contramedidas

- No se recomienda usar FTP anónimo, pero en caso de hacerlo de debe instalar y configurar Snort para detectar los accesos al servidor ftp en modo anónimo para

buscar controlar el acceso a la sesión. A continuación, se presentan una regla definida para enviar un mensaje de alarma cuando se dé un acceso de FTP anónimo.

#alert tcp 192.168.1.1/24 any -> any 21 (msg:"ACCESO FTP DESDE USUARIO ANONIMO"; content:"Anonymous"; classtype:suspicious-login; sid:99999901; rev:1;)

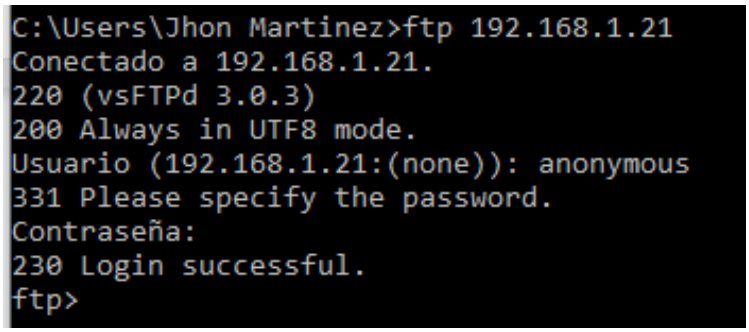

Figura 24 Ingreso al servidor ftp usuario Anonymous. Fuente Autores

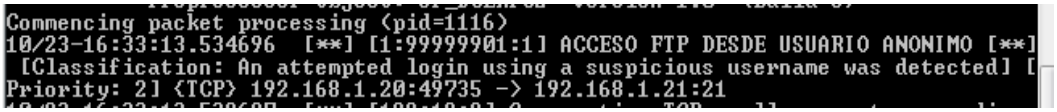

Figura 25 Alerta generada por snort al ingresar con usuario Anonymous. Fuente Autores

- Una buena práctica en la configuración de servicios es no usar el usuario root para el acceso, evitar dejar activo acceso a root, hace que, si se presenta un incidente, el atacante no tendrá directamente privilegios de super administrador, lo que le hará más difícil el ataque.
- En el caso de necesitar permitir que los usuarios puedan entrar sin usuario y contraseña una buena práctica es crear y habilitar una carpeta de solo lectura, para evitar que los clientes que se conecten al servicio puedan escribir, ejecutar o subir cualquier tipo de archivo.

10.2.3 IP SPOOFING

10.2.3.1 Vector de ataque

En este ataque se inyectan paquetes TCP o UDP donde la dirección IP de la cabecera de origen es falsa y suplanta una dirección autorizada o de confianza, evitando que el paquete sea filtrado y bloqueado por listas de alertas blancas o negras, o de sistemas basados en firmas IP (blockbit, 2019). Este ataque permite interceptar tráfico IP entre sistemas informáticos para su manipulación sin ser identificado, llevando a ataques de denegación de servicio DoS y DDoS. (IONOS, 2020).

10.2.4 DNS SPOOFING

10.2.4.1 Vector de ataque

En este ataque se hace una falsificación de las direcciones IP correspondientes a nombres de dominios legítimos para que la resolución de nombres se de en un plano diferente, llevando a que los equipos clientes sin darse cuenta ingresen a sitios falsos, cuando se hace una

petición a dominio real redireccionado al siente y estableciendo conexión con un servidor que cuenta con la IP falsa. (ciyi, 2019)

10.2.4.2 Resultados

- Se evidencia que los atacantes tienen el conocimiento y los medios para realizar este tipo ataques, mientras que los usuarios desconocen este tipo de ataques haciéndolos victimas fáciles.
- Se evidencia que los usuarios normales desconocen los riesgos que representan las tecnologías en la web, y a los que se exponen por no tener los conocimientos básicos para identificar entre un sitio seguro y uno clonado llevándolos a ingresar y comprometer información y datos importantes.

10.2.5 Cross-site scripting (XSS)

10.2.5.1 Vector de ataque

Este ataque permite inyectar código no confiable sobre los campos de entrada de texto, login, campos de búsqueda o formularios de registro u opinión, en sitios y aplicaciones web locales dinámicas, o comprometer el navegador, donde la vulnerabilidad XSS ejecutará el código sin una validación y codificación adecuada en el navegador del cliente para robar información, secuestrar sesiones de usuario, robar cookies y atacar la integridad del sistema (Carpio, 2018). El XSS ocurre cuando los datos ingresan a través de una solicitud web de una fuente no confiable o cuando se incluyen dentro del contenido dinámico no validado enviado al cliente web de forma maliciosa en formato JavaScript o con contenido HTML, Flash o en general cualquier código interpretable por el navegador. (KirstenS, 2020)

10.2.5.2 Vector de ataque Ataques XSS almacenados

Este XSS persistente o tipo I, es un ataque donde se inyectan scripts para almacenarlos de forma permanentemente en el servidor, base de datos, o campos de registro de visitantes y comentarios para que un cliente lo recupere del servidor al solicitar acceso al archivo almacenado mediante un enlace. (KirstenS, 2020)

10.2.5.3 Vector de ataque Ataques XSS reflejados

Este XSS no persistente o tipo II, es un ataque donde se inyecta una secuencia de comandos que será reflejada como un mensaje de error, o un resultado de búsqueda en el servidor web, en donde se incluye un apartado o la totalidad del script malicioso como parte de la solicitud. Este tipo de ataque se envía engañando al cliente por medio de mensajes de correo o en sitios web para dar clic en un enlace malicioso, se rellene un formulario o se reenvié para navegar en sitio malicioso, donde el código inyectado refleja el sitio vulnerable en el navegador que lo ejecuta pensando que es confiable. (KirstenS, 2020)

10.2.5.4 Resultados

- Se evidencia que inyectar scripts para un ataque xss puede ser sencillo para un atacante, pero muy peligroso para una organización ya que este puede llevar código malicioso.
- Se evidencia que, aunque se puede tener seguridad para evitar scripts externos, los

ataques xss también pueden ser lanzados con código HTML.

- Se evidencia que al tener varias formas de ataque estos pueden actuar sobre las bases de datos llevando a que cada vez que se ejecuta la aplicación se ejecute nuevamente este código malicioso.
- Se comprueba que con Snort se pudo configurar una regla que permitió por medio de expresiones regulares detectar ataques de este tipo.

10.2.5.5 Contramedidas

- Se recomienda instalar y configurar Snort para detectar las expresiones regulares que frecuentemente se utilizan para inyectar código malicioso XSS. A continuación, se presentan una regla definida para enviar un mensaje de alarma cuando se dé un XSS.

  alert tcp 192.168.1.1/24 any -> any 80 (msg: "POSIBLE ATAQUE XSS"; pcre: "/ script |body |onload /"; sid:10000012;)

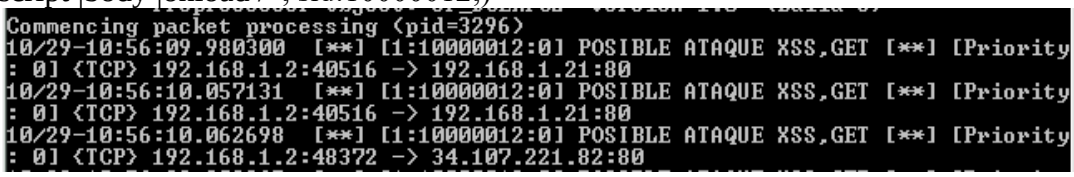

Figura 26 Alerta generada cuando snort detecta las expresiones regulares. Fuente Autores

- Instalar y configurar Snort para detectar el envió de paquetes por el método GET, para así poder prevenir un posible secuestro de cookies. A continuación, se presentan una regla definida para enviar un mensaje de alarma cuando se dé un XSS, GET.
  #alert tcp 192.168.1.1/24 any -> any 80 (msg: "POSIBLE ATAQUE XSS, GET";content:"GET"; http_method ;sid:10000013;)

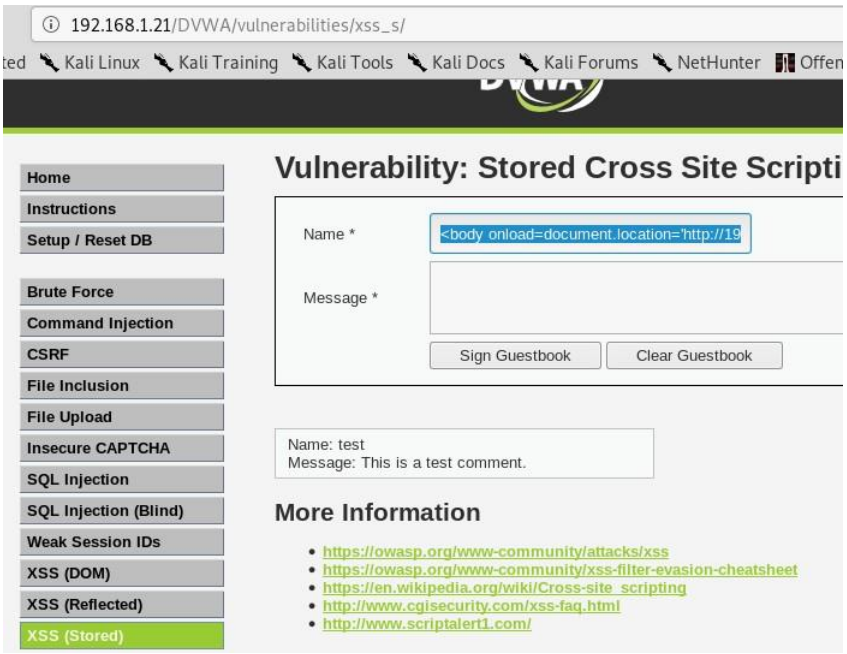

Figura 27 Inyección de código XSS para robo de cookies. Fuente Autores

Figura 28 Cookies robadas. Fuente Autores

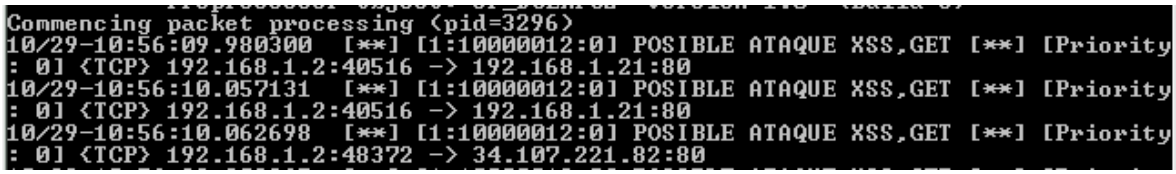

Figura 29 Alerta generada cuando snort detecta método GET. Fuente: Autores

- Una buena práctica es controlar a nivel de programación lo que se va a introducir en las cajas de texto de la aplicación web, para evitar que se ejecuten comandos que pueden ser maliciosos, es importante usar las funcionalidades de los lenguajes de programación que permiten filtrar la salida de contenido que se muestra en el navegador.

11 RECOMENDACIONES DE BUENAS PRÁCTICAS

Como estrategia para fortalecer el proceso que representa la seguridad de la información enfocado, no solo a la protección de la infraestructura de las pymes, sino también a la implementación de espacios de sensibilización y capacitación que a través de políticas, lineamientos y procedimientos de seguridad informática permitan fortalecer el ámbito tecnológico de las mismas, apoyando su gestión y procesos misionales, se plantean una serie de recomendaciones de buenas prácticas que se basan en los resultados obtenidos en este proyecto junto con las contramedidas generadas, buscando además que las pymes estén preparadas a los ataques de los ciberdelincuentes, y no logren explotar las vulnerabilidades para su accionar delictivo, protegiendo la información como su activo más valioso.

En el campo de la ciberseguridad es fundamental para las pymes realizar una adecuada gestión de su infraestructura tecnológica en la cual implementan sus procesos, tales como: servidores, dispositivos de red, aplicaciones web, bases de datos, y sistemas de gestión, los cuales están constantemente expuestos a ciberataques, mientras que los encargados de las pymes ni siquiera saben o conocen las vulnerabilidades o riesgos que les asechan. Esta nueva situación permite la generación de recomendaciones como guía para que los usuarios y administradores puedan tener una base para proteger su información, obteniendo una primera contextualización que les permita reconocer los conceptos de ciberseguridad más relevantes para la comprensión de un primer nivel que ira madurando en el tiempo.

A continuación, se plantea una serie de recomendaciones de seguridad que permitirán una gestión de la seguridad de la información más eficiente.

11.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Este lineamiento general que se establece con la finalidad de reglamentar la seguridad de la información y por consiguiente los sistemas informáticos e infraestructura tecnológica de una organización, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información. Una política puede estar compuesta de políticas puntuales, procedimientos y estándares. Para el caso de una pyme se recomienda como primer paso para la gestión de la seguridad de la información sus sistemas informáticos, e infraestructura tecnológica establecer la política de la seguridad de la información que le permita delimitar el marco normativo en el interior de la organización. Una vez se defina la política se establecen las políticas y procedimientos puntuales que la respaldan. A continuación, se definen las políticas y procedimientos puntuales. Las políticas que dan los lineamientos para que se cumplan a partir de los procedimientos que se deben ejecutar.

Procedimientos

- Administrar que usuarios tendrán acceso a los recursos de la información
- Definir políticas de copias de respaldo con el fin de tener una guía para una correcta recuperación de la información llegado el caso sufrir una pérdida de este activo.
- Precisar claramente la información que cada persona dentro de la organización puede manejar.

- Tener licenciado el software que maneje la organización, esto aplica a todas las empresas según la ley 603 del 2000 la cual obliga a la entidad a presentar un informe detallado de gestión, sobre la evolución de la empresa. En donde se hace énfasis en el tipo de software que usa la compañía para proteger la propiedad intelectual.
- Asegurar las comunicaciones para proteger la información en procesos de transmisión y recepción de datos en las redes.
- Realizar auditorías de los sistemas de información la cual permitirá ver cómo está la seguridad de los sistemas para realizar mejoras constantes.
- Proteger los equipos de cómputo donde se almacena, transmite y procesa la información.

11.1.1 POLÍTICAS DE PERFILES DE USUARIO

Se deben definir los lineamientos para gestionar los privilegios de usuario para cada una de las unidades administrativas, departamentos o dependencias de acuerdo con la estructura organizacional u organigrama y el manual de funciones teniendo claro cuáles son las actividades y la interacción de cada usuario con los sistemas informáticos en la organización para limitar el acceso, en caso de que la pyme no tenga dicha información, esta se debe construir teniendo en cuenta las funciones de los usuarios de cada sistema.

Procedimientos

- Asignar los roles correspondientes a cada persona de la organización teniendo en cuenta el cargo y la responsabilidad del mismo según sus funciones.
- Crear la cuenta de acceso a cada usuario ya sea empleado, cliente, proveedor u otros, definiendo el rol de cada uno y así asignar que acciones puede realizar dentro de los sistemas de la organización.
- La política debe definir claramente cuál es la responsabilidad de cada usuario donde se especifique que cada persona es responsable se las acciones que se realicen de su parte dentro de programas y aplicaciones accedidos con el usuario. Cada cuenta es personal e intransferible,
- La cuenta debe tener asignada una contraseña para su protección la cual deberá cumplir los parámetros de la construcción de una contraseña segura que se definan en la política de gestión de contraseñas.

11.1.2 POLÍTICA DE BACKUP

Se deben hacer copias de respaldo de los activos de información de la pyme buscando evitar pérdidas de los datos para cuando se haga una eliminación accidental, exista una corrupción de los datos, una falla del sistema, un desastre natural o un ataque informático por ejemplo un ransomware.

Procedimientos

- Cuando los recursos de almacenamiento sean limitados se debe clasificar la información de manera cuantitativa y cualitativa según su nivel de importancia para la empresa, esto hace que se pueda dar prioridad a la información sobre la cual se hace

la copia de seguridad (ej.: servidor completo, software, datos y estructura de datos, archivos de usuarios)

- Siempre controlar el acceso a la información resguardada en todo momento antes, durante y después de la generación del backup.
- Las copias de respaldo deben hacerse periódicamente, esta periodicidad se debe calcular de acuerdo con loa recursos y requerimientos de la pyme, seleccionando la frecuencia para la ejecución del proceso por ejemplo mediante un proceso automatizado.
- Dependiendo de los recursos con los que la pyme cuente se debe escoger la forma apropiada para resguardar la información, ya sea en la nube, en repositorios como USB, o discos duro para guardar en una caja fuerte, o en repositorios externos en servidores a una distancia apropiada de la sede principal.

11.1.3 POLÍTICA DE PANTALLA LIMPIA

Para la protección de cualquier dispositivo, buscando mantener el orden de la información para evitar pérdidas por repetición, o no ubicación. Dicho orden puede estar sujeta a tablas de retención documental sobre las cuales se tenga organizado el archivo de gestión en formato digital de la pyme. Igualmente, se deben implementar procedimientos de restricción de permisos para no dejar guardar en escritorio, bloqueo de pantalla, y cierre de sesión por inactividad o no uso.

Procedimientos

- Siempre que los usuarios se deban ausentar de su puesto de trabajo, o que se presente una inactividad superior a 3 minutos se deben bloquear las pantallas de sus equipos.
- Todos sistemas informáticos, y aplicaciones deben tener definido un tiempo máximo de inactividad para el cierre o bloqueo de sesión.
- Las pantallas de los computadores deben estar libres de archivos o enlaces directos a archivos, cada uno de estos se deben almacenar en carpetas.
- Los dispositivos de trabajo deben contar con un fondo de pantalla y protector de pantalla predefinido.
- Cuando la jornada laboral termine, todos los dispositivos deben ser apagados, esto se puede automatizar por medio de un directorio activo.

11.1.4 POLÍTICA DE CONTRASEÑAS SEGURAS

Se debe definir una política con los lineamientos de la gestión de contraseñas, denotando la importancia de la seguridad de estas mediante el establecimiento de requisitos mínimos de tamaño y composición, además de debe recalcar que una contraseña débil puede dar accesos no autorizados a la información y esto será responsabilidad directa de los usuarios.

Procedimientos:

- Los usuarios no deben usar la misma contraseña para dispositivos personales y para dispositivos de la empresa, igualmente se deben tener contraseñas diferentes para cada sistema dentro de la organización, y se debe en lo posible usar un directorio activo.

- Todas las contraseñas de nivel administrador incluidas las de root deben ser cambiadas cada dos meses y las contraseñas de usuarios limitados cada 3 meses.
- Las contraseñas de correos electrónicos y dispositivos deben ser cambiadas cada seis meses.
- El tamaño de las contraseñas debe ser de mínimo 10 dígitos donde se incluyan mayúsculas minúsculas, números y caracteres alfanuméricos, exceptuando los que son usados en consultas SQL.
- Se debe socializar a los usuarios la importancia de No revelar o compartir las contraseñas a ningún usuario o agente externo de la pyme y que No se deben guardar por default no anotar en libretas o teclados, haciendo énfasis en las repercusiones e inconvenientes que esto puede acarrear.

11.2 DIFUSIÓN DE LAS POLÍTICAS DE SEGURIDAD

Una vez creadas la política de seguridad y las políticas de implementación se debe generar una estrategia de difusión como parte importante del programa de gestión de la seguridad que se quiera implementar, esto ya que se requiere que todos los que integran la organización participen para producir un buen nivel de seguridad.

Procedimientos:

- Dar charlas informativas a todo el personal, incluyendo los jefes para que de esta manera ellos puedan exigir el cumplimiento a sus colaboradores.
- Se debe usar la página de la pyme y su correo electrónico para enviar información actualizada sobre las políticas y de esta forma garantizar que todo el personal este informado sobre el tema.
- Se deben publicar en carteleras, fondos de escritorio, pad mouse o protectores de pantalla, etc., como estrategia para mostrar las políticas de manera llamativa y concreta.

11.3 IMPLEMENTAR UN IDS

La implementación de la herramienta Snort permite auditar en tiempo real y de manera continua la red, ello además establecer reglas propias que vayan de la mano de las políticas establecidas, para validar su cumplimiento en cuanto a tener alarmas y logs de ingresos y acciones en páginas web detectar ataques de Inyección Sql, XSS y controlar el acceso a servicios como FTP o SSH entre otros.

11.4 CIFRADO DE DATOS Y CONTRASEÑAS

Se deben aplicar técnicas criptográficas que permitan un uso apropiado y eficaz de la información, para proteger la confidencialidad, la autenticidad y la integridad de la información.

Procedimiento

- Se debe hacer uso de controles criptográficos en todos los servicios y en especial aquellos con soporte web que están de cara a internet como: portales, interconexión con terceros, comunicación con proveedores o clientes, para evitar que se exponga la información intercambiada, manteniendo su confidencialidad.
- Se debe tener procedimientos para el uso, la protección y la vida útil de las claves criptográficas, evitando que se usen cuando estas expongan o caduquen.

11.5 PROTECCIÓN CON ANTIVIRUS

Toda pyme sin importar su tamaño debe definir los estándares y lineamientos básicos para el uso de software antivirus a todos los equipos de su infraestructura, el cual debe estar debidamente actualizado.

Procedimiento

- Se debe utilizar solo el antivirus adquirido y licenciado por el proveedor de servicios informáticos de la empresa, incluyendo computadores y dispositivos móviles.
- Los empleados no deben abrir archivos de correos electrónicos no confiables.
- Se deben eliminar los correos no deseados, cadenas y demás correos con estas características.
- Si el antivirus llega a detectar una amenaza se debe poner en cuarentena el computador aislándolo de la red y formatear inmediatamente.
- Se debe capacitar a los usuarios sobre el uso y manejo del software antivirus y los planes de contingencia.

11.6 IMPLEMENTAR SEGURIDAD POR CAPAS

Es importante que las pymes implemente seguridad por capas ya que esta garantiza en mayor manera la seguridad mediante herramientas ubicadas en diferentes niveles logrando detectar amenazas potenciales en caso de que estas ya hayan cruzado algún nivel de seguridad. A continuación, se definen las tres capas mínimas que debería implementar una pyme.

- **Primera capa:** Asegurar la ubicación de los usuarios y empleados restringiendo sus acciones sobre el sistema operativo y su configuración, así como el acceso a las aplicaciones. Para este caso una pyme se puede implementar un directorio activo mediante una máquina Linux para habilitando el servicio de samba el cual se puede administrar con una herramienta de administración remota como RSAT la cual ha sido liberada por Windows y permite la gestión de unidades organizativas y políticas GPO. El uso de la herramienta Winselect también hace posible configurar un equipo sin un directorio activo para pymes pequeñas limitando las funciones según un rol y evitando el uso no autorizado de información o aplicaciones.
- **Segunda capa:** Todo equipo del que disponga la pyme debe ser protegido con un software antivirus, para detectar y eliminar virus, gusanos y troyanos. Igualmente se debe usar un IDS el cual le protege ante ataques, anomalías e intrusiones y un firewall que bloquee el tráfico no deseado.

- **Tercera capa:** Se deben implementar estrategias que impidan ejecutar códigos maliciosos o programas no autorizados, que sean ilegales o no deseados.

11.7 REALIZAR AUDITORIAS PERIODICAS

Por ultimo una recomendación de buenas prácticas fundamental en el proceso de madurez de un sistema de gestión y la mejora continua consiste en realizar auditorías periódicas a nivel de personal interno y si es posible a nivel externo para identificar, describir y evidenciar el cumplimiento de las políticas de seguridad y las vulnerabilidades a las que están expuestas los sistemas, para tomar acciones correctivas y conocer el nivel de seguridad en el cual se está dentro del proceso de la seguridad de la información, para lo cual se pueden implementar estándares internacionales como ISO 27001, o COBIT.

12 CONCLUSIONES

- La búsqueda sistemática de información permitió evidenciar los diferentes ataques a los que están expuestas las pymes, tales como Sql Injection, IP spoofing, DNS spoofing, haciendo que en la actualidad para los ciberdelincuentes sea más rentable atacar pymes aprovechando que estas no cuentan con una infraestructura de seguridad robusta, manteniendo poca o ninguna seguridad y presentando vulnerabilidades conocidas como por ejemplo una mala configuración de servicio FTP.

- La nueva realidad de este milenio presenta un acceso vertiginoso de las pymes al ciberespacio y sus servicios, lo cual presenta múltiples sus ventaja, pero al mismo tiempo les expone a las amenazas, riesgos y vulnerabilidades que son inherentes a la tecnología, sin embargo, las pymes no se han preocupado por securizar sus entornos o infraestructuras digitales, esta nueva situación les hace presas fáciles de los ciberdelincuentes por lo que se requieren estrategias que permitan que las pymes reconozcan el contexto o ámbito de la ciberseguridad de sus tecnologías.

- Snort es una de las herramientas de monitoreo de redes para la detección y análisis de tráfico más apropiadas para pymes ya que permite que se puedan generar reglas adaptables, permitiendo además una integración con las estrategias firewall, para fortalecer los niveles de seguridad de las pymes teniendo en cuenta la seguridad por capas y seguridad perimetral.

- Es importante que las pymes cimenten la seguridad de la información como un proceso con niveles de madurez mediante la implementación de escenarios de prueba que le permitan además de asegurar los recursos, la infraestructura, la información sensible y el software, hacer que no se vean afectados los recursos reales en caso que las pruebas no resulten como se esperaba, además permite probar el funcionamiento de herramientas sin exponer el entorno real.

- Al realizar la prueba de Sql Injection en una web vulnerable se evidencio que si una organización en su plataforma no controla los datos que se ingresan en los campos de texto, pueden ser víctimas de un ataque de este tipo, que enviará parámetros en estos campos, y si no son analizados exponen información privilegiada de la organización.

- En la actualidad es fundamental que las pymes tomen conciencia sobre ciberseguridad sabiendo que uno de los puntos vulnerables son los usuarios, por esto se deben generar políticas y procedimientos de seguridad, así como recomendaciones de buenas prácticas para que mediante capacitaciones y sensibilizaciones orienten a su recurso humano y stakehoders hacia la protección de la confidencialidad, integridad y disponibilidad de la información que se procesa, trasmite y almacena en sus infraestructuras tecnológicas para el tratamiento de riesgos.

- A nivel de la academia buscar que los desarrolladores realicen aplicaciones seguras encaminadas a la protección de los entornos web y los datos, buscando al máximo que la seguridad no recaiga únicamente en los usuarios o administradores del sistema.

13 TRABAJO FUTURO

Dando continuación a este trabajo de grado se propone una serie de trabajos futuros que se pueden implementar para ofrecer un servicio más completo y útil para las pymes:

- Realizar pruebas y generar un estudio para la detección de intrusos usando otras herramientas como, por ejemplo: Kismet para entornos inalámbricos, OSSEC que es basado en host, ZScalar como IDS cloud, Cortex. o con Suricata uno de los más robustos.

- Implementar las pruebas y recomendaciones generadas en este proyecto, en un escenario real en diferentes pymes en Santander donde se revise el impacto desde la instalación y configuración para establecer un primer nivel de madurez y generar indicadores para reconocer el estado de la ciberseguridad en el Departamento.

- Para próximos proyectos implementar un escenario real mediante una honeypot para realizar ataques a una organización e implementar las recomendaciones de ciberseguridad y snort dadas en la guía presentada para validar su funcionamiento y obtener una retroalimentación para realizar mejoras en una segunda versión.

- Desarrollar una estrategia software de IDS que use inteligencia artificial, machine learning, o herramientas basadas en redes neuronales para supervisar y analizar el tráfico, buscando detectar incidentes que no son considerados por los sistemas de seguridad convencionales y así disminuir el porcentaje de falsos positivos.

14 Referencias

Arney, C., & Wang, X. (Septiembre de 2016). *Active Snort Rules and the Needs for Computing Resources: Computing Resources Needed to Activate Different Numbers of Snort Rules.* Obtenido de https://doi-org.aure.unab.edu.co/10.1145/2978178.2978189

Bagheri, S., & Shameli-Sendi, A. (27 de Abril de 2020). *Dynamic Firewall Decomposition and Composition in the Cloud.* Obtenido de IEEE Transactions on Information Forensics and Security: 10.1109/TIFS.2020.2990786

Boughrara, A., & Mammar, S. (21 de Marzo de 2013). *Implementation of a SNORT's output Plug-In in reaction to ARP Spoofing's attack.* Obtenido de IEEE: 10.1109/SETIT.2012.6481988

Gaddam, R., & M. Nandhini. (17 de Julio de 2017). *An analysis of various snort based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in Kali Linux environment.* Obtenido de IEEE: https://ieeexplore-ieee-org.aure.unab.edu.co/document/7975177

GARZON PADILLA, G. (2015). *PROPUESTA PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE DETECCION DE INTRUSOS (IDS) EN LA DIRECCION GENERAL SEDE CENTRAL DEL INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO INPEC "PIDSINPEC".* Obtenido de http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3494/3/86057

Perafán Ruiz, J., & Caicedo Cuchimba, M. (2014). *Análisis de Riesgos de la Seguridad de la Información para la Institución.* Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf?sequence=3&isAllowed=y

UIT-R, M.-1. (MARZO de 2012). *Vocabulario de términos de las telecominicaciones moviles internacionales (IMT).* Obtenido de https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.1224-1-201203-I!!PDF-S.pdf

31000, I. (2018). *Gestión del riesgo — Directrices.* Obtenido de https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf

Academy, A. (19 de Mayo de 2020). *Avast Academy - Inyección SQL.* Obtenido de https://www.avast.com/es-es/c-sql-injection#topic-1

Aghababaeian, H, Asgarkhani, AM, & Mirabbasi, SB. (2018). *Cybercrimes and government responsibility for cyber-attacks.* Obtenido de Ciberdelitos y responsabilidad gubernamental por ciberataques: https://cutt.ly/WfiHY2U

Alnabulsi, H., Islam, M. R., & Mamun, Q. (4 de noviembre de 2014). *Detecting SQL injection attacks using SNORT IDS.* Obtenido de 10.1109/APWCCSE.2014.7053873

Anonimo. (Noviembre de 2019). *ECURED*. Obtenido de https://www.ecured.cu/index.php?title=IDS&action=history

Antiun. (2020). *Antiun.com.* Obtenido de Firewall: https://antiun.com/firewall/

AO Kaspersky Lab. (2020). *Kaspersky daily*. Obtenido de EDR: https://www.kaspersky.es/blog/epp-edr-importance/16154/

Avila, F. (21 de Abril de 2018). *securityhacklabs*. Obtenido de Herramientas para ataque a servidores FTP: https://securityhacklabs.net/articulo/herramientas-para-ataque-a-servidores-ftp

bibing. (2020). *SNORT.* Obtenido de http://bibing.us.es/proyectos/abreproy/12077/fichero/memoria%252Fpor_capitulos%252F04.snort.pdf

Bin, C. (23 de septiembre de 2015). *Formalized Description and Analysis of FTP on Petri Net.* Obtenido de 10.1109 / IIH-MSP.2015.118

blockbit. (19 de Noviembre de 2019). *blockbit*. Obtenido de Conozca qué es IP Spoofing y proteja su red: https://www.blockbit.com/es/blog/conozca-que-es-ip-spoofing-y-proteja-su-red/

Bouziani, O., Benaboud, H., Chamkar, A. S., & Lazaar, S. (Marzo de 2019). *A Comparative study of Open Source IDSs according to their Ability to Detect Attacks.* Obtenido de https://dl-acm-org.aure.unab.edu.co/doi/abs/10.1145/3320326.3320383

BUITRON, V. A. (2015). *¿QUÉ TAL ESTA COLOMBIA EN CUESTIÓN DE CIBERSEGURIDAD?* Obtenido de https://repository.unimilitar.edu.co/bitstream/handle/10654/7794/Qu%E9?sequence=1

Carpio, M. (08 de Mayo de 2018). *IMF Business School*. Obtenido de https://blogs.imf-formacion.com/blog/tecnologia/xss-que-es-y-como-funciona-201805/#Como_funciona_el_Cross_Site_Scripting

Ceron, J. M., Scholten, C., Pras, A., & Santanna, J. (20 de abril de 2020). *MikroTik Devices Landscape, Realistic Honeypots, and Automated Attack Classification.* Obtenido de 10.1109/NOMS47738.2020.9110336

Cheng-yu, W. Shi-jun, Y. De-hao R.y Xiao-ping, J. "Investigación e implementación de NIDS basada en IXP2400", Segunda Conferencia Internacional de 2009 sobre Tecnología de la Información e Ingeniería de Gestión del Futuro , Sanya, 2009 , págs. 104-106, doi: 10.1109 / FITME.2009.32.

Ciberseguridad. (2019). *Ciberseguridad de las bases de datos*. Obtenido de https://ciberseguridad.com/guias/bases-datos/

CISCO. (2020). *¿Qué es un firewall?* Obtenido de https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

ciyi, C. G. (26 de Agosto de 2019). *Hacking Ético - Blog de seguridad de la información*. Obtenido de https://hacking-etico.com/2010/08/26/hablemos-de-spoofing/#:~:text=Ip%20Spoofing,-

Suplantaci%C3%B3n%20o%20falseamiento&text=El%20spoofing%20trae%20consigo%20el,la%20cual%20se%20desea%20suplantar

Clavijo , D., & Ciro Antonio. (2006). *Políticas de seguridad informática.* Obtenido de https://www.redalyc.org/pdf/2654/265420388008.pdf

Codigo, L. d. (Septiembre de 2009). *Escapar caracteres en JavaScript*. Obtenido de http://lineadecodigo.com/javascript/escapar-caracteres-en-javascript/?

Cosimo, I., Ahsan, A., Morabito, F. c., & Hussain, A. (Abril de 2020). *A novel statistical analysis and autoencoder driven intelligent intrusion detection approach.* Obtenido de https://doi.org/10.1016/j.neucom.2019.11.016

Coyla Jarita, Y. (26 de Mayo de 2019). Obtenido de Implementación de un sistema de detección y prevención de intrusos (IDS/IPS), basado en la norma ISO 27001, para el monitoreo perimetral de la seguridad informática, en la red de la Universidad Peruana Unión – Filial Juliaca: https://repositorio.upeu.edu.pe/handle/UPEU/2002

Coyla Jarita, Y. (25 de Mayo de 2019). *Implementación de un sistema de detección y prevención de intrusos (IDS/IPS), basado en la norma ISO 27001, para el monitoreo perimetral de la seguridad informática, en la red de la Universidad Peruana Unión – Filial Juliaca*. Obtenido de https://repositorio.upeu.edu.pe/handle/UPEU/2002

DETAILS, C. (2020). *Security Vulnerabilities*. Obtenido de https://www.cvedetails.com/vulnerability-list/vendor_id-11936/Tp-link.html

duiops. (s.f.). *duiops.net.* Obtenido de ¿Qué es un FTP / FTP Anónimo?: https://www.duiops.net/manuales/faqinternet/faqinternet15.htm

engineering, N. (s.f.). *¿Qué es Shodan y por qué deberías buscarte en él ahora mismo?* Obtenido de https://netcloudengineering.com/shodan-motor-busqueda/

Erlacher, F., & Dressler, F. (Agosto de 2018). *How to Test an IDS?: GENESIDS: An Automated System for Generating Attack Traffic.* Obtenido de How to Test an IDS?: GENESIDS: An Automated System for Generating Attack Traffic: https://dl-acm-org.aure.unab.edu.co/doi/abs/10.1145/3229598.3229601

GÓMEZ BAUTISTA, F. A., & REY SEPULVEDA, Y. A. (2019). DISEÑO DE RED BAYESIANA PARA LA PREDICCIÓN DE ATAQUES INFORMÁTICOS DE TIPO RANSOMWARE. Bucaramanga, Colombia.

Gupta, Alka, & Sharma, Lalit Sen. (Marzo de 2019). *Performance evaluation of Snort and Suricata intrusion detection systems on Ubuntu server.* Obtenido de SCOPUS: 10.1007/978-3-030-29407-6_58

H1RD SECURITY. (MAYO de 2017). *Ataque SQL Injection por error*. Obtenido de http://www.h1rd.com/hacking/sql-injection-por-error

HOSTALIA. (Diciembre de 2013). *Ataques de inyección SQL: qué son y cómo protegerse*. Obtenido de https://pressroom.hostalia.com/white-papers/ataques-inyeccion-sql/

IONOS, D. G. (15 de Mayo de 2020). *Digital Guide IONOS*. Obtenido de IP spoofing: así manipulan los atacantes tus paquetes de datos: https://www.ionos.es/digitalguide/servidores/seguridad/ip-spoofing-fundamentos-y-contramedidas/

ITCL. (10 de Julio de 2018). *La importancia de la Ciberseguridad*. Obtenido de https://itcl.es/itcl-noticias/la-importancia-de-la-ciberseguridad/

ITU X.1209. (2010). *X.1209 : Capabilities and their context scenarios for cybersecurity information sharing and exchange.* Obtenido de https://www.itu.int/rec/T-REC-X.1209-201012-I

ITU-X 1205. (2008). *Aspectos generales de la ciberseguridad.* Obtenido de https://www.itu.int/rec/T-REC-X.1205-200804-I

Jayner, Q. H. (19 de febrero de 2018). *IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN DE INTRUSOS*. Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/17438/8867918.pdf?sequence=1&isAllowed=y

Jimenez Castro, R. (21 de Diciembre de 2018). *Vulnerabilidades en redes WiFi ELO-323*. Obtenido de http://profesores.elo.utfsm.cl/~agv/elo323.ipd438/2s18/projects/reports/RodrigoJimenez/Informe_Proyecto_ELO323.pdf

John Galindo, CEO de Digiware. (23 de Noviembre de 2018). *La importancia de implementar políticas digitales para el 2020.* Obtenido de https://www.eltiempo.com/tecnosfera/dispositivos/la-ciberseguridad-un-tema-crucial-para-el-2020-297184

KirstenS. (2020). *OWASP*. Obtenido de Cross Site Scripting (XSS): https://owasp.org/www-community/attacks/xss/

Komar, B., Beekelaar, R., & Wettern, J. (2003). FIREWALL FOR DUMMIES. New York: Wiley Publishing, Inc.

Koskinen, T., Ihantola, P., & Karavirta, V. (3 de septiembre de 2012). *Quality of WordPress Plug-Ins: An Overview of Security and User Ratings.* Obtenido de 10.1109/SocialCom-PASSAT.2012.31

Kotenko, I., & Komashinsky, N. (Septiembre de 2019). *Combining spark and snort technologies for detection of network attacks and anomalies: assessment of performance for the big data framework.* Obtenido de https://dl-acm-org.aure.unab.edu.co/doi/abs/10.1145/3357613.3357630

Ley De Software Libre En Colombia. (2020). Obtenido de https://sites.google.com/site/unicesarlegislacion/Inf/home/Ley-De-Software-Libre-En-Colombia

M. Nandhini, & RaviTeja , G. (17 de Julio de 2017). *An analysis of various snort based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in Kali Linux environment.* Obtenido de 10.1109/ICICCT.2017.7975177

MAESTROS DEL WEB. (19 de Agosto de 2020). *Sistemas de Detección de intrusos y Snort.* Obtenido de http://www.maestrosdelweb.com/snort/

Martínez Cortes, J. F. (2015). *Seguridad de la Información en pequeñas y medianas empresas (PYMES)*. Obtenido de http://polux.unipiloto.edu.co:8080/00002332.pdf

MARTÍNEZ FLÓREZ, K. Y. (2014). *DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS SNORT Y UN SISTEMA TRAMPAS TIPO HONEYPOTS DE BAJA INTERACCION EN LA RED DEL GRUPO DE INVESTIGACIÓN GEOMATICA.* Obtenido de http://noesis.uis.edu.co/bitstream/123456789/37382/1/155750.pdf

Martinez, M. (Abril de 2017). *OWASP LATAM* . Obtenido de SQL INJECTION DEEP DIVE: https://owasp.org/www-pdf-archive//LatamTour2017_MateoMartinez_SQL_Injection_DeepDive.pdf

Micosoft. (16 de Marzo de 2017). *Inyección de código SQL.* Obtenido de https://docs.microsoft.com/es-es/sql/relational-databases/security/sql-injection?view=sql-server-ver15#:~:text=La%20inyecci%C3%B3n%20de%20c%C3%B3digo%20SQL%20es%20un%20ataque%20en%20el,para%20su%20an%C3%A1lisis%20y%20ejecuci%C3%B3n.

Mieres, J. (2009). *Ataques informáticos.* Obtenido de https://www.academia.edu/8522766/Ataques_inform%C3%A1ticos_Debilidades_de_seguridad_com%C3%BAnmente_explotadas

Minero Guardado, J. (22 de Julio de 2011). *Identificación y Clasificación de las Mejores Prácticas para Evitar la Inyección SQL en Aplicaciones Desarrolladas en PHP y PostgreSQL*. Obtenido de https://cimat.repositorioinstitucional.mx/jspui/bitstream/1008/412/1/ZACTE16.pdf

MINTIC. (04 de ENERO de 2009). *Ley 1273 de 2009.* Obtenido de https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

MinTIC. (28 de Diciembre de 2019). *MinTIC.* Obtenido de https://www.mintic.gov.co/portal/inicio/5306:Gobierno-en-L-nea-GEL

Molero, I. L. (1998). *REDES DE DATOS* . Obtenido de https://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/Redes%20de%20Area%20Local%20y%20Metropolitana-cd2/Contenido/RedesdeDatos.pdf

NetCloud Engineering. (2019). *NetCloud Engineering*. Obtenido de https://netcloudengineering.com/shodan-motor-busqueda/

NORMA TECNICA COLOMBIANA 27001. (2013). *TECNOLOGÍA DE LA INFORMACIÓN. TECNICAS DE SEGURIDAD. SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION.* BOGOTA: INCONTEC.

Normativa, S. Ú. (OCTUBRE de 2012). *JURISCOL*. Obtenido de http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507

Pacheco, R., Zambrano B., A., & Guailacela, F. (2019). *ANÁLISIS DE LA EFICIENCIA DE LOS IDS OPEN SOURCE SURICATA Y SNORT EN LAS PYMES.* Obtenido de http://repositorio.uees.edu.ec/handle/123456789/2926

Pacheco, R., Zambrano B., A., & Guailacela, F. (13 de Fevrero de 2019). *ANÁLISIS DE LA EFICIENCIA DE LOS IDS OPEN SOURCE SURICATA Y SNORT EN LAS PYMES.* Obtenido de Repositorio digital de la Universidad de Especialidades Espíritu Santo: http://repositorio.uees.edu.ec/handle/123456789/2926

pagelayer, & WordPress. (s.f.). *Complementos*. Obtenido de https://wordpress.org/plugins/pagelayer/

Patel, S. K., Rathod, V., & Parikh, S. (15 de marzo de 2011). *Joomla, Drupal and WordPress - a statistical comparison of open source CMS.* Obtenido de 10.1109/TISC.2011.6169111

POLNAL, D. C. (OCTUBRE de 2019). *INFORME DE LAS TENDENCIAS DEL CIBERCRIMEN EN COLOMBIA (2019-2020.* Obtenido de http://www.evaluamos.com/pdf/TENDENCIASCIBERCRIMEN.pdf

Pomsathit, A. (1 de Diciembre de 2017). *Performance analysis of IDS with honey pot on new media broadcasting.* Obtenido de IEEE: 10.1109/ICCDS.2017.8120478

QUINTERO HERRERA, J. A. (2018). *IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN DE INTRUSOS EN LA RED INTERNA DE LA ALCALDIA DE MONTERIA USANDO SOFTWARE LIBRE.* Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/17438/8867918.pdf?sequence=1&isAllowed=y

Risaralda, G. d. (16 de Marzo de 2019). *Política de Gobierno Digital*. Obtenido de https://www.risaralda.gov.co/tic/publicaciones/151547/politica-de-gobierno-digital/

Rodríguez Uribe, E. D., & Porras Medina, C. H. (2006). *SNORT*. Obtenido de http://www.fce.unal.edu.co/media/files/UIFCE/Otros/Snort.pdf

Romero Castro, M., Figueroa Moràn, G., & Vera Navarrete, D. (2018). *INTRODUCCIÓN A LA SEGURIDAD.* Obtenido de https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Romero Castro, M., Figueroa Moràn, G., & Vera Navarrete, D. (OCTUBRE de 2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMATICA Y EL ANÁLISIS DE*

VULNERABILIDADES. Obtenido de https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (Abril de 2018). *A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM).* Obtenido de IEEE: 10.1109/INCISCOS.2017.20

Sagala, A. (29 de octubre de 2015). *Automatic SNORT IDS rule generation based on honeypot log.* Obtenido de 10.1109/ICITEED.2015.7409013

Salehi, H., Shirazi, H., & Moghadam, R. A. (25 de abril de 2009). *Increasing Overall Network Security by Integrating Signature-Based NIDS with Packet Filtering Firewall.* Obtenido de 10.1109/JCAI.2009.12

Security, E. I. (01 de Junio de 2020). *Vulnerabilidad en WordPress*. Obtenido de https://www.entelgy.com/divisiones/innotec-security/actualidad-innotec-security/vulnerabilidades-innotec-security/vulnerabilidades/vulnerabilidad-en-wordpress-10926

Siva Kumar, K., Nanduri, Ashok Kumar, & Sujatha, V. (Febrero de 2020). *Implementation of intrusion detection system.* Obtenido de SCOPUS: https://url2.cl/4FMdS

SNORT. (2020). *Sistema de detección y prevención de intrusiones en la red*. Obtenido de https://www.snort.org/#documents

Suarez, D. (2018). Seguridad en redes. (pág. 20). España: UNIR.

TICbeat. (25 de Marzo de 2014). *Pymes, ¿un agujero de seguridad para las empresas grandes?* Obtenido de https://www.ticbeat.com/pymes/pymes-agujero-de-seguridad-para-las-empresas-grandes/

Vulnerabilidades en Joomla y Drupal. (Marzo de 2020). Obtenido de https://www.entelgy.com/divisiones/innotec-security/actualidad-innotec-security/vulnerabilidades-innotec-security/vulnerabilidades/vulnerabilidades-en-joomla-y-drupal

WordPress.org. (23 de Septiembre de 2020). *Plugins*. Obtenido de https://es-co.wordpress.org/plugins/elementor/#description

Xiaofeng, Jiahao, D., & Yifang, Z. (Abril de 2020). *An intrusion prevention scheme for malicious network traffic based on SDN.* Obtenido de SCOPUS: 10.1088/1757-899X/790/1/012030

Yang, J. Chen, X. Xiang X. y Wan, J. "HIDS-DT: An Effective Hybrid Intrusion Detection System Based on Decision Tree", Conferencia Internacional de 2010 sobre Comunicaciones y Computación Móvil, Shenzhen, 2010, págs. 70- 75, doi: 10.1109 / CMC.2010.73.

Zhang, B.-Y., Wei, C.-Z., Yang, X.-H., & Song, B.-B. (23 de Enero de 2020). *Design and implementation of a network based intrusion detection systems.* Obtenido de IEEE: 10.1109/SPAC46244.2018.8965538

A. Begum, MM Hassan, T. B. y M. S. (2016). *Inclusión de archivos locales (LFI) e inclusión de archivos remotos (RFI)*. *1*(December), 12–13.

Albataineh, A., & Alsmadi, I. (2019). IoT and the risk of internet exposure: Risk assessment using shodan queries. *20th IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks, WoWMoM 2019*. https://doi.org/10.1109/WoWMoM.2019.8792986

Asghar, M. T., Riaz, M., Ahmad, J., & Safdar, S. (2008). Security model for the protection of sensitive and confidential data on mobile devices. *IEEE- International Symposium on Biometrics and Security Technologies, ISBAST'08*, 1–5. https://doi.org/10.1109/ISBAST.2008.4547665

Bachmann, M. (2014). Passwords are dead: Alternative authentication methods. *Proceedings - 2014 IEEE Joint Intelligence and Security Informatics Conference, JISIC 2014*, 322. https://doi.org/10.1109/JISIC.2014.67

Farah, T., Shojol, M., Hassan, M., & Alam, D. (2016). Assessment of vulnerabilities of web applications of Bangladesh: A case study of XSS & CSRF. *2016 6th International Conference on Digital Information and Communication Technology and Its Applications, DICTAP 2016*, 74–78. https://doi.org/10.1109/DICTAP.2016.7544004

Gaddam, R. T., & Nandhini, M. (2017). An analysis of various snort based techniques to detect and prevent intrusions in networks: Proposal with code refactoring snort tool in Kali Linux environment. *Proceedings of the International Conference on Inventive Communication and Computational Technologies, ICICCT 2017*, *Icicct*, 10–15. https://doi.org/10.1109/ICICCT.2017.7975177

Hernán, C., & Medina, P. (2016). *Edson Dirceu Rodríguez Uribe Carlos Hernán Porras Medina*. http://www.fce.unal.edu.co/media/files/UIFCE/Otros/Snort.pdf

Kara, I., & Aydos, M. (2019). Detection and Analysis of Attacks Against Web Services by the SQL Injection Method [SQL Enjeksiyon Yöntemiyle Web Hizmetine Yönelik Saldiri Tespit ve Analizi]. *3rd International Symposium on Multidisciplinary Studies and Innovative Technologies, ISMSIT 2019 - Proceedings*, 6–9. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85078062305&doi=10.1109%2FISMSIT.2019.8932755&partnerID=40&md5=0576582b3b1968e1b3a9670f45dbbab7

Kaspersky. (2020). *¿Quién le espía? Ninguna empresa está a salvo del ciberespionaje*. 18. https://media.kaspersky.com/es/business-security/Cyber_Espionage_WhitePaper_FINAL_ES.pdf

Liu, T., & Zhang, L. T. (2019). Application of logistic regression in WEB vulnerability scanning. *Proceedings - 2018 International Conference on Sensor Networks and Signal Processing, SNSP 2018*, *978*, 486–490. https://doi.org/10.1109/SNSP.2018.00097

Martínez Cortes, J. F. (2015). Seguridad de la Información en pequeñas y medianas empresas (pymes). *Polux - Universidad Piloto de Colombia*, 8.

Martinez, M. (2017). *Sql injection deep dive*.

Mohammad, S., & Pourdavar, S. (2010). Penetration test: A case study on remote command execution security hole. *2010 5th International Conference on Digital Information Management, ICDIM 2010*, 412–416. https://doi.org/10.1109/ICDIM.2010.5664671

Monje Álvarez, C. A. (2011). Metodología de la investigación cuantitativa y cualitativa. Guía didáctica. *Universidad Surcolombiana*, 1–216. http://carmonje.wikispaces.com/file/view/Monje+Carlos+Arturo+-+Guía+didáctica+Metodología+de+la+investigación.pdf

Nacional Policia, CCIT, D. (2019). *TENDENCIAS CIBERCRIMEN EN COLOMBIA 2019-2020.*

https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf
Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE Communications Surveys and Tutorials*, *21*(3), 2702–2733. https://doi.org/10.1109/COMST.2019.2910750
Pranathi, K., Kranthi, S., Srisaila, A., & Madhavilatha, P. (2018). Attacks on Web Application Caused by Cross Site Scripting. *Proceedings of the 2nd International Conference on Electronics, Communication and Aerospace Technology, ICECA 2018*, *Iceca*, 1754–1759. https://doi.org/10.1109/ICECA.2018.8474765
Sabetghadam, S., Niamanesh, M., & Esmaeili, J. (2009). A model for assured software download on mobile terminals. *Proceedings - 2009 WRI International Conference on Communications and Mobile Computing, CMC 2009*, *2*, 432–436. https://doi.org/10.1109/CMC.2009.332
Sandirigama, M., & Idamekorala, R. (2009). Security weaknesses of WEP protocol IEEE 802.11b and enhancing the security with dynamic keys. *TIC-STH'09: 2009 IEEE Toronto International Conference - Science and Technology for Humanity*, 433–438. https://doi.org/10.1109/TIC-STH.2009.5444462
Sivaraman, K., & Khanna, V. (2016). Implementation of an extension for browser to detect vulnerable elements on web pages and avoid clickjacking. *Journal of Chemical and Pharmaceutical Sciences*, *9*(2), E396–E400.
Tenable, P. P. O. R. (2018). *Medir y gestionar los riesgos cibernéticos en las operaciones de negocios*.
VICTOR ANTONIO HOYOS BUITRON. (2015). *¿QUÉ TAL ESTA COLOMBIA EN CUESTIÓN DE CIBERSEGURIDAD? 3*(2), 54–67.
Yang, J., Chen, X., Xiang, X., & Wan, J. (2010). HIDS-DT: An effective hybrid intrusion detection system based on decision tree. *2010 WRI International Conference on Communications and Mobile Computing, CMC 2010*, *1*(2), 70–75. https://doi.org/10.1109/CMC.2010.73
Yusuf, S. E., Ge, M., Hong, J. B., Kim, H. K., Kim, P., & Kim, D. S. (2017). Security modelling and analysis of dynamic enterprise networks. *Proceedings - 2016 16th IEEE International Conference on Computer and Information Technology, CIT 2016, 2016 6th International Symposium on Cloud and Service Computing, IEEE SC2 2016 and 2016 International Symposium on Security and Privacy in Social Netwo*, 249–256. https://doi.org/10.1109/CIT.2016.88
Zambrano, A., & Guailacela, F. (2019). *Analysis of the efficiency of open source IDS Suricata and Snort in PYMES*.