INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 5 Núm. 2 (27-29 Octubre, 2021), pp. 1-17 https://doi.org/10.33936/isrtic.v5i2.3708 | ISSN 2550-6730

Recibido: 17/09/2021
Aceptado: 28/09/2021

Mecanismos de ciberseguridad basados en honeypots.

Alex Fernando Gilces Zambrano [1], Viviana Demera Centeno [1], Leticia Vaca-Cárdenas [1]

[1]Universidad Técnica de Manabí
[1]alex.gilces@utm.edu.ec [1]viviana.demera@utm.edu.ec [1]leticia.vaca@utm.edu.ec

RESUMEN La evolución vertiginosa de las tecnologías de la información y comunicación, ha generado en la sociedad contemporánea una creciente necesidad de interacción entre medios digitales y la mayoría de nuestras actividades productivas; sin embargo, a la par del auge de mayores y mejores oportunidades que nacen de esta sinergia, han ido apareciendo nuevos tipos de riesgos y amenazas computacionales, que han convertido a la seguridad de las redes en un problema de proporciones masivas; bajo este contexto, es necesario prestar mayor atención en el estudio de soluciones que permitan asegurar las disponibilidad de las comunicaciones. El objetivo de la presente investigación se enfocó en aplicar mecanismos de ciberseguridad basados en honeypots para mejorar la disponibilidad de la red en el Cuerpo de Bomberos de Portoviejo (CBP). Con este propósito sé definió un caso de estudio que permitió analizar la disponibilidad de la red de datos y evaluar el uso de mecanismos de ciberseguridad basados en honeypots; para lo cual, se implementó una infraestructura compuesta por un sistema de seguridad perimetral, sistema de detección y prevención de intrusos, honeypots, herramientas de monitoreo de red, herramientas de hacking ético, herramientas de análisis de vulnerabilidades, y servicios de usuario final. Los resultados obtenidos demuestran que la aplicación de mecanismos de ciberseguridad basados en honeypots mejoró la disponibilidad de la red en un 42.86 %.

Palabras claves: ciberseguridad, firewall, honeypot, T-Pot.

Cybersecurity mechanisms based on honeypots.

ABSTRACT The vertiginous evolution of information and communication technologies has generated in contemporary society a growing need for interaction between digital media and most of our productive activities; However, along with the rise of greater and better opportunities that arise from this synergy, new types of computer risks and threats have appeared, which have turned network security into a problem of massive proportions; In this context, it is necessary to pay greater attention to the study of solutions that allow ensuring the availability of communications. The objective of this research was focused on applying cybersecurity mechanisms based on honeypots to improve the availability of the network in the Portoviejo Fire Department (CBP). For this purpose, a case study was defined that allowed us to analyze the availability of the data network and evaluate the use of cybersecurity mechanisms based on honeypots; For which, an infrastructure composed of a perimeter security system, intrusion detection and prevention system, honeypots, network monitoring tools, ethical hacking tools, vulnerability analysis tools, and end-user services was implemented. The results obtained show that the application of cybersecurity mechanisms based on honeypots improved network availability by 42.86%.

KEYWORDS: cybersecurity, firewall, honeypot, T-Pot.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

1. Introducción

Los sistemas de información y redes de comunicación emergen como parte importante de la sociedad contemporánea, ya que su uso se encuentra asociado a la mayoría de actividades productivas de las organizaciones y ciudadanos. Con el desarrollo acelerado del internet, también emerge el lado oscuro y surgen nuevos términos como cibercrimen, ciberdelito o ciberdelincuencia, que describen de forma genérica los aspectos ilícitos cometidos en el ciberespacio. [1].

En un contexto mundial, el Foro Económico Mundial informo mediante el Global Risks Report 2019 que por tercer año consecutivo, los ciberataques junto a los fenómenos meteorológicos extremos, el fracaso de la protección del clima y los desastres naturales, se encuentran entre las amenazas mundiales más graves [2]. Los efectos de los ataques cibernéticos se están sintiendo en todo el mundo en múltiples sectores e industrias. Los daños causados incluyen directamente daños financieros, así como problemas de reputación, la pérdida de negocio, la incapacidad de proporcionar los servicios esperados, oportunidad costos y la pérdida de confianza [3]. Según fuentes especializadas, durante el primer semestre de 2020 los ataques con phising y malware pasaron de menos de 5 000 a más de 200 000 por semana. En ese lapso, la cantidad de ciberataques a nivel global creció un 34 % respecto al período inmediato anterior [4]. Entre los acontecimientos relacionados con los ciberataques más conocidos, podemos mencionar: Kosovo (1999) [5], ILoveYou (2000) [6], Taiwan (2003) [7], Conficker (2008) [8], Stuxnet (2010) [9], Petya (2016) [10], NotPetya (2017) [11], WannaCry (2017) [12].

En América Latina no se ha presentado un ciberataque importante que involucre a actores privados con gubernamentales, con fines o motivaciones políticas, como el ataque de denegación de servicio (DoS/DDoS) acontecido en Tallin-Estonia (2007) y Georgia-USA (2008) o ataques enfocados al daño de Infraestructura Nacional Crítica (INC), como el de Stuxnet (2010) [13]. Sin embargo, el Reporte de Seguridad de Latinoamérica 2019 de la prestigiosa empresa de ciberseguridad ESET revela que, del análisis de los datos suministrados por empresas de toda Latinoamérica, el 61 % de las mismas sufrió por lo menos un incidente de seguridad, siendo la infección con códigos maliciosos el más recurrente, (2 de cada 5 empresas sufrieron una infección de malware, incluyendo ransomware, en 2018) [14]. La Organización de Estados Americanos OEA reconoce que el sector financiero es tradicionalmente uno de los principales blancos de las amenazas cibernéticas. De acuerdo con el estudio de la OEA "El Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe," publicado en octubre de 2018, el 92 % de las entidades bancarias identificaron algún tipo de evento (ataques exitosos y no exitosos) de seguridad digital, y el 37 % de entidades bancarias manifestaron que sí fueron víctimas de ataques exitosos. La principal motivación de dichos ataques durante el año 2017 fueron motivos económicos (79 % de las entidades bancarias víctimas) [15]. El Reporte "Seguridad en el ruteo de América Latina y el Caribe" del Proyecto FORT, iniciativa conjunta de LACNIC y NIC.MX que busca aumentar la seguridad y la resiliencia de los sistemas de enrutamiento, señaló que registraron 4950 incidentes de seguridad de routing en el año 2017 y en el año 2018 registraron 3286; siendo Brasil donde ocurren más del 70 % de estos incidentes de América Latina, seguido de Colombia, como el segundo país con mayor cantidad de sistemas autónomos en los cuales algunos de sus prefijos fueron anunciados fraudulentamente por otros [16].

En el caso de Ecuador, se estima que además de los diez países más poblados de América Latina, entre los que cuentan con un acceso mayoritario a Internet se encuentra Ecuador con 81 % de penetración de internet [17]. La Fiscalía General de Estado de Ecuador a través de su Boletín titulado "Los delitos informáticos van desde el fraude hasta el espionaje" informa, que Internet abrió el paso a esas nuevas formas de delincuencia común y organizada que pone en riesgo la información privada, la seguridad en la navegación y de las instituciones públicas y privadas. Estos actos que se registran a través de la Internet son: fraude, robo, falsificaciones, suplantación de identidad, espionaje, clonación de tarjetas de crédito, entre otros [18]. Por otro lado, el Centro de Respuesta a Incidentes Informáticos (EcuCERT) de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), reportó que en el año 2018 gestionó diferentes tipos de vulnerabilidades distribuidas en 2′139,409 direcciones IP's, de entre las cuales registró 1′609,997 direcciones IP's comprometidas, detectando que los tipos de incidentes

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 5 Núm. 2 (27-29 Octubre, 2021), pp. 1-17 https://doi.org/10.33936/isrtic.v5i2.3708 | ISSN 2550-6730

denominados "Drones_Botnet" son los ataques que afectaron a mayor cantidad de direcciones IPs con un número de 898,512 direcciones IP en Ecuador [19]. De acuerdo al estudio "Deloitte 2018 Cyber Risk Information Security Study Ecuador" de la prestigiosa firma auditora Deloitte, se estima que 4 de cada 10 organizaciones en Ecuador sufrieron un incidente de seguridad en los últimos 24 meses [20]. El Reporte de Incidentes de Octubre 2019 del Equipo de Respuesta ante Incidencias de Seguridad Informáticas (CSIRT) de la importante empresa de Seguridad de la Información en Ecuador GMS, señala que Ecuador en el año 2018, tiene un alto índice de infecciones de ransomware, indicando que el 22 % de las empresas en Ecuador sufrieron de un ataque de ransomware, lo cual ubicó a Ecuador en el primer lugar del top de infección con códigos maliciosos de Latinoamérica en 2018; además también informó que durante este mismo año 2018, Ecuador se ubicó en el Top 10 de ataques de suplantación de identidad a nivel mundial con un porcentaje de 15,03 % [21].

En el marco de la pandemia COVID-19, en Ecuador se aceleró la transformación digital y la adopción de herramientas digitales, principalmente en el ámbito laboral, con escenarios y características de trabajo distintos a los que normalmente podrían encontrarse en una red corporativa; estas nuevas condiciones también definieron la proliferación de diversas amenazas informáticas [22]. En febrero de 2021, el Banco Pichincha admitió que se produjo un acceso no autorizado a los sistemas de un proveedor que presta servicios de mercadeo del Programa Pichincha Miles, mediante el cual presuntamente se filtró información sensible del banco respecto a datos de clientes, empleados, acceso a sistemas, tarjetas de crédito [23]; posteriormente se inició una campaña de correos electrónicos fraudulentos, en la que el atacante envío comunicaciones en nombre de Banco Pichincha a algunos clientes de dicho programa con el fin de obtener información necesaria para realizar transacciones ilegítimas [24]. Por otra parte, en julio de 2021, la empresa pública Corporación Nacional de Telecomunicaciones (CNT), presentó una denuncia ante la Fiscalía General del Estado por el delito de "ataque a los sistemas informáticos"; el ciberataque se habría registrado el 14 de julio 2021, y ocasionó intermitencias en los sistemas de atención al cliente, agencias y contact center, además alteró las áreas de facturación, activaciones y recargas; se conoció de fuentes internas de la empresa pública que el ataque informático es de tipo ransomware [25]. Así mismo, en julio de 2021, las autoridades de la Agencia Nacional de Tránsito (ANT), presentaron denuncias relacionadas con la vulneración de los sistemas informáticos y la entrega ilegal de licencias a nivel nacional. La situación llega hasta la existencia de una supuesta ANT virtual, a través de la cual se estaría entregando de manera fraudulenta entre 20.000 y 30.000 títulos habilitantes mediante el sistema hackeado, provocando perjuicios al Estado por concepto de evasión de pagos [26]. La ANT calculó que la afectación a los ciudadanos bordea los 23 millones de dólares y la perdida aproximada para el Estado, que deja de percibir los montos por el verdadero valor del documento, es de 2,5 millones de dólares [27].

2. Background

2.1. Honeypot

En la constante lucha para hacer que los sistemas de información sean más seguros, las organizaciones siempre están tratando de encontrar nuevas formas de abordar adecuadamente las cuestiones de seguridad [28]. La innovación tecnológica acelerada de los últimos años, ha hecho que las infraestructuras de red organizacionales necesiten, nuevos y diferentes tipos de equipos de redes, estaciones de trabajo, sistemas operativos, bases de datos y otros servicios; esto se traduce en la necesidad de utilizar como mecanismos de defensa varios dispositivos, sistemas, herramientas, o soluciones de seguridad al mismo tiempo, como, cortafuegos, sistemas de detec-ción y prevención de intrusos, honeypots, servidores, etc.

Un Honeypot es un dispositivo de seguridad basado en software, implementado para atraer a piratas informáticos mediante la visualización de servicios y puertos abiertos que son potencialmente vulnerables. Mientras los atacantes son desviados, sus actividades pueden ser monitoreadas y analizadas para identificar los métodos y tendencias de ataque actuales [29].

Según Joshi et al. [30], se puede agrupar los honeypots en 4 grandes categorías:

- **Basado en el uso:**
  - **Honeypots de producción:** aquellos que se utilizan para proteger a las organizaciones en entornos operativos de producción real [31].
  - **Honeypots de Investigación:** son desplegados y utilizados por investigadores para obtener información sobre los métodos de ataque utilizados por la comunidad blackhat para diseñar mejores herramientas de seguridad [32].

- **Basado en el nivel de interacción:**
  - **Honeypots de baja interacción:** utiliza clientes simulados en lugar de un sistema real para interactuar con los servidores [33].
  - **Honeypots de interacción media:** combina los aspectos más fuertes de los honeypots de baja y de alta interacción. La diferencia entre interacción media y alta es el nivel de riesgo asociado. Este tipo de honeypot se ejecuta en la capa de aplicación virtual y, por lo tanto, no emula completamente un entorno de sistema operativo [34].
  - **Honeypots de alta interacción:** constituyen una solución bastante compleja, puesto que implican la utilización de sistemas operativos y aplicaciones implementadas en hardware real, evitando la necesidad de utilizar software de emulación [35].

- **Basado en el tipo de implementación de hardware:**
  - **Honeypots físicos:** se trata de un equipo real dispuesto para ser atacado desde el exterior. Al ser un equipo físico, su funcionalidad es la que ofrezca de serie el equipo, sin ningún tipo de restricción [36].
  - **Honeypots virtuales:** se implementan utilizando una sola máquina física. Un solo sistema físico puede emular más de uno honeypot virtual. Pueden emular a más de un sistema operativo y pueden emular diferentes IP direcciones [37].

- **Basado en el rol de Honeypot:**
  - **Honeypot del lado del servidor:** la mayoría de los honeypots son del lado del servidor, como, por ejemplo: Honeyd y Dionaea, que esperan pasivamente ser atacados. Los adversarios encuentran estos honeypots por su propia iniciativa y los investigan y atacan [38].
  - **Honeypot del lado del cliente:** tiene como objetivo las vulnerabilidades de las aplicaciones del cliente. Requiere de una fuente de datos, la cual visita de forma activa, para detectar todas las actividades y juzgar si son seguras. Este tipo de honeypot adquiere activamente malware que se propaga a través del software de la aplicación cliente que los honeypot tradicionales no pueden obtener [39].

A continuación, se mencionan, algunas herramientas y servicios usadas regularmente en proyectos Honeypots:

- **Droidbox:** Es una herramienta para detectar aplicaciones maliciosas de Android. DroidBox detecta fugas de datos contaminando datos confidenciales y colocando sumideros de contaminación en toda la API. Además, al registrar parámetros de función API y valores de retorno relevantes, se puede descubrir un malware potencial y reportarlo para un análisis posterior [40].

- **Cowrie:** Emula un sistema de archivos y un shell para cada usuario que inicia sesión. Intenta imitar el comportamiento de un sistema real de la manera más fiel posible, mientras registra cada acción que un usuario realiza desde la conexión hasta la desconexión. Cada sesión comienza con una nueva configuración idéntica y cualquier cambio, como la creación de nuevos archivos, solo dura la duración de esa sesión. Además, cada sesión está protegida para que las acciones de diferentes usuarios no tengan impacto en sus pares [41].

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 5 Núm. 2 (27-29 Octubre, 2021), pp. 1-17 https://doi.org/10.33936/isrtic.v5i2.3708 | ISSN 2550-6730

- **Dionaea:** Es un honeypot de baja interacción, que proporciona algunos servicios como SMB, FTP, TFTP, VoIP. LibEmu son servicios proporcionados por Dionaea, este proporciona un shell al atacante mediante el enlace de puerto. El atacante intenta ejecutar su carga útil de malware en el shell [8] [9]. Dionaea registra todas las actividades del atacante. El objetivo principal de dionaea es obtener la copia del malware. Dionaea recolecta las llamadas API y Argument, usando las funciones que descargará la copia del malware usando HTTP [42].

- **Cuckoo Sandbox:** Conocidas también como cajas de arena. La Investigación dinámica de código malicioso se realiza mediante el uso de sandboxes. Donde las muestras no confiables se envían a cajas de arena. Los analistas de seguridad utilizan cajas de arena para descubrir el código malicioso de la muestra ejecutándolos en un entorno similar a la cárcel. Para realizar análisis dinámico de malware se puede utilizar Cuckoo sandbox. El objetivo principal, es que Cuckoo permite ejecutar clientes virtuales como VMware, KVM o Virtual Box. Este software de virtualización puede ejecutar sistemas operativos Windows, Linux y Mac. No solo archivos binarios, Cuckoo facilita hacer el análisis de las URL. Después de completar la investigación, los resultados se registran en una base de datos interna de Cuckoo, que finalmente genera reportes [43].

- **T-POT:** Es un sistema que se basa en daemons honeypots incluidos en contenedores, lo cual permite ejecutar múltiples daemons honeypot en la misma interfaz de red, manteniendo un pequeño espacio y restringiendo cada honeypot dentro de su propio entorno. La idea detrás de T-Pot es crear un sistema, cuyo rango completo de red TCP, así como algunos servicios UDP importantes, actúen como honeypot, y reenviar todo el tráfico de ataque entrante a los daemons honeypots más adecuados para responder y procesarlo [44]. T-Pot combina varias de las mejores tecnologías de honeypot disponibles (adbhoney, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, elasticpot, heralding, glutton, honeysap, honeytrap, mailoney, medpot, rdpy, glastopf, kippo) con la red IDS / IPS suricata, la monitorización y visualización de datos triple elasticsearch-logstash-kibana [45].

T-Pot también incluye las siguientes herramientas [46]:

- **Cockpit:** para una webgui liviana para docker, sistema operativo, monitoreo de rendimiento en tiempo real y terminal web.
- **Cyberchef:**una aplicación web para encriptación, codificación, compresión y análisis de datos.
- **ELK stack:** para visualizar todos los eventos capturados.
- **Elasticsearch Head:** un front-end web para navegar e interactuar con un clúster de Elastic Search.
- **Fatt:** un script basado en pyshark para extraer metadatos de red y huellas digitales de archivos pcap y tráfico de red en vivo.
- **Spiderfoot:** una herramienta de automatización de OSINT (Open Source Intelligence).
- **Suricata:** motor de monitoreo de seguridad de red.

Para efectos del presente estudio, después de evaluar algunas alternativas, se decidió utilizar la plataforma honeypot todo en uno T-POT, puesto que es un sistema honeypot fácil de implementar, requiere poco mantenimiento y agrupa algunas de las mejores tecnologías de honeypot en un solo sistema [44]; además cuenta con una interfaz gráfica web atractiva, responsiva, rápida, intuitiva y de fácil navegación.

Por todo lo mencionado con anterioridad, se planteó como objetivo de la investigación: "Aplicar mecanismos de ciberseguridad basados en honeypots para mejorar la disponibilidad de la red en Cuerpo de Bomberos de Portoviejo". En concordancia con lo manifestado anteriormente, se planteó como Hipótesis de esta investigación, lo siguiente: "Aplicar mecanismos de ciberseguridad basados en sistemas Honeypot mejorará la disponibilidad de la red de Cuerpo de Bomberos de Portoviejo".

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Figura 1: Dashboard T-POT

3. Materiales y Métodos

Para la realización del proyecto, se utilizó una metodología propuesta por los autores, que constaba de cuatro fases: 1) Fase de especificaciones, 2) Fase de diseño de caso de estudio aplicando mecanismos de ciberseguridad basados en sistemas honeypots, 3) Fase de implementación de entorno de pruebas, y 4) Fase de análisis de resultados. Cada una de las fases se detalla a continuación:

3.1. Fase de especificaciones

Se realizó un levantamiento de información preliminar, con el fin de obtener información relevante, respecto a los requerimientos técnicos necesarios para la realización de la presenta investigación. Se efectuó la revisión de normas, estándares, mejores prácticas, y de técnicas y herramientas utilizadas en las TICs. Se consideró entre los elementos básicos para una infraestructura TICs: los componentes de hardware y software, los componentes de red, la optimización de recursos, el análisis vulnerabilidades, las brechas en seguridad informática, así como las de la seguridad de la información, entre otros. Así mismo, se tomó conocimiento de la infraestructura de red actual de la entidad; en la Fig. 2 se muestra el diagrama de la topología de red actual del Cuerpo de Bomberos de Portoviejo, la cual no cuenta con mecanismos de ciberseguridad basados en sistemas honeypots que permitan desviar, monitorear, analizar e identificar los métodos y tendencias actuales de los ataques de los piratas informáticos.

3.2. Fase de diseño de caso de estudio aplicando mecanismos de mecanismos de ciberseguridad basados en sistemas honeypots

Considerando la información analizada en la fase de especificaciones, se determinó la necesidad de implementar diferentes herramientas que actuaron de soporte para el funcionamiento de dispositivos y aplicaciones; Se utilizó la solución de seguridad perimetral pfSense, las herramientas de monitoreo de red Bandwidth y Ntopng, las herramientas de seguridad informática Metasploit, Kali Linux, la herramienta de Análisis de Vulnerabilidades Nessus; así mismo se instaló servicios de Nextcloud y MariaDB. Por otra parte, como dispositivos de usuario final se utilizaron host con S.O. Ubuntu 18.04, Ubuntu 20.04 y Windows 10. Adicional, se aplicó mecanismos de ciberseguridad basados en sistemas Honeypot mediante la implementación de la solución honeypot T-Pot. En la 1 se detalla las herramientas utilizadas.

Todos estos dispositivos y herramientas utilizadas conformaron **escenarios de evaluación**, los cuales proporcionaron información medible y cuantificable. La recopilación de esta información medible

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 5 Núm. 2 (27-29 Octubre, 2021), pp. 1-17 https://doi.org/10.33936/isrtic.v5i2.3708 | ISSN 2550-6730

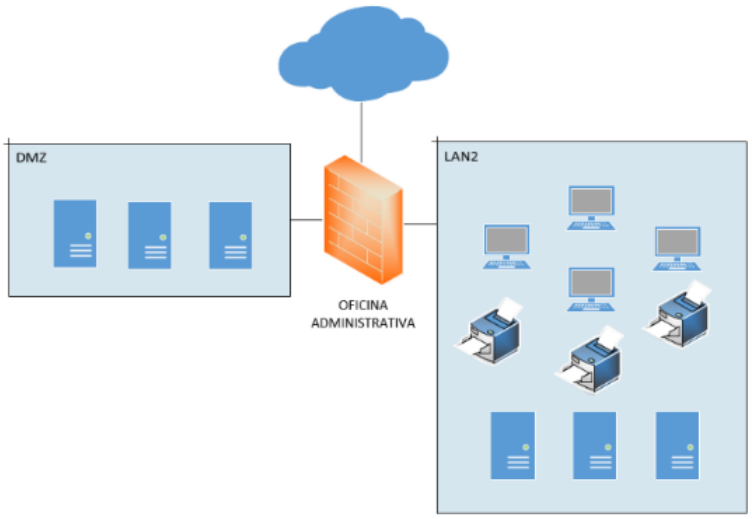


Figura 2: Topología actual de la red CBP.

Tabla 1: Herramientas utilizadas en el caso de estudio.

Componente	**Características**	**Breve descripción**
Kali Linux	Kali Linux Nessus	Herramienta de hacking ético y pruebas de penetración.
Honeypot	Tpot	Herramienta de seguridad informática para detectar y obtener información de ataques.
Firewall	pfSense	Herramienta de seguridad informática para filtrar tráfico de y bloquear accesos no autorizados.
Metasploit	Metasploit	Herramienta de seguridad informática para realizar pruebas vulnerabilidades de la red.
Cloud service	Ubuntu 18.04 Nextcloud	Herramienta que permite crear servicio de alojamiento de archivos.
Database service	Ubuntu 18.04 MariaDB	Sistema de gestión de bases de datos
VMWare Workstation	VMWare Workstation	Plataforma de Virtualización de Sistemas Operativos

y cuantificable, se la realizó en intervalos de tiempos de igual duración (7 días), a los cuales nos referiremos como **periodos de evaluación**.

Como parte del diseño de caso de estudio, se consideró el despliegue de **dos escenarios de evaluación**, cada uno realizado en un periodo de evaluación distinto. La diferencia entre los dos escenarios de evaluación, consiste en que, en el **primer escenario de evaluación no se aplicó mecanismos de ciberseguridad basados en sistemas honeypot**, de modo que las mediciones obtenidas en este primer escenario de evaluación, correspondieron a una red en su estado natural. Mientras que, por lo contrario, **en el segundo escenario de evaluación, si se aplicó mecanismos de ciberseguridad**

basados en sistemas honeypot; este segundo escenario de evaluación se constituyó al integrar la solución honeypot T-Pot a los dispositivos y herramientas desplegados en el primer escenario de evaluación; en consecuencia, se cuantificó el efecto causado al aplicar mecanismos de ciberseguridad basados en sistemas honeypot sobre un escenario de evaluación de red en su estado natural.

Luego de haber definido los escenarios de evaluación, se determinó la factibilidad de implementarlos en un entorno virtual. La 3 y 4 describen el diseño de las infraestructuras implementadas, correspondiente a los escenarios de evaluación del caso de estudio.

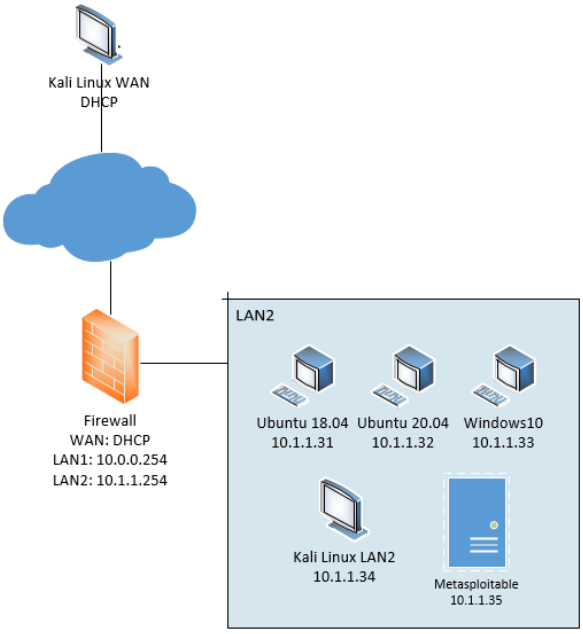


Figura 3: Diseño de caso de estudio; escenario de evaluación 1.

3.3. Fase de implementación de entornos de pruebas

Conforme a la información generada en la fase de diseño de caso de estudio aplicando mecanismos de mecanismos de ciberseguridad basados en sistemas honeypots, se procedió a realizar la instalación y configuración de las herramientas, en un entorno virtual, a través de la plataforma de virtualización VMWare Workstation. Cabe señalar que el host anfitrión de este entorno virtual, se ubicó en un segmento de red aislado a la red corporativa del Cuerpo de Bombero de Portoviejo, de tal manera, que se logró integrar los nuevos com-ponentes, sin interrumpir la red existente o crear puntos de vulnera-bilidad.

En primer lugar, se desplegó el **Escenario de Evaluación 1**, para lo cual se instaló el firewall pfSense y se configuró con 3 interfaces de red: WAN, LAN1 y LAN2. Se procedió a configurar los parámetros del firewall accediendo desde un navegador web a la IP asignada al puerto LAN2, donde se configuró reglas de tráfico de red de todas las interfaces del firewall pfSense; se configuró la primera interfaz como WAN; la segunda interfaz denominada LAN1 fue configurada como DMZ y en la tercera interfaz de red del firewall pfSense se dio de alta una red privada con la descripción LAN2. Además, se habilitó en el firewall pfSense el paquete IDS/IPS Suricata. Luego, se procedió a levantar en la LAN2, las herramientas de Pentesting Metasploit, Kali Linux y Nessus, los sistemas operativos de usuario final Ubuntu 18.04, Ubuntu 20.04, Windows 10 y habilitar servicios de Nextcloud y MariaDB.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 5 Núm. 2 (27-29 Octubre, 2021), pp. 1-17 https://doi.org/10.33936/isrtic.v5i2.3708 | ISSN 2550-6730

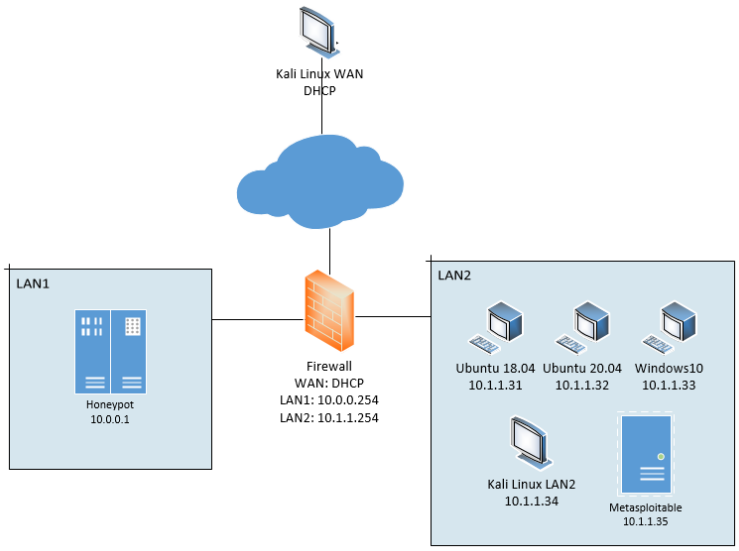


Figura 4: Diseño de caso de estudio; escenario de evaluación 2.

Posteriormente, en un segundo periodo de evaluación, se procedió a desplegar el **Escenario de Evaluación 2**, en el que se dio de alta en la DMZ (LAN1), la solución Honeypot T-Pot, cuyo objetivo es atraer los ataques de los piratas informáticos mediante la visualización de servicios y puertos abiertos que son potencialmente vulnerables, desviando sus actividades del tráfico legítimo para poder monitorear y analizar los métodos y tendencias de ataque actuales.

Por otra parte, cabe resaltar que, ambos escenarios, se encontraban expuestos a ciberataques desde el exterior; en este sentido, como parte del experimento, los investigadores generaron ataques de fuerza bruta (Brute Force Attack) y de denegación de servicio (Denial of Service Attack - DoS) desde un equipo Kali Linux localizado externamente (WAN) como se observa en la 3 y 4.

Finalmente, también es preciso señalar que, para realizar las mediciones de los escenarios de evaluación, se procedió con la monitorización de los componentes de la red de los escenarios de evaluación a través de las **herramientas instaladas en pfSense y Kali Linux LAN2.** Una vez que se obtuvieron los datos del tráfico de las comunicaciones de los dos escenarios de evaluación, se procedió a el análisis correspondiente.

3.4. Fase de análisis de resultados

El análisis de los resultados obtenidos durante la fase de implementación del entorno de pruebas se llevó a cabo, lo que nos permitió negar o aceptar la hipótesis propuesta y así poder concluir sobre lo observado en el caso de estudio. Para esta fase, se consideró las métricas señaladas en la 2; los valores de los parámetros de ancho de banda, paquetes recibidos y enviados, se obtuvieron mediante el uso de las herramientas Bandwidth y Ntopng, incluidos en el software pfSense. Además, se monitorizó el número de eventos sospechos con el paquete IDS/IPS Suricata de pfSense y el número de vulnerabilidades detectadas con la herramienta Nessus incluida en Kali Linux LAN2.

A continuación, se detalla los resultados obtenidos.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Tabla 2: Métricas consideradas para evaluar el entorno de prueba de caso de estudio.

Componente	**Características**	**Breve descripción**
Volumen de datos transferidos utilizando la red	Ancho de banda, Paquetes recibidos Paquetes enviados	Promedio de cantidad de datos que se pueden transferir en un lapso de tiempo específico. Se expresó en kbit/s.Volumen de tráfico entrante. Se expresa en MB. Volumen de tráfico saliente. Se expresa en MB.
Incidentes de Seguridad	Número eventos sospechosos Número de vulnerabilidades detectadas.	Cantidad de alertas recibidas en IDS. Se expresa en número enteros. Cantidad de vulnerabilidades detectadas en Pentesting. Se expresa en número enteros.

3.4.1. Verificación de volumen de datos transferidos utilizando la red

El volumen de datos transferidos se evaluó con las mediciones de ancho de banda, paquetes recibidos y paquetes enviados de los equipos de usuario final Ubuntu 18.04, Ubuntu 20.04 y Windows 10 que se realizaron en dos periodos de evaluación distintos; en la 3 se observa los resultados obtenidos en el **Escenario de Evaluación 1**, mientras que en la 4 se presentan los resultados obtenidos en el **Escenario de Evaluación 2**; donde se observa que el **Escenario de Evaluación 2** presenta una disminución en el volumen de datos transferidos, en relación con el **Escenario de Evaluación 1**.

Tabla 3: Métricas de volumen de datos transferidos obtenidos en el Escenario de Evaluación 1.

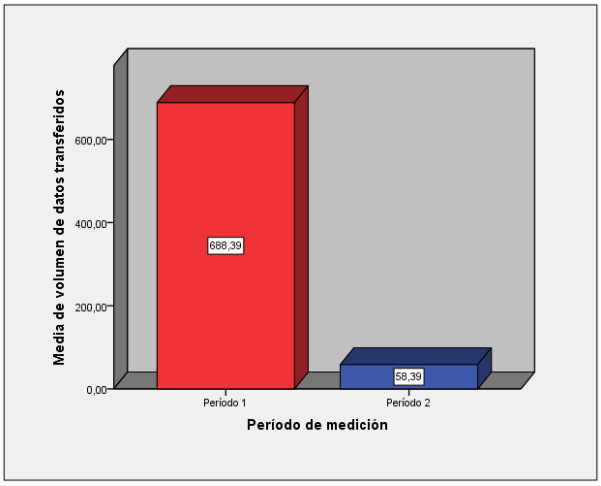
		Ubuntu 18.04 10.1.1.31	Ubuntu 20.04 10.1.1.32	Windows 10 10.1.1.33
Volumen de datos transferidos	Ancho de banda	Ancho de banda	25.83 kbits/s	38.12 kbits/s
	Paquetes Recibidos	1500 MB	498.9 MB	2100 MB
	Paquetes Enviados	508.6 MB	1200 MB	292.3 MB

Tabla 4: Métricas de volumen de datos transferidos obtenidos en el Escenario de Evaluación 2.

		Ubuntu 18.04 10.1.1.31	Ubuntu 20.04 10.1.1.32	Windows 10 10.1.1.33
Volumen de datos transferidos	Ancho de banda	24.28 kbits/s	25.83 kbits/s	26.28 kbits/s
	Paquetes Recibidos	99 MB	101.6 MB	212.7 MB
	Paquetes Enviados	14.6 MB	12.4 MB MB	8.8 MB

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 5 Núm. 2 (27-29 Octubre, 2021), pp. 1-17 https://doi.org/10.33936/isrtic.v5i2.3708 | ISSN 2550-6730

Figura 5: Gráfico de media de volumen de datos transferidos.



3.4.2. Verificación de Incidentes de Seguridad

La cantidad de incidentes de seguridad se evaluó con las mediciones de número de eventos sospechosos y número de vulnerabilidades detectadas de los equipos de usuario final Ubuntu 18.04, Ubuntu 20.04 y Windows 10 que se realizaron en dos periodos de evaluación distintos; en la 5 se observa los resultados obtenidos en el **Escenario de Evaluación 1**, mientras que en la 6 se presentan los resultados obtenidos en el **Escenario de Evaluación 2**; donde se observa que el **Escenario de Evaluación 2** presenta una disminución en la cantidad de incidentes de seguridad en relación al **Escenario de Evaluación 1**.

Tabla 5: Métricas de incidentes de seguridad obtenidos en el Escenario de Evaluación 1.

		Ubuntu 18.04 10.1.1.31	Ubuntu 20.04 10.1.1.32	Windows 10 10.1.1.33
Incidentes de seguridad	Número de eventos sospechosos	28557	17747	8588
	Número de vulnerabilidades detectadas	14	14	14

Tabla 6: Métricas de incidentes de seguridad obtenidos en el Escenario de Evaluación 2.

		Ubuntu 18.04 10.1.1.31	Ubuntu 20.04 10.1.1.32	Windows 10 10.1.1.33
Incidentes de seguridad	Número de eventos sospechosos	12980	7784	3143
	Número de vulnerabilidades detectadas	9	6	8

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

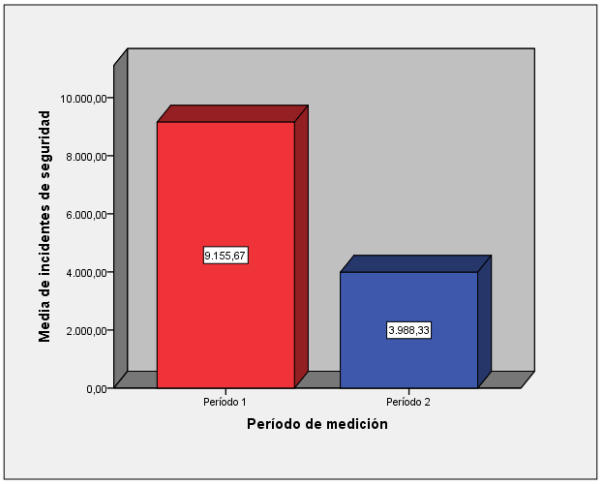


Figura 6: Gráfico de media de incidentes de seguridad.

3.4.3. Evaluación de los escenarios de evaluación

De lo señalado en el numeral 3.4.1 y 3.4.2, se desprende que las mediciones de los indicadores de volumen de datos transferidos e incidentes de seguridad realizados en equipos de usuario final Ubuntu 18.04, Ubuntu 20.04 y Windows 10, en dos periodos de evaluación distintos; demuestran que la media de las métricas del Escenario de Evaluación 1 corresponden al 71.43 %, lo cual es mayor a la media de las métricas del Escenario de Evaluación 2 que representan el 28.57 %, tal como se observa en la 7 y en la 7; lo cual denota una disminución en el volumen de datos transferidos e incidentes de seguridad de 42.86 % en el Escenario de Evaluación 2, con respecto al Escenario de Evaluación 1.

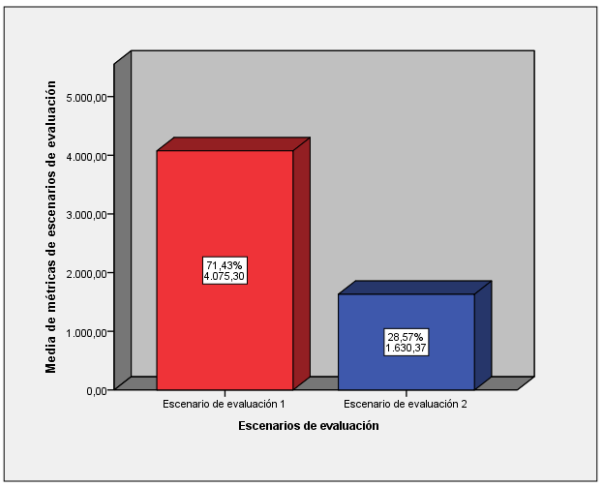


Figura 7: Gráfico de evaluación de media de métricas en los escenarios de evaluación.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 5 Núm. 2 (27-29 Octubre, 2021), pp. 1-17 https://doi.org/10.33936/isrtic.v5i2.3708 | ISSN 2550-6730

4. Resultados y Discusión

De acuerdo a Wang et al. [47], la tecnología de seguridad basada en honeypot, puede combatir eficazmente los ataques a la red. Así mismo, Sekar et al. [48] opina que el mecanismo basado en honeypot puede representar un gran obstáculo para los intrusos y piratas informáticos en la red. De la misma manera Ali y Kumar [42] señalan que Honeypot es uno de los mejores métodos para la captura de malware. Igualmente, Patel et al. [49] establece que los honeypots constituyen una buena mejora para el sistema de seguridad.[42]

En relación a la opinión de estos autores y de acuerdo a lo descrito en el apartado 3.2 y 3.3; se procedió a la creación de un entorno virtual donde se pudo reproducir la funcionalidad de una red, lo cual facilitó la evaluación de escenarios de experimentación o pruebas honeypots y la utilización de algunas herramientas. Estos escenarios de evaluación fueron expuestos en igualdad de condiciones a ciberamenzas externas al tiempo que se llevaron cabo ataques de Denegación de Servicios por parte de los investigadores.

Los resultados demostraron, conforme lo señalado en el apartado 3.4.3; que sin aplicar mecanismos de ciberseguridad basados en honeypots (Escenario de evaluación 1) se obtuvo un volumen de datos transferidos e incidentes de seguridad que afectan la disponibilidad de la red en un 71.43 %; mientras que al aplicar mecanismos de ciberseguridad basados en honeypots el volumen de datos transferidos e incidentes de seguridad fue mucho menor representando el 28.57 %. Esto significa que al aplicar mecanismos de ciberseguridad basados en honeypots se obtuvó una disminución en el volumen de datos transferidos e incidentes de seguridad lo cual representa una mejora en la disponibilidad de la red de 42.86 %.

Para la selección del tipo de prueba de hipótesis se realizó la Prueba de Wilcoxon, que corresponde a una prueba no paramétrica de comparación de dos muestras relacionadas; y para lo cual se utilizó el software estadístico IBM SPSS Statistics. A continuación, se presenta el detalle del análisis estadístico realizado y los resultados obtenidos conforme se muestra en la Tabla 7, 8 y 9.

Tabla 7: Estadísticos descriptivos.

	N	Media	Desviación Estandar	Mínimo	Máximo
Escenario1	15	4075,3013	8297,10586	14,00	28557,00
Escenario2	15	1630,3660	3771,56696	6,00	12980,00

Tabla 8: Métricas de incidentes de seguridad obtenidos en el Escenario de Evaluación 1.

		Ubuntu 18.04 10.1.1.31	Ubuntu 20.04 10.1.1.32	Windows 10 10.1.1.33
Escenario2 - Escenario1	Rangos negativos	14^a	7,50	105,00
	Rangos positivos	0^b	,00	,00
	Empates	0^c		
	Total	15		

a. Escenario2 <Escenario1 b. Escenario2 >Escenario1 c. Escenario2 = Escenario1

Tabla 9: Estadísticos de *prueba*[a]

	Escenario2-Escenario1
Z	$-3,296^{b}$
Sig. asintótica (bilateral)	,001
a. Prueba de rangos con signo de Wilcoxon b. Se basa en rangos positivos.	

A la luz de los resultados obtenidos en esta investigación, se evidencia que el valor de p (Sig. asintót. (bilateral)) es menor que 0,05, por tanto, se rechaza la hipótesis nula y se concluye que hay evidencias suficientes para plantear que efectivamente la aplicación de mecanismos de ciberseguridad basados en sistemas honeypots, si contribuyó a la mejora de la disponibilidad de la red de la organización en un 42.86 % con un nivel de significación del 5 %.

5. Conclusiones

La investigación realizada demuestra que el campo de la a ciberseguridad es un paradigma amplio y complejo, debido al vertiginoso incremento de riesgos informáticos que aparecen cada día; por esta razón se analizó diferentes elementos respecto a mecanismos de ciberseguridad y se determinó que la practica más acertada consiste en combinar adecuadamente varias tecnologías de seguridad, de tal forma que se complementen entre sí para proteger nuestros sistemas contra intrusiones basadas en la red y en el host.

En el caso de estudio se consideraron los recursos disponibles, la seguridad, los riesgos y la asequibilidad en la recopilación de datos; el uso de un entorno virtual, permitió la ejecución de pruebas de seguridad informática con un enfoque novedoso y poco explotado de la ciberseguridad; así mismo, posibilitó el ahorro de tiempo y la disminución de costos de experimentación, en comparación con pruebas en escenarios con equipos reales. A partir de la captura, detección y reconocimiento del tráfico sospechoso obtenidos de las mediciones realizadas en los escenarios de evaluación, se efectuó la valoración de trazas maliciosas en la red, lo que permitió analizar y generar estadísticas que ayudaron a concluir con éxito esta investigación.

Durante el desarrollo de esta investigación se observó que, aun disponiendo de un firewall como medida de seguridad, existen amenazas que están tratando de ingresar a la red, por lo que con la evidencia y explicación de los resultados del caso de estudio se pudo determinar que de acuerdo a la hipótesis establecida, la aplicación de mecanismos de ciberseguridad basados en sistemas honeypots si contribuye a la mejora de la disponibilidad de la red; sin embargo, esto no significa que se deba reemplazar las tecnologías de seguridad existentes, sino más bien a adoptar mecanismos de ciberseguridad basados en honeypots como un componente esencial en una operación de seguridad a nivel organizacional.

Referencias

[1] Vicente Pons Gamón. «Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad». En: *URVIO, Revista Latinoamericana de Estudios de Seguridad* 20 (2017), págs. 80-93.

[2] Marsh & McLennan Companies y Zurich Insurance Group. *The Global Risks Report 2019: insight report*. 2019.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 5 Núm. 2 (27-29 Octubre, 2021), pp. 1-17 https://doi.org/10.33936/isrtic.v5i2.3708 | ISSN 2550-6730

[3] Anna Nagurney y Shivani Shukla. «Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability». En: *European Journal of Operational Research* 260.2 (2017), págs. 588-600.

[4] Mariano Bartolomé y André Gustavo Monteiro Lima. «El ciberespacio, durante y después de la pandemia covid-19». En: *Revista de la Academia del Guerra del Ejército Ecuatoriano* 14.1 (2021), pág. 10.

[5] Francisco J Urueña Centeno. «Ciberataques, la mayor amenaza actual». En: *Revista del instituto español de estudios estratégicos* 1 (2015), pág. 42.

[6] S Hajioff y M McKee. «The'I love you'virus and its implications for genodiversity.» En: *Journal of the Royal Society of Medicine* 93.8 (2000), págs. 398-399.

[7] Luis Recalde H. «El ciberespacio: El nuevo teatro de guerra global». En: *Revista de Ciencias de Seguridad y Defensa* 1.2 (2016), pág. 5.

[8] Seungwon Shin, Guofei Gu, Narasimha Reddy y Christopher P Lee. «A large-scale empirical study of conficker». En: *IEEE Transactions on Information Forensics and Security* 7.2 (2012), págs. 676-690.

[9] P Shakarian. «Stuxnet: Revolución de ciberguerra en los asuntos militares». En: *Air & Space power journal* 11 (2010), págs. 50-59.

[10] Asibi O Imaji. «Ransomware Attacks: Critical Analysis, Threats, and Prevention Methods». En: *Hays, Kansas, Fort Hays State University* 39 (2019).

[11] Krzysztof Jan Jakubski. *Petya'2017. Kierunkowe ataki cybernetyczne*. Ago. de 2017.

[12] Saira Ghafur, Soren Kristensen, Kate Honeyford, Guy Martin, Ara Darzi y Paul Aylin. «A retrospective impact analysis of the WannaCry cyberattack on the NHS». En: *NPJ digital medicine* 2.1 (2019), págs. 1-7.

[13] Juan Antonio Manuel Aguilar. «Hechos ciberfiésicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad». En: *URVIO Revista Latinoamericana de Estudios de Seguridad* 25 (2019), págs. 24-40.

[14] ESET. *Eset security report Latinoamerica*. 2019.

[15] OEA y Asobancaria. *Desafíos del riesgo cibernético en el sector financiero para Colombia y América latina*. 2019.

[16] Augusto Luciano Mathurin. *Seguridad en el ruteo de América Latina y el Caribe*. Lanic, 2019.

[17] Statista. *¿Cuántos usuarios de Internet hay en América Latina?* Infografía. 2018.

[18] FGE: Fiscalía General del Estado. *Los delitos informáticos van desde el fraude hasta el espionaje*. Infografía. 2015.

[19] Arcotel. «EcuaCert». En: *Revista Institucional Arcotel Informa* 20 (2019), págs. 12-13.

[20] Deloitte. *Encuesta 2018 sobre Tendencias de Cyber Riesgos y Seguridad de la Información en Ecuador*. 2018.

[21] GMS. *GMS CSIRT: Computer Security Incident Response Team*. Oct. de 2018.

[22] D Ortiz. *Ecuador está entre los países con más ciberataques en América Latina*. 2021.

[23] Diario Expreso. *Banco Pichincha da más información sobre la supuesta filtración de datos de usuarios*. 2021.

[24] Banco Pichincha. *Comunicados Oficiales: Banco Pichincha*. 2021.

[25] El Comercio. *CNT apaga todas sus computadoras tras fuerte ataque informático*. 2021.

[26] Diario La hora. *ANT presenta quinta denuncia contra ataques informáticos*. 2021.

[27] Diario El Universo. *ANT anula 35.000 licencias de conducir fraudulentas. Así puede conocer la vigencia de su documento*. 2021.

[28] Vıéctor Daniel Gil Vera y Juan Carlos Gil Vera. «Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas». En: *Scientia et technica* 22.2 (2017), págs. 193-197.

[29] Diane Gan y Gary Kelly. «Analysis of Attacks Using a Honeypot». En: *International cybercrime, security and digital forensics conference*. Jun. de 2014.

[30] RC Joshi y Anjali Sardana. *Honeypots: a new paradigm to information security*. CRC Press, 2011.

[31] Miguel Hernández López y Carlos Francisco Lerma Reséndez. «Honeypots: basic concepts, classification and educational use as resources in information security education and courses». En: *Proceedings of the Informing Science & IT Education Conference (InSITE)*. Citeseer. 2008.

[32] Yogendra Kumar Jain y Surabhi Singh. «Honeypot based secure network system». En: *International Journal on Computer Science and Engineering* 3.2 (2011), págs. 612-620.

[33] Christian Seifert, Ian Welch, Peter Komisarczuk & et al. «Honeyc-the low-interaction client honeypot». En: *Proceedings of the 2007 NZCSRCS, Waikato University, Hamilton, New Zealand* 6 (2007).

[34] Christopher Kelly, Nikolaos Pitropakis, Alexios Mylonas, Sean McKeown y William J Buchanan. «A Comparative Analysis of Honeypots on Different Cloud Platforms». En: *Sensors* 21.7 (2021), pág. 2433.

[35] Tatiana Alexandra Vinueza Jaramillo. «Honeynet virtual híebrida en el entorno de red de la Universidad Técnica del Norte de la ciudad de Ibarra.» B.S. thesis. 2012.

[36] Incibe. *Guía de implantación de un honeypot industrial*. Instituto Nacional de Ciberseguridad de España. 2018.

[37] Yonas Kibret y Wang Yong. «Design and Implementation of Dynamic Hybrid Virtual Honeypot Architecture for Attack Analysis». En: *International Journal of Networked and Distributed Computing* 1.2 (2013), págs. 108-123.

[38] Wenjun Fan, Zhihui Du, David Fernández y Vıéctor A Villagrá. «Enabling an anatomic view to investigate honeypot systems: A survey». En: *IEEE Systems Journal* 12.4 (2018), págs. 3906-3919.

[39] Supinder Kaur y Harpreet Kaur. «Client honeypot based malware program detection embedded into web pages». En: *International Journal of Engineering Research and Applications* 3.6 (2013), págs. 849-854.

[40] Chun-Ying Huang, Ching-Hsiang Chiu, Chih-Hung Lin y Han-Wei Tzeng. «Code coverage measurement for Android dynamic analysis tools». En: *2015 IEEE International Conference on Mobile Services*. IEEE. 2015, págs. 209-216.

[41] Timothy Barron y Nick Nikiforakis. «Picky attackers: Quantifying the role of system properties on intruder behavior». En: *Proceedings of the 33rd Annual Computer Security Applications Conference*. 2017, págs. 387-398.

[42] P Dilsheer Ali y T Gireesh Kumar. «Malware capturing and detection in dionaea honeypot». En: *2017 Innovations in Power and Advanced Computing Technologies (i-PACT)*. IEEE. 2017, págs. 1-5.

[43] Sainadh Jamalpur, Yamini Sai Navya, Perla Raja, Gampala Tagore y G Rama Koteswara Rao. «Dynamic malware analysis using cuckoo sandbox». En: *2018 Second international conference on inventive communication and computational technologies (ICICCT)*. IEEE. 2018, págs. 1056-1060.

[44] The Honeynet Project. *Honeypot research*. Página Web.

[45] Telekom. *Introduction into T-Pot: A Multi-Honeypot Platform*. Página Web.

[46] Telekom. *Introduction into T-Pot: A Multi-Honeypot Platform*. Página Web.

[47] Keyong Wang, Mengyao Tong, Dequan Yang y Yuhang Liu. «A Web-Based Honeypot in IPv6 to Enhance Security». En: *Information* 11.9 (2020), pág. 440.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 5 Núm. 2 (27-29 Octubre, 2021), pp. 1-17 https://doi.org/10.33936/isrtic.v5i2.3708 | ISSN 2550-6730

[48] KR Sekar, V Gayathri, Gollapudi Anisha, KS Ravichandran y R Manikandan. «Dynamic honeypot configuration for intrusion detection». En: *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*. IEEE. 2018, págs. 1397-1401.

[49] Keyong Wang, Mengyao Tong, Dequan Yang y Yuhang Liu. «Implementation and behaviour analysis of honeypot». En: *International Journal of Research and Analytical Reviews (IJRAR)* 6.2 (2019), págs. 120-126.