



**UNIVERSIDAD CÉSAR VALLEJO**

**FACULTAD DE INGENIERÍA Y ARQUITECTURA  
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

**Sistema de seguridad usando Deep Learning para la prevención  
de ataques de denegación de servicio web en la empresa  
SISTEC, 2022**

**TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:  
Ingeniero de Sistemas**

**AUTOR:**

Rivera Mallma, Juan Willians (orcid.org/0000-0003-3602-9764)

**ASESOR:**

Cohello Aguirre, Rogelio Gonzalo (orcid.org/0000-0001-5526-5231)

**LÍNEA DE INVESTIGACIÓN:**

Sistemas de Información y Comunicaciones

**LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:**

Apoyo a la reducción de brechas y carencias en la educación en todos sus niveles

LIMA – PERÚ

2022

## **Dedicatoria**

Este trabajo esta principalmente dedicado a mi padre Juan Rivera Altamirano y a mi madre Angelica Mallma Zamora quienes me brindaron su apoyo y un soporte necesario para tener una motivación y así lograr mis objetivos, también dedico la tesis a mis docentes y mis compañeros que me apoyaron constantemente de manera emocional.

## **Agradecimiento**

En primero lugar quiero agradecer a mis padres que gracias a ellos tengo el apoyo necesario para seguir adelante, por todo el amor que me dan cada día, los alientos y los ánimos que suman constantemente para ser un buen profesional con visiones a futuros.

Por otra parte, agradezco a todas las personas que contribuyeron con esta investigación gracias por su aportes y conocimientos

## Índice de contenidos

Caràtula.....	i
Dedicatoria .....	ii
Agradecimiento .....	iii
Índice de contenidos .....	iv
Índice de tablas .....	v
Índice de anexos .....	vii
Índice de gráficos y figuras.....	viii
Resumen.....	xi
Abstract.....	xii
I. INTRODUCCIÓN.....	1
II. MARCO TEÓRICO.....	5
III. METODOLOGÍA.....	10
3.1. <i>Tipo y diseño de investigación</i> .....	10
3.2. <i>Variables y operacionalización</i> .....	11
3.3. <i>Población, muestra y muestreo</i> .....	12
3.4. <i>Técnicas e instrumentos de recolección de datos</i> .....	14
3.5. <i>Procedimientos</i> .....	16
3.6. <i>Método de análisis de datos</i> .....	18
3.7. <i>Aspectos éticos</i> .....	20
IV. RESULTADOS .....	21
V. DISCUSIÓN.....	42
VI. CONCLUSIONES.....	43
VII. RECOMENDACIONES .....	44
REFERENCIAS.....	45
ANEXOS .....	64

## Índice de tablas

Tabla 1 Tabla de indicadores .....	15
Tabla 2 Matriz de Confusión.....	16
Tabla 3 Equipos de ataque.....	18
Tabla 4: Wilcoxon – Prueba de Detección de ataques .....	21
Tabla 5: Contraste Estadístico - Detección de ataques.....	22
Tabla 6: Wilcoxon – Prueba de Exhaustividad .....	23
Tabla 7: Contraste Estadístico - Prueba de Exhaustividad.....	24
Tabla 8: Wilcoxon – Prueba de Tasa de error .....	25
Tabla 9: Contraste Estadístico - Prueba de Tasa de error .....	26
Tabla 10: Historia de usuario Login .....	65
Tabla 11: Historia de usuario Dashboard .....	66
Tabla 12: Historia de usuario Modulo de Mitigación DDoS .....	66
Tabla 13: Historia de usuario Modulo protección contra spam .....	67
Tabla 14: Historia de usuario Modulo protección contra bots .....	68
Tabla 15: Historia de usuario Modulo de clasificación de ataques .....	68
Tabla 16: Historia de usuario Modulo de banear IP.....	69
Tabla 17: Historia de usuario Entrenamiento del algoritmo de detección .....	69
Tabla 18: Tarjetas CRC Login .....	70
Tabla 19: Tarjetas CRC Dashboard .....	70
Tabla 20: Tarjetas CRC Módulo de Mitigación DDoS.....	71
Tabla 21: Tarjetas CRC Módulo de Protección contra Spam .....	71
Tabla 22: Tarjetas CRC Módulo de Protección contra Bots .....	72
Tabla 23: Tarjetas CRC Módulo de clasificación de ataques .....	72

Tabla 24: Tarjetas CRC Módulo de Banear IP .....	73
Tabla 25: Tarjetas CRC Entrenamiento de algoritmo de detección.....	74
Tabla 26: Prueba de aceptación Login.....	76
Tabla 27: Prueba de aceptación Modulo Dashboard .....	77
Tabla 28: Estrategia de búsqueda de información .....	79
Tabla 29: Recolección de datos .....	80
Tabla 30: Características de algoritmos para mitigar ataques de DDoS .....	81
Tabla 31: Características de algoritmos para mitigar ataques de DDoS 2 .....	82
Tabla 32: Clasificación de algoritmos para evitar ataques de DDoS.....	83

## Índice de anexos

Anexo 1: Matriz de operacionalización de variables.....	60
Anexo 2: Matriz de Consistencia.....	61
Anexo 3: Ficha de observación.....	62
Anexo 4: Arquitectura tecnológica para el usuario final.....	63
Anexo 5: Arquitectura tecnológica para el desarrollo del Sistema.....	64
Anexo 6: Metodología de desarrollo.....	68
Anexo 7: Clasificación de algoritmos para evitar ataques de Denegación de Servicio Web.....	82
Anexo 8: Algoritmo que usa El Software.....	87
Anexo 9: Prototipos del Software.....	91

## Índice de Gráficos y Figuras

Figura 1. Diseño Pre-Experimental .....	22
Figura 2: Registro del ataque con la Herramienta SLOWLORIS.....	40
Figura 3: Registro del ataque sin el sistema de seguridad.....	40
Figura 4: Sin acceso a la página web Durante el ataque DDoS sin el sistema de seguridad .....	41
Figura 5: Datos de IP y fecha al momento de hacer el ataque.....	42
Figura 6: Sin acceso a la página web Durante el ataque DDoS de 60 minutos sin el sistema de seguridad .....	43
Figura 7: Sin acceso a la página web Durante el ataque DDoS de 90 minutos sin el sistema de seguridad.....	43
Figura 8: Sin acceso a la página web Durante el ataque DDoS de 120 minutos sin el sistema de seguridad .....	44
Figura 9: Datos de IP y fecha al momento de hacer el ataque.....	44
Figura 10: Número de accesos de manera satisfactoria en cada tiempo del pre-Test.....	45
Figura 11: Ataque Post-test de 30 minutos .....	46
Figura 12: Resultado Post-Test Ataque de 30 minutos .....	47
Figura 13: Resultado Ataque post test de 30 minutos en el sistema de seguridad .....	47
Figura 14: Ataque Post-test de 60 minutos .....	48
Figura 15: Resultado Post-Test Ataque de 60 minutos .....	49
Figura 16: Resultado Ataque post test de 60 minutos en el sistema de seguridad .....	49
Figura 17: Ataque Post-test de 90 minutos .....	50



Figura 18: Resultado Ataque Post Test de 90 minutos .....	49
Figura 19: Resultado Ataque post test de 90 minutos en el sistema de seguridad .....	50
Figura 20: Ataque Post-test de 120 minutos .....	52
Figura 21: Resultado Post-Test Ataque de 120 minutos.....	53
Figura 22: Resultado Post-Test Ataque de 120 minutos con el sistema de seguridad .....	53
Figura 23. Arquitectura tecnológica para el usuario final.....	66
Figura 24. Arquitectura tecnológica para el desarrollo del Sistema .....	67
Figura 25: Código del sistema de protección .....	77
Figura 26: Código del sistema de protección 2 .....	77
Figura 27: Código del sistema de protección 3 .....	78
Figura 28: Código del sistema de protección 4 .....	78
Figura 29: Estructura de directorios y convenciones de nomenclatura de archivos .....	79
Figura 30: Prueba de Carga Utilizando la herramienta JMeter .....	80
Figura 31: Prueba de Carga Utilizando la herramienta JMeter 2 .....	81
Figura 32: Prueba de Carga Utilizando la herramienta JMeter 3 .....	82
Figura 33. Datos que serán enviados .....	87
Figura 34. Algoritmo Análisis de datos.....	88
Figura 35. Algoritmo puntajes de precisión .....	89
Figura 36. Algoritmo puntajes de Modelo de entrenamiento .....	90
Figura 37. Interfaz de registro de login.....	91
Figura 38. Interfaz de Dashboard.....	92
Figura 39. Interfaz de Modulo Protección DDoS .....	93
Figura 40. Interfaz de Modulo Protección DDoS Desactivado .....	94

Figura 41. Interfaz de Modulo Protección Checking Desactivado .....	95
Figura 42. Interfaz de Modulo Protección contra Spam Activado.....	96
Figura 43. Interfaz de Modulo Protección contra Spam Desactivado.....	96
Figura 44. Interfaz de Modulo Protección contra Bots.....	97
Figura 45. Interfaz de Modulo Protección contra bots falsos y bots anónimos.....	98
Figura 46. Interfaz de Lista de los ataques DDoS .....	99
Figura 47. Interfaz de interfaz de búsqueda por palabra.....	100
Figura 48. Interfaz de interfaz de ban por IP .....	100
Figura 49. Interfaz de interfaz de ban por País. ....	101
Figura 50. Interfaz de interfaz de lista Blanca .....	102
Figura 51. Interfaz de usuario .....	102
Figura 52. Interfaz de interfaz de agregar usuario .....	103
Figura 53. Interfaz de interfaz de Checking DDoS .....	104
Figura 54. Interfaz de interfaz Core.....	105

## Resumen

La presente investigación tiene como problemática principal la respuesta de dicha pregunta ¿Como un sistema de seguridad usando Deep Learning previene y detecta ataques de DDoS en un servidor web?

Advisors (2022) Para llevar a cabo este tipo de ataques, los ciberdelincuentes realizan multitud de peticiones al sistema desde múltiples ordenadores, que en conjunto forman una enorme botnet o botnet. Como resultado, los dispositivos de red, los sistemas operativos y los servicios del servidor no pudieron responder ni procesar las solicitudes dentro del período de tiempo especificado.

Tomando en cuenta como referencia diversos estudios enfocados al tema, se desarrollará el presente proyecto. Teniendo como objetivo principal de dicha investigación determinar el efecto del uso de un sistema de seguridad usando Deep Learning para mitigar ataques de denegación de servicio web

Para la presente tesis se tomó como tipo de investigación un diseño preexperimental enfocándose a un resultado cuantitativo, en primer lugar, se consideran estas variables o métricas definidas, como el número de ataques a prevenir.

Los resultados obtenidos nos brindan un enfoque de ciberseguridad para la mitigación de riesgos utilizando los métodos y algoritmos propuestos en el estudio.

**Palabras clave:** Machine learning, deep Learning, algoritmos, denegación de servicio

## **Abstract**

The main problem of this research is the answer to this question: How does a security system using Deep Learning prevent and detect DDoS attacks on a web server?

Advisors (2022) To carry out this type of attack, cybercriminals make a multitude of requests to the system from multiple computers, which together form a huge botnet or botnet. As a result, network devices, operating systems and server services were unable to respond or process the requests within the specified time period.

Taking into account as a reference several studies focused on the subject, the present project will be developed. The main objective of this research is to determine the effect of using a security system using Deep Learning to mitigate web denial of service attacks.

For the present thesis, a pre-experimental design was taken as a type of research focusing on a quantitative result, first of all, these variables or metrics defined as the number of attacks to be prevented are considered.

The results obtained provide us with a cybersecurity approach for risk mitigation using the methods and algorithms proposed in the study.

**Keywords:** Machine learning, deep learning, algorithms,  
denial of service

## I. INTRODUCCIÓN

En seguridad informática, la detección de intrusos es el arte de atrapar o detectar usuarios no autorizados o malintencionados que intentan acceder a una red.

Según Cañola (2020) “A medida que los servicios y servicios de Internet aumentan de tamaño y a pesar de los esfuerzos para proteger los sistemas informáticos, los delitos informáticos continúan creciendo exponencialmente y los profesionales se ven con la necesidad de optar herramientas sofisticadas para detectar intrusos y pasar de una respuesta preventiva a una reactiva.”

Guaigua (2021) afirma que la naturaleza de estos ataques puede requerir el uso de métodos logarítmicos complejos, la mayoría de los cuales estudian el comportamiento del usuario, separando a los usuarios legítimos de los atacantes. Para sistemas vulnerables, se comunica internamente con otros sistemas afectados para lograr el objetivo del servicio vulnerable.

De acuerdo con Alcántara (2017) Se han implementado protocolos para proteger los datos de quienes utilizan estos canales, así como el uso de métodos y herramientas especializadas algunas tareas Sistema de detección de intrusos (IDS) Son útiles para encontrar seguridad al proporcionar medidas de detección cuando se encuentran acceso no autorizado a la red.

Herranz, y otros, (2018) indica que, En los últimos tiempos, la población ha extendido la carencia de crear, difundir y gestionar datos, la cual ha comenzado a jugar un papel importante en todos los aspectos, desde el aspecto cultural y de ocio hasta el económico, sanitario y de prestación de servicios de recursos comunes.

Con respecto a la seguridad informática es difícil no leer las noticias diarias sobre piratería de datos, ataques DDOS en servidores y muchos otros robos cometidos por piratas informáticos. De acuerdo Lizares y otros, (2017) manifiesta que un atacante es una forma por el cual ciertos individuos intentan tener el control de un sistema informático con el objetivo, interrumpir o dañar otros sistemas informáticos.

También puede ser un intento organizado y deliberado de una o más personas para dañar o interrumpir un sistema informático o una red.

Tenga en cuenta que la mayoría de las computadoras contienen información que es sensible a las vulnerabilidades de la computadora, por lo que las empresas están expuestas a una variedad de amenazas., como la pérdida de oportunidades comerciales debido a la falta de fuerza en tiempo real. Esto puede perjudicar la reputación de la Compañía y reducir sus potenciales comerciales.

Se puede decir que los ataques DDoS pueden llegar a tener consecuencias nefastas para dichas organizaciones que carecen de una protección adecuada contra este tipo de vulnerabilidad. En ese mismo sentido. En ese mismo sentido Aguilar (2019) aclara que Los ataques informáticos consisten en explotar vulnerabilidades en software y hardware del entorno informático. Tiene un beneficio económico predominante que impacta de forma negativa a la seguridad del sistema y perjudica directamente a los activos de dicha organización.

Se puede decir que entre los diferentes tipos de ataques informáticos que existen, se pueden distinguir en primer lugar los ataques que provocan cambios perjudiciales en el estado de la información y los recursos del sistema, y los ataques leves que limitan el consumo de recursos o el acceso a la información. sistema.

Del mismo modo Gómez (2020) nos menciona que Hoy en día, casi todos los ataques DDoS se lanzan desde redes informáticas, zombis o botnets remotos, bien organizados y controlados de forma remota Internet está atacando a todos los mismos objetivos

Como se muestra, la justificación del estudio actual se evalúa con base en los resultados obtenidos durante el diseño y análisis de sistemas basados en Sistemas de seguridad basado en algoritmos de Deep Learning para mitigar ataques de denegación de servicio.

En la justificación teórica, Guaigua (2021) justifica demostrando que los estudios anteriores se sustentan teóricamente con el objetivo de prevenir y detectar ataques DDoS en una organización, ya que cada organización siempre busca limitar su riesgo tanto como sea posible.

Con base en lo que los autores han demostrado hasta el momento, afirmamos que la razón fundamental de esta investigación es prevenir posibles ataques de denegación de servicio favoreciendo los sistemas afectados por dichos ataques, aumentando así la integridad y disponibilidad de los servicios proporcionados por las empresas.

En la justificación Metodológica, para lograr los objetivos de la investigación, utilizar métodos de investigación tales como actas para medir las variables identificadas.

Sobre la base de la realidad problemática descrita se planteó e identificó como problema general ¿De qué manera influye un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web en la empresa Sistec? Por lo que mediante este se sugirieron problemas específicos.

- PE1: ¿De qué manera influye un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web en la empresa Sistec en base a la Detección de anomalías?
- PE2: ¿De qué manera influye un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web en la empresa Sistec en base a la exhaustividad?

Como Objetivo General se busca determinar de qué manera influye un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web en la empresa Sistec

OE1: Determinar de qué manera influye un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web en la empresa Sistec en base a la Detección de anomalías.

OE3: Determinar de qué manera influye un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web en la empresa Sistec en base a la exhaustividad.

Como Hipótesis general es el uso de un sistema seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web mejorara la seguridad de la empresa SISTEC, 2022.

- H1: El uso de un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web aumentará la detección de anomalías en la empresa SISTEC
- H2: El uso de un sistema seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web aumentará la exhaustividad en la empresa SISTEC, 2022

Gómez (2020) Señala que el uso de algoritmos de aprendizaje profundo ayuda a la identificación de IP malignas y las clasifica según su complejidad.

## **II. MARCO TEÓRICO**



A continuación de este capítulo hay una colección de hallazgos de investigación, precedentes, estudios y estudios encontrados en el ámbito nacional e internacional de varias fuentes de datos y repositorios académicos relacionados con este proyecto, teniendo en cuenta la referencia general de mi título. El análisis de estos documentos proporciona información relacionada con el tema de investigación actual y proporciona diferentes tipos de información para su refinamiento preciso.

Cañola (2020) Desarrolló de un software para la prevención de ataques de denegación de servicio web utilizando Deep Learning. Cañola (2020) tuvo como objetivo Desarrollar un software para la prevención de ataques de denegación de servicio web utilizando un algoritmo de aprendizaje profundo. Como conclusión, el trabajo realizado proporciona una aplicación para sistemas IDS/IPS utilizando un modelo entrenado de aprendizaje profundo que ha sido probado con ataques DoS que incluyen conjuntos de datos de entrenamiento y ataques que no están incluidos en el conjunto de datos. Cañola (2020) recomiendan que hay muchos otros algoritmos que pueden probar y validar los resultados, por lo que se recomienda que utilice otros algoritmos de aprendizaje profundo para entrenar su modelo de clasificación.

Lizares, y otros (2017) Investigo Los ataques informáticos y su incidencia en la seguridad de servidores con sistema operativo Linux de entidades de gobierno local. Lizares, y otros (2017) Tuvo como objetivo Elaborar una propuesta para reducir el riesgo de phishing y ataques DDoS en los servidores Linux de GADPO (Gobierno Autónomo Descentralizado de la Provincia de Orellana). Cuenta con un enfoque cualitativo y cuantitativo. Es cuantitativo ya que intenta determinar la frecuencia que pueda llegar a tener los ataques informáticos a la seguridad de los servidores. Lizares, y otros (2017) concluye que la metodología de gestión de riesgos de MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) sirvió como guía para identificar vulnerabilidades, impactos y riesgos causados por el phishing de GADPO contra servidores Linux y ataques informáticos DDoS.

Gómez (2020) Diseño un Sistema de detección de ataques de DDoS basado en modelos de aprendizaje de máquina para la arquitectura sdn. Macias (2020) cuyo

objetivo es la clasificación del flujo que debe hacerse en tiempo real dos clases de redes bidireccionales. Así mismo utilizó la metodología experimental, esto se hace para la evaluación de un mecanismo de detección de ataques DDoS. En concreto, describe los escenarios de prueba utilizados y el modelo de clasificación utilizado. Gómez (2020) recomienda utilizar otros lenguajes de programación para entrenar y optimizar modelos de aprendizaje profundo como Python y C/C++.

Alvarado y Changoluisa (2019) Investigaron sobre el Análisis de la ciberseguridad a la infraestructura tecnológica de la universidad técnica de Cotopaxi. Alvarado y Changoluisa (2019) Así mismo utilizaron la metodología experimental ya que se utiliza para conocer los antecedentes, versión, características, fortalezas, debilidades y demás aspectos necesarios para establecer una vulnerabilidad que existe en un país. Alvarado y Changoluisa (2019) recomiendan que para el caso de las vulnerabilidades web, es importante investigar las alertas detectadas con más detalle. Sin embargo, no son críticos, pero es importante capturarlos.

Garzón, Ratkovich y Vergara (2013) En el artículo METODOLOGÍA DE ANÁLISIS DE VULNERABILIDADES PARA EMPRESAS DE MEDIA Y PEQUEÑA ESCALA, desarrollado por la Pontificia Universidad Javeriana de Colombia donde el enfoque principal fue proteger los recursos corporativos con los pilares fundamentales que son la integridad a los datos, la disponibilidad y la auditabilidad. Garzón, Ratkovich y Vergara (2013) concluye que, Mediante la configuración adecuada de dispositivos, servicios y aplicaciones, las empresas pueden eliminar significativamente las vulnerabilidades de seguridad que presentan y aumentar el potencial de ataques de terceros que podrían aprovechar dichas vulnerabilidades.

Barrera, Manuel (2007) Investigó sobre la Mitigación de DDoS Mediante técnicas de Minería de datos usando ambientes virtuales en Linux, Desarrollado en el Instituto Tecnológico y Estudios Superiores de Monterrey donde tuvo como objetivo la mitigación de ataques DDoS sin poder afectar el trafico legitimo que este pueda brindar. Barrera, Manuel (2007) concluye que el objetivo de este documento es validar

la eficacia de la tecnología de minería de datos para defenderse de los ataques DDoS y demostrar el enorme potencial que esta tecnología puede lograr.

Santivañez (2020) Estudio del Rendimiento de sistemas de detección de intrusos en redes, Desarrollado en la universidad Católica del Perú donde tuvo como objetivo realizar investigaciones sobre el desempeño de diversas soluciones de sistemas de detección de intrusos basados en redes estandarizadas por un software. En su trabajo se utiliza la metodología de investigación. Esto significa que se utilizan burós de crédito. B. Documentos proporcionados en revistas y conferencias sobre soluciones IDS. Santivañez (2020) concluye que la propuesta de solución IDPS más interesante fue IntelliFlow por su arquitectura y funcionalidad. Además, su primer resultado fue la evaluación fue alentadora, ya que mostró la mitigación de los ataques DoS y Escaneo de puertos y fuerza bruta

Aguinaga (2018) Los ataques de vulnerabilidad funcionan enviando uno o más paquetes especialmente diseñados a una aplicación con una vulnerabilidad particular. Los ataques de inundación, por otro lado, funcionan mediante el envío de una avalancha de mensajes al objetivo del ataque, por lo que lidiar con ellos significa agotar recursos críticos para esa víctima. Cuando se agoten los recursos, los clientes legítimos no podrán utilizar el servicio.

### **Ataques de Denegación de Servicio Distribuido**

Cantón (2021) nos menciona que el concepto de "distribuido" se refiere al hecho de que estas solicitudes se realizan desde cientos o miles de máquinas infectadas (a menudo denominadas "zombis") que se gestionan a través de una "red de bots" de forma coordinada. Al mismo tiempo, supongamos que el servidor no puede admitir ancho de banda, uso de memoria y procesamiento, el servicio termina siendo atacado debido a que no puede cumplir con todas las solicitudes.

## **Inteligencia artificial**

López (2022) nos define que La inteligencia artificial consiste en permitir que las máquinas resuelvan problemas que solo pueden ser resueltos por humanos. Usando inteligencia artificial, las computadoras están tratando de resolver problemas que solo los humanos pueden resolver.

## **Deep Learning**

El aprendizaje profundo utiliza redes neuronales artificiales con múltiples jerarquías para llevar a cabo el proceso de aprendizaje automático. La red aprende algo sencillo en la parte inferior de la jerarquía y pasa ese conocimiento al siguiente nivel. La segunda capa combina esta información básica con información un poco más compleja y la transfiere a la tercera capa, y así sucesivamente.

## **Algoritmo Token Bucket**

Hernández (2018) Este es un algoritmo que nos permite tener un mejor control de tráfico a nuestra red, lo que reduce el consumo de recursos de nuestros enrutadores. Esto se logra mediante la creación de una cola que permite la transferencia de paquetes con tokens disponibles, que se impone en un límite de tasa de transferencia aceptable.

## **Ataque por inundación de paquetes SYN**

Cloudflare, Inc. (2022) Un ataque DDoS (denegación de servicio) llamado inundación SYN (ataque semiabierto) tiene como objetivo hacer que un servidor sea inaccesible para el tráfico legítimo al consumir todos los recursos. Un atacante puede obligar a un dispositivo a responder muy lentamente o no responder en absoluto al tráfico legítimo inundando todos los puertos del servidor atacante con paquetes de solicitud de conexión inicial (SYN).

## **Ataque DDoS Botnet**

Advisors (2022) Para llevar a cabo este tipo de ataques, los ciberdelincuentes realizan multitud de peticiones al sistema desde múltiples ordenadores, que en conjunto forman una enorme botnet o botnet. Como resultado, los dispositivos de red, los sistemas operativos y los servicios del servidor no pudieron responder ni procesar las solicitudes dentro del período de tiempo especificado.

## **Inundación UDP**

De Luz (2022) El protocolo UDP se utiliza principalmente para intentar saturar el ancho de banda objetivo para sobrecargar el puerto del servidor. Este tipo de ataque es el más poderoso ya que te permite saturar servicios con alto ancho de banda. Al igual que la inundación de ping, el principio es saturar el sistema de destino en función de una gran afluencia de datos entrantes.

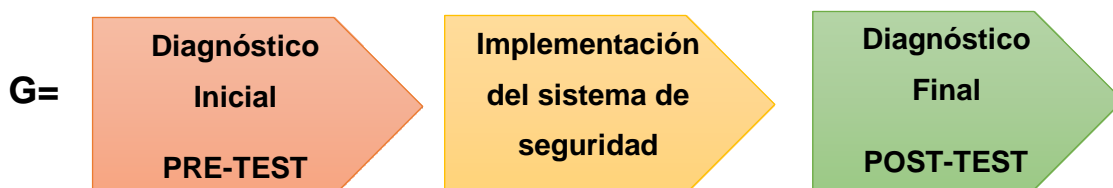
### III. METODOLOGÍA

Este capítulo se mencionará el tipo y diseño del estudio, las variables de análisis y operativas, la muestra, la población, la muestra que se seleccionará, las herramientas de recopilación de datos utilizadas, los procedimientos analíticos y los métodos y técnicas de análisis. Se cumplen los estándares éticos y de análisis de datos precisos.

#### 3.1 Tipo y diseño de investigación

##### 3.1.1 Tipo de investigación

El tipo de investigación será aplicada Chávez (2019) muestran como el tipo de investigación aplicada es principalmente para resolver problemas en poco tiempo. Nuestro objetivo es la aplicación inmediata a través de acciones concretas para abordar el problema. Por lo tanto, las acciones futuras están dirigidas a actividades concretas para abordar el problema, no para desarrollar la teoría y sus consecuencias. (p. 134). En otras palabras, la investigación aplicada está estrechamente relacionada, dado que la investigación básica, el último resultado y el progreso son importantes, toda investigación empírica que interesa a los investigadores es el resultado práctico de la fuente.



**Figura 1. Diseño Pre-Experimental**

En esta figura se detalla lo siguiente

- G= Grupo Experimental
- Diagnóstico Inicial: Ataques de Denegación Web al servidor antes de la implementación del Sistema de Seguridad
- Implementación del Sistema de Seguridad

- Diagnostico Final: Ataques de Denegación Web al servidor después de la implementación del Sistema de Seguridad

Hernández y Fernández (2018) muestran que la investigación cuantitativa muestra que el conocimiento debe ser objetivo y es producido por un proceso deductivo que utiliza la inferencia y el análisis estadístico numérico para probar hipótesis formadas previamente. (p.34) En otras palabras utilizar la recopilación de datos para dar un enfoque claro a las preguntas de investigación o mostrar nuevas preguntas durante la interpretación. De acuerdo a la presente investigación se toma en cuenta el tipo de investigación cuantitativa porque intenta determinar la frecuencia de los ataques cibernéticos contra la seguridad del servidor basándose en mediciones numéricas y análisis estadísticos. También es cualitativo porque toma decisiones de valor sobre la seguridad del servidor.

### **3.1.2 Diseño de investigación**

Para la realización del presente proyecto de investigación se optó por un diseño pre experimental. Según Arias (2012) un estudio pre experimental viene a ser un proceso por el cual se expone a un grupo de objetos o individuos a condiciones o tratamientos específicos (variables independientes) para identificar los efectos o respuestas (variables dependientes) que se producen. El diseño pre-experimental permitirá crear intencionalmente circunstancias que comprometan la seguridad de los servidores mencionados en conjunto con la información de estos autores, permitiendo estimar los resultados obtenidos y seleccionar el proceso de aseguramiento más adecuado.

### 3.2 Variables y operacionalización

Para el presente proyecto de investigación tendremos como variable de estudio: “Sistema de seguridad usando Deep Learning “. Del mismo modo, se visualiza la matriz de operacionalización de variables en ANEXO 1.

### 3.3 Población, muestra y muestreo

Según Arias (2016) Definimos la población como “Un conjunto finito o infinito de elementos con características típicas que fortalecen las conclusiones del estudio” es como definimos a la población. Esto está limitado por los problemas y los objetivos de la investigación. Los ataques informáticos serán la población de estudio para la presente investigación.

Para el presente estudio tuvo una población 10,784 ataques de Denegación de servicio web en los últimos 2 meses de recibió la empresa.

Una muestra puede ahorrarle tiempo y dinero. Con una selección adecuada, puede contribuir a la exactitud y exactitud de sus datos. (Rivas 2020). Dada la gran cantidad de ataques informáticos, necesitamos crear una muestra que permita una investigación adecuada.

el objetivo es tener la capacidad de producir resultados que se apliquen a toda la población. Luego se realizó el cálculo apropiado de la muestra utilizando la siguiente fórmula:

$$n = \frac{N * (z^2) * p * q}{(e^2)(N - 1) + (z^2) * p * q}$$

Donde:

n= Tamaño de la muestra

N= Tamaño de la población 100



z= Nivel de Confianza 95%

p= Probabilidad de éxito 0,5%

q= Probabilidad de fracaso 0,5%

e= Error de estimación 5%

Según el autor Arias (2006, p. 83) El muestreo se define como “un proceso en el que se conoce la probabilidad de inclusión de cada elemento en la muestra”

$$n = \frac{10784 * (1.96^2) * 0.5 * 0.5}{(0.05^2)(10784 - 1) + (1.96^2) * 0.5 * 0.5}$$

$$n = \frac{10356.9536}{27.9179}$$

$$n = 371$$

Con respecto a la Muestra Para realizar diferentes verificaciones con respecto a la mitigación de los ataques DDoS que estuvo constituida por 371 ataques que a su vez se dividirán en 4 tiempos

Dichos ataques tendrán una duración de 2 hora con periodos cortos de 30, 60, 90 y 120 minutos ya que se busca comprobar y poder determinar la eficiencia del sistema de seguridad mediante diversos periodos de tiempos efectivos

### 3.4 Técnicas e instrumentos de recolección de datos

Las técnicas que se utilizarán para recopilar datos en este estudio son las siguientes:

**Análisis documental:** Baena (2017) nos menciona este tipo de técnica recopila datos de fuentes alternas como tesis, libros, maestrías, periódicos, revistas, etc., y se utiliza como fuente para recopilar información sobre variables relacionadas a lo indicado.

**Observación:** Arias (2018) nos describe que una técnica consiste en sentir de valla un fenómeno, eventualidad o índole, conseguir documentación y registrarla para su posterior observación.

#### Ficha de observación

Baena (2017) Se refiere que la herramienta para recopilar información de datos es un método tradicional en la que se recopila datos de una investigación. Gracias a su capacidad para manipular y agregar datos fácilmente, se garantiza que los resultados se procesen y analicen. (pág. 107). En el anexo 3 se muestra la ficha de observación de los falsos positivos y falsos negativos.

Para clasificar los datos se tienen en cuenta diferentes intervalos de tiempo incrementales para entender el impacto de los ataques en el servidor. El uso de técnicas de monitoreo y análisis de documentos para recolectar datos, a través de formato físico y digital para realizar análisis de la información y así tener resultados que nos ayuden a probar e identificar la hipótesis.

Torres, Paz y Salazar (2019) comenta que la observación forma parte esencial de cualquier tipo de investigación; Los investigadores confían en él para tener la mayor cantidad de información posible. Es un registro óptico de lo que está sucediendo en un entorno de la vida real, registrando eventos relevantes de acuerdo a un patrón planificado y de acuerdo al problema en estudio. Antes de realizar una observación, el investigador debe identificar las metas que busca lograr, identificar su unidad de observación, las condiciones bajo las cuales está realizando la observación y los comportamientos que necesitan ser registrados nuevamente.

- ✓ Guerrero (2018) Observación científica se define como la observación de un objetivo preciso y específico. El investigador mide lo que quiere observar y por qué realizarlo, por lo que debe estar bien preparado para la observación.
- ✓ Observación Directa: Torres (2015) cuando los investigadores están personalmente expuestos al evento o fenómeno que están tratando de estudiar. Cuando se obtiene la información precisa, el investigador se auto incluye en el equipo, y observa claramente para obtener la información.
- ✓ Observación Experimental: Torres (2015) menciona que es un procedimiento básico de investigación, el cual es planificado, controlado, verificado y controlado para su validez y confiabilidad.
- ✓ Observación de laboratorio: Torres (2015) menciona que es un evento que tiene lugar en lugares predeterminados, con grupos predeterminados de personas.
- ✓ Observación de equipo o de grupo: Torres (2015) menciona que esta es una encuesta realizada por muchos individuos que forman parte de un equipo de trabajo haciendo la misma encuesta.

DIMENSIÓN	INDICADOR	TECNICA	INSTRUMENTO
Detección de ataques	Detección de anomalías	observación	Ficha de observación
Rendimiento	exhaustividad		

Tabla 1 tabla de indicadores

### 3.5 Procedimientos

Arias (2021) Teniendo en cuenta los procedimientos se describen semánticos, lógicos, lingüísticos, estadísticos, etc. de este modo se emplea el significado de la interpretación de los datos obtenidos y las implicancias que se decidirán. Así mismo Los indicadores que utilizaremos a la hora de desarrollar la tesis serán, tasa de error, detección de anomalías y exhaustividad.

Para poder medir la el indicador exhaustividad descrita en este proyecto, vamos a utilizar sus indicadores con sus respectivas formulas

- Matriz de Confusión

Utilizaremos esta matriz para poder calcular los VP, FP, VN, FN

		Predicción	
		Positivos	Negativos
OBSERVACION	Positivos	<i>Verdaderos Positivos (VP)</i>	<i>Falsos Negativos (FN)</i>
	Negativos	<i>Falsos Positivos (FP)</i>	<i>Verdaderos Negativos (VN)</i>

Tabla 2 Matriz de Confusión

Correa (2016) menciona “De acuerdo a estas métricas son verdadero positivo (VP – un ataque identificado de manera correcta), verdadero negativo (VN). tráfico normal correctamente identificado como tráfico normal), falso positivo (FP - tráfico normal

identificado incorrectamente como ataque) y falso negativo (FN - ataque identificado incorrectamente como tráfico normal).” (p.36).

- Precisión

La utilizaremos para poder medir la precisión del Algoritmo

$$Precisión = \frac{VP}{VP + FP}$$

- Recall

Nos indicara la cantidad de muestras correctas encontradas

$$Recall = \frac{VP}{VP + FN}$$

- Exactitud

Nos ayudara a medir el nivel de porcentaje de las muestras que fueron acertadas

$$Exactitud = \frac{VP + VN}{VP + VN + FP + FN}$$

- F-SCORE

Verifica el rendimiento de la precisión y el recall

$$F1 = 2 \cdot \frac{Precisión \cdot Recall}{Precisión + Recall}$$

Según lo definido por el equipo de ataque bajo el desarrollo del proyecto de investigación, hay 3 equipos físicos, incluidos 2 portátiles (laptops) y 1 computadora

de escritorio (PC). Cada computadora portátil es una computadora virtual que ejecuta una máquina virtual. En el caso de un PC, también es una máquina virtual, en este caso funciona con dos máquinas virtuales. Espere tener 4 máquinas virtuales preinstaladas.

1. Establecer un cronograma de actividades y pasos a seguir
2. Establecer un método de control con un Pretest y Postest
3. Para asignar el rol se tuvo en cuenta las características de cada dispositivo físico, en la siguiente tabla se asigna el rol de cada atacante.

<i>Equipo físico</i>	<i>Nombre del equipo virtual</i>	<i>Sistema operativo</i>	<i>Memoria RAM</i>	<i>Maquina virtual</i>	<i>Memoria RAM virtual</i>
PC	Atacante PC	Windows 11	4gb	Virtual box	1 gb
	Atacante PC-2	Windows 11	4gb	VMware	1gb
Laptop	Atacante- WIN10	Windows 11	4gb	VMware	1gb
Laptop 2	Atacante Win10-2	Windows 11	2gb	VMware	1gb

*Tabla 3 Equipos de ataque*

### **3.6 Método de análisis de datos**

En esta sección se detalla los métodos empleados para recopilar los datos

Para clasificar los datos se tienen en cuenta diferentes intervalos de tiempo incrementales para entender el impacto de los ataques en el servidor.

A través de una serie de pruebas u operaciones, Las siguientes acciones se han llevado a cabo con la ayuda de herramientas de software y con la ayuda de otras organizaciones que pueden actuar como "atacadores":

- demostrar con éxito la debilidad del servidor poniéndolo a prueba en escenarios de ataques de denegación de servicio.

- Realizar una segunda serie de ataques previamente monitorizados para la clasificación del ataque DDoS.

Una vez realizadas las comprobaciones finales, compruebe que la unidad está haciendo su labor, registre los errores, identifique las causas, arrégelos y cree acciones preventivas.

#### Unidad de Análisis

Balcells (1994) nos da una definición sobre dicho análisis que contiene (método de investigación) “las unidades de análisis son las partes de los documentos o comunicaciones que forman la base de una investigación”.

Se utiliza un enfoque cuantitativo para el análisis de los datos de la investigación. Primero, se consideran ciertas variables o métricas, como la cantidad de ataques que el módulo de seguridad de la estructura frustró con éxito y la cantidad de ataques que el servidor detectó con éxito. su efectividad depende del porcentaje de ataques reales que pueden detectar sin errores. También es necesario lidiar con los falsos positivos, es decir, la capacidad de distinguir entre usuarios legítimos y no pirateados que tienen acceso.

### **3.7 Aspectos éticos**

La presente investigación a realizar se fundamenta mediante los valores éticos normas, principios, conductas, mediante la resolución y lineamiento establecido por la Universidad Cesar Vallejo. Así mismo los autores mencionados estarán debidamente citados en la investigación y referenciados de acuerdo a la ley N° 822 sobre los derechos del autor. Se usarán fuentes de bases de datos de tesis, artículos, revistas y trabajos de investigación teniendo en cuenta las normas establecidas por la universidad, así mismo para optar grados académicos y títulos profesionales de trabajos de investigación nos basamos a los reglamentos de superintendencia nacional- RENATI



## IV. RESULTADOS

### 4.1. Análisis Descriptivo

Indicador 1: Detección de anomalías

0 = "Servidor no responde"

1 = "Detectado/Anomalía"

Estadísticos descriptivos

	atackPre1	AtackPos
Válidos	371	371
Perdidos	0	0
Media	,06	,95
Mediana	,00	1,00
Mínimo	0	0
Máximo	1	1

Fuente: Elaboración propia SPSS

Con respecto a la detección de anomalías, el valor obtenido antes de la implementación fue 0,06, que representa el 6 %, por otro lado, para el pos test 0,95 que representa el 95%, tal cual como esta demostrado en la tabla

Indicador 2: Exhaustividad

Estadísticos descriptivos

	preexhaustividad	posexhaustividad
Válidos	371	371
Perdidos	0	0
Media	6,47	90,42
Mediana	,00	96,00
Mínimo	0	0
Máximo	100	100

Fuente: Elaboración propia SPSS

Con respecto a la exhaustividad, el valor obtenido antes de la implementación fue 6,47, que representa el 6.47 %, por otro lado, para el pos test 90,42 que representa el 90,42%, tal cual como está demostrado en la tabla

## 4.2. Estadística Inferencial

### 4.2.1 Prueba de normalidad

Para este punto se dio a establecer dos lineamientos para determinar si la distribución de la muestra tomada es una distribución normal o no normal

Hipótesis estadísticas para este punto:

- Ho: "La distribución de la muestra es normal".
- Ha: "La distribución de la muestra es no normal".

Donde:

El grado de significancia es igual a 0.05

Resumiendo, la regla de decisión:

Ho: " $\geq 0.05$ ; Se considera una muestra con una distribución normal". Ha: " $< 0.05$ ; Se considera una muestra con una distribución no normal".

Indicador 1: Detección de anomalías

	Kolmogorov-Smirnov <sup>a</sup>		
	Estadístico	gl	Sig.
atackPre1	,539	371	,000
AtackPos	,540	371	,000

Se detalla en la tabla que el Sig. del pre test es de 0.00 y el post test es 0.0, en lo cual uno o más valores es menor a 0.05, rechazándose así la hipótesis Ho, dando lugar a que los datos presentan distribución no normal

Indicador 2: Exhaustividad

Pruebas de normalidad			
	Kolmogorov-Smirnov <sup>a</sup>		
	Estadístico	gl	Sig.
preexhaustividad	,539	371	,000
posexhaustividad	,373	371	,000

Se detalla en la tabla que el Sig. del pre test es de 0,00 y el post test es 0,0, en donde uno o más valores es menor a 0.05, rechazándose así la hipótesis Ho, dando lugar a que los datos presentan distribución no normal

#### 4.2.2 Prueba de hipótesis.

##### 4.2.2.1. Hipótesis General

El sistema seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web aumentará la Detección de anomalías en la empresa SISTEC.

Nivel de Significancia:

Se considera como nivel de significancia  $\alpha$  0,05 haciendo que el nivel de confianza sea de 95%.

Dado que las distribuciones no normales se tienen en cuenta en todas las medidas, continúe utilizando la prueba de Wilcoxon. la prueba incluye una comparación con el número de categorías de signos positivos bajo ambos requisitos con para rechazar la hipótesis nula y aceptar la hipótesis de investigación, además las muestras relevantes deben cumplir con las condiciones del experimento, esto es antes y después.

#### 4.2.2.2. Hipótesis Específicas

##### Indicador 1: Detección de anomalías

H1: El uso de un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web aumentará la detección de anomalías en la empresa SISTEC.

Hipótesis H10: El uso de un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web no aumentará la detección de anomalías en la empresa SISTEC.

H10: DAa-Dad  $\leq$  0

Hipótesis H1a: El uso de un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web si aumentará la detección de anomalías en la empresa SISTEC.

H1 a: DAa-Dad  $>$  0

En la tabla de resumen resultados de Pre test y Post test del Indicador 1, se detalla que la de detección de anomalías reportadas en el pre test es del 6 %, y post test fue de 95%. Se llega a contestar que existe un alza en la detección de las anomalías del 89%.

Tabla de prueba de rangos de indicador 1

Rangos			
	N	Rango promedio	Suma de rangos
AtackPos - atackPre1	Rangos negativos	0 <sup>a</sup>	,00
	Rangos positivos	327 <sup>b</sup>	164,00
	Empates	44 <sup>c</sup>	
	Total	371	

a. AtackPos < atackPre1

b. AtackPos > atackPre1

c. AtackPos = atackPre1

*Tabla de contraste para el indicador 1*

	AtackPos - atackPre1
Z	-18,083 <sup>b</sup>
Sig. asintót. (bilateral)	,000

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

Tal como se detalla en la tabla, el mérito de Sig. es de 0,000, siendo menor a 0.05, se acepta la hipótesis alternativa, para ello El uso de un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web si aumentará la detección de anomalías en la empresa SISTEC.

Indicador 2: Exhaustividad

H2: El uso de un sistema seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web aumentará la exhaustividad en la empresa SISTEC, 2022.

Hipótesis H2<sub>0</sub>: El uso de un sistema seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web no aumentará la exhaustividad en la empresa SISTEC, 2022.

H2<sub>0</sub>: DAa-Dad  $\leq$  0

Hipótesis H2<sub>a</sub>: El uso de un sistema seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web si aumentará la exhaustividad en la empresa SISTEC, 2022.

H2 a: DAa-Dad > 0

En la tabla de resumen resultados de Pre test y Post test del Indicador 2, se detalla que la exhaustividad reportada en el pre test es del 6.47 %, y post test fue de 90,42%. Se llega a contestar que existe un alza en la exhaustividad del 83,95%.

Rangos			
	N	Rango promedio	Suma de rangos
posexhaustividad - preexhaustividad	Rangos negativos	20 <sup>d</sup>	210,00
	Rangos positivos	327 <sup>e</sup>	60168,00
	Empates	24 <sup>f</sup>	
	Total	371	

d. posexhaustividad < preexhaustividad

e. posexhaustividad > preexhaustividad

f. posexhaustividad = preexhaustividad

Tabla estadístico contraste para el indicador 2

Estadísticos de contraste	
	posexhaustividad - preexhaustividad
Z	-16,056 <sup>b</sup>
Sig. asintót. (bilateral)	,000

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

Tal como se detalla en la tabla, el mérito de Sig. es de 0,000, siendo menor a 0.05, se acepta la hipótesis alternativa, para ello El uso de un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web si aumentará la exhaustividad en la empresa SISTEC.

En este capítulo se describirá los resultados obtenidos de la presente investigación, utilizando los indicadores de Tiempo de respuesta, detección de ataques, Sensibilidad.

### **3.1. Análisis Descriptivo**

Empleando el sistema de seguridad en el servidor web, fue que se obtuvieron mejores resultados al proteger el servidor

Al buscar una solución efectiva a la problemática planteada, se implementó el sistema de seguridad y a su vez se realizaron 371 ataques en 2 horas con el fin de medir la efectividad del sistema

“Dado a que se busca conseguir una clasificación que funcione en tiempo real y pueda detectar y clasificar comportamientos anómalos en el servidor, es necesario poder reducir la complejidad a la que se somete.

### **DISEÑO PRE TEST**

Utilizare un diseño pretest (Sin protección alguna) y se realizaron diversos ataques para medir el rendimiento del servidor ante peticiones masivas

### **ATAQUE AL SERVIDOR EN LOS PRIMEROS 30 MINUTOS**

Se obtuvieron los resultados que se muestran a continuación:

- El resultado antes de implementar el sistema de seguridad al servidor fue el siguiente

**Figura 2:** Registro del ataque con la Herramienta SLOWLORIS

```
bo0ltlixuz@DESKTOP-MD596T8:~/SlowLoris$ python3 SlowLoris.py

SLOWLORIS
~ DOS ATTACK VECTOR ~

The Slow Loris DOS attack works by specifying an IP or domain to attack, then slowly
consuming all available bandwidth by requesting but not closing connections.

John Kearney

**CTRL + C to Quit**
Enter Target IP >> 88.99.30.217
Enter Target Port (80 for websites, vulnerable port for hosts) >> 80
Enter Number of Sockets >> 100000

***** SLOWLORIS *****

You have entered:
Target IP >> 88.99.30.217
Target Port >> 80
```

*Fuente: Elaboración propia*

**Figura 3:** Registro del ataque sin el sistema de seguridad

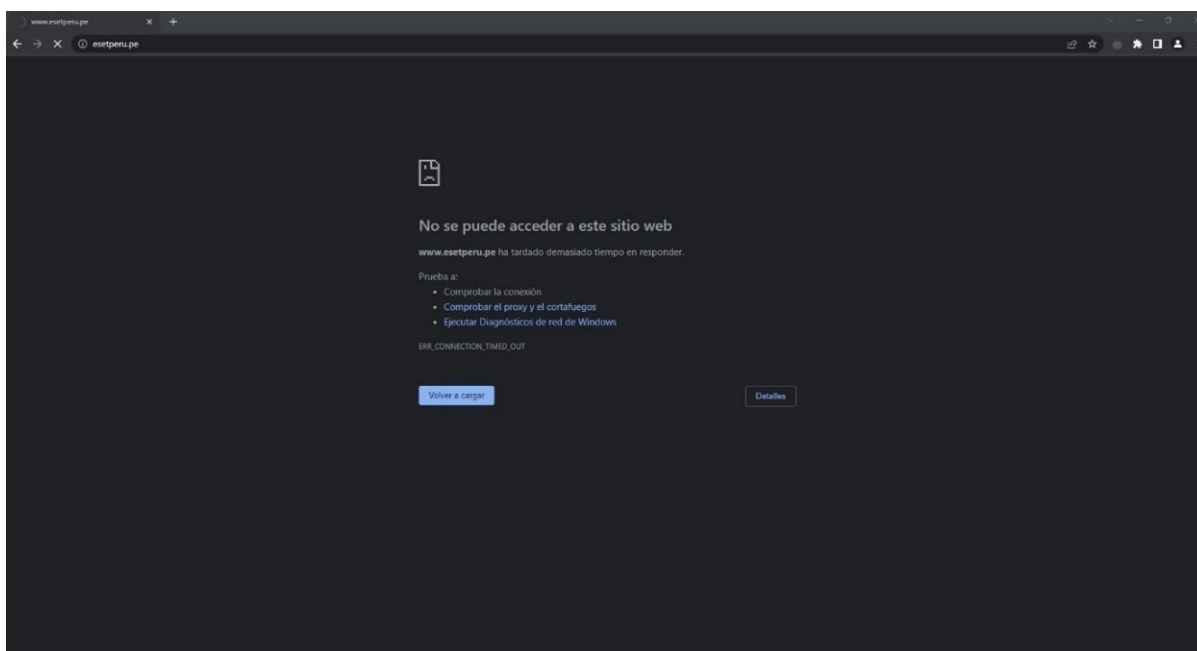
```
Selecionar bo0ltlixuz@DESKTOP-MD596T8: ~/PXE-DOS
:26:01 [378] < ip address 88.99.30.217 > #دوھت_نل_نپٹسلف
:26:01 [379] < ip address 88.99.30.217 > #دوھت_نل_نپٹسلف
:26:01 [380] < ip address 88.99.30.217 > #دوھت_نل_نپٹسلف
:26:01 [381] < ip address 88.99.30.217 > #دوھت_نل_نپٹسلف
:26:01 [382] < ip address 88.99.30.217 > #دوھت_نل_نپٹسلف
:26:01 [383] < ip address 88.99.30.217 > #دوھت_نل_نپٹسلف
:26:01 [384] < ip address 88.99.30.217 > #دوھت_نل_نپٹسلف
:26:01 [385] < ip address 88.99.30.217 > #دوھت_نل_نپٹسلف
:26:01 [386] < ip address 88.99.30.217 > #دوھت_نل_نپٹسلف
:26:01 [387] < ip address 88.99.30.217 > #دوھت_نل_نپٹسلف
:26:01 [388] < ip address 88.99.30.217 > #دوھت_نل_نپٹسلف
:26:01 [389] < ip address 88.99.30.217 > #دوھت_نل_نپٹسلف
```

*Fuente: Elaboración propia*



Podemos observar el momento en el que se efectúa el ataque durante los 30 minutos a la dirección IP del servidor y su puerto. Se logra saturar el servidor con peticiones masivas haciendo que los usuarios no puedan acceder a la página, por tal motivo el servicio no responde a ninguna solicitud.

**Figura 4:** Sin acceso a la página web Durante el ataque DDoS sin el sistema de seguridad



**Fuente:** Elaboración propia

- En la siguiente figura se muestra las IP que efectuaron el ataque y su respectiva fecha, hora, minuto comprobando que el pretest fue realizado de manera correcta obteniendo resultados que se verán reflejados a continuación

**Figura 5: Datos de IP y fecha al momento de hacer el ataque**

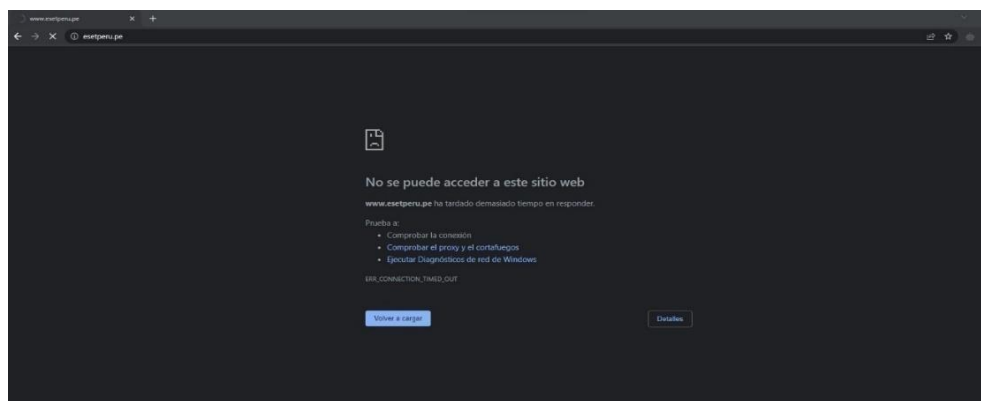
(21,	'194.149.73.237',	'13 Octubre 2022',	'09:02',	('/',index.php',	'',	'Mass Requests',	'Opera 90.
(22,	'203.9.196.199',	'13 Octubre 2022',	'09:03',	('/',index.php',	'',	'Proxy',	'Opera 90.0.4480.10
(23,	'188.47.67.134',	'13 Octubre 2022',	'09:04',	('/',index.php',	'',	'Mass Requests',	'Opera 90.0
(24,	'184.59.98.160',	'13 Octubre 2022',	'09:05',	('/',index.php',	'',	'Mass Requests',	'Opera 90.0
(25,	'16.54.63.132',	'13 Octubre 2022',	'09:06',	('/',index.php',	'',	'Mass Requests',	'Opera 90.0.
(26,	'70.77.94.126',	'13 Octubre 2022',	'09:07',	('/',index.php',	'',	'Mass Requests',	'Opera 90.0.
(27,	'19.178.50.124',	'13 Octubre 2022',	'09:08',	('/',index.php',	'',	'Mass Requests',	'Opera 90.0
(28,	'191.208.5.93',	'13 Octubre 2022',	'09:09',	('/',index.php',	'',	'Mass Requests',	'Opera 90.0.
(29,	'117.165.204.9',	'13 Octubre 2022',	'09:10',	('/',index.php',	'',	'Mass Requests',	'Opera 90.0
(30,	'76.204.217.254',	'13 Octubre 2022',	'09:11',	('/',index.php',	'',	'Mass Requests',	'Opera 90.
(31,	'116.246.169.162',	'13 Octubre 2022',	'09:12',	('/',index.php',	'',	'Mass Requests',	'Opera 90
(32,	'161.147.99.209',	'13 Octubre 2022',	'09:13',	('/',index.php',	'',	'Spammer',	'Opera 90.0.4480
(33,	'13.77.206.187',	'13 Octubre 2022',	'09:14',	('/',index.php',	'',	'Spammer',	'Opera 90.0.4480.
(34,	'134.213.29.211',	'13 Octubre 2022',	'09:15',	('/',index.php',	'',	'Spammer',	'Opera 90.0.4480
(35,	'204.238.251.67',	'13 Octubre 2022',	'09:16',	('/',index.php',	'',	'Spammer',	'Opera 90.0.4480
(36,	'68.166.216.95',	'13 Octubre 2022',	'09:17',	('/',index.php',	'',	'Spammer',	'Opera 90.0.4480.
(37,	'203.97.163.39',	'13 Octubre 2022',	'09:18',	('/',index.php',	'',	'Spammer',	'Opera 90.0.4480.
(38,	'69.145.2.200',	'13 Octubre 2022',	'09:19',	('/',index.php',	'',	'Spammer',	'Opera 90.0.4480.1
(39,	'49.179.106.179',	'13 Octubre 2022',	'09:20',	('/',index.php',	'',	'Spammer',	'Opera 90.0.4480
(40,	'84.189.37.21',	'13 Octubre 2022',	'09:21',	('/',index.php',	'',	'Spammer',	'Opera 90.0.4480.1
(41,	'89.7.210.131',	'13 Octubre 2022',	'09:22',	('/',index.php',	'',	'Spammer',	'Opera 90.0.4480.1
(42,	'93.131.171.125',	'13 Octubre 2022',	'09:23',	('/',index.php',	'',	'Spammer',	'Opera 90.0.4480
(43,	'61.106.133.105',	'13 Octubre 2022',	'09:24',	('/',index.php',	'',	'Spammer',	'Opera 90.0.4480
(44,	'17.189.137.26',	'13 Octubre 2022',	'09:25',	('/',index.php',	'',	'Spammer',	'Opera 90.0.4480
(45,	'155.175.207.180',	'13 Octubre 2022',	'09:26',	('/',index.php',	'',	'Spammer',	'Opera 90.0.448
(46,	'241.11.219.243',	'13 Octubre 2022',	'09:27',	('/',index.php',	'',	'Spammer',	'Opera 90.0.4480

*Fuente: Elaboración propia*

## ATAQUE AL SERVIDOR EN A LOS 60 MINUTOS

Durante el transcurso de los 60 minutos del día 13 de octubre a las 10:00 am el servidor web no daba una respuesta a ninguna petición de los usuarios, por tal motivo es inaccesible.

**Figura 6: Sin acceso a la página web Durante el ataque DDoS de 60 minutos sin el sistema de seguridad**

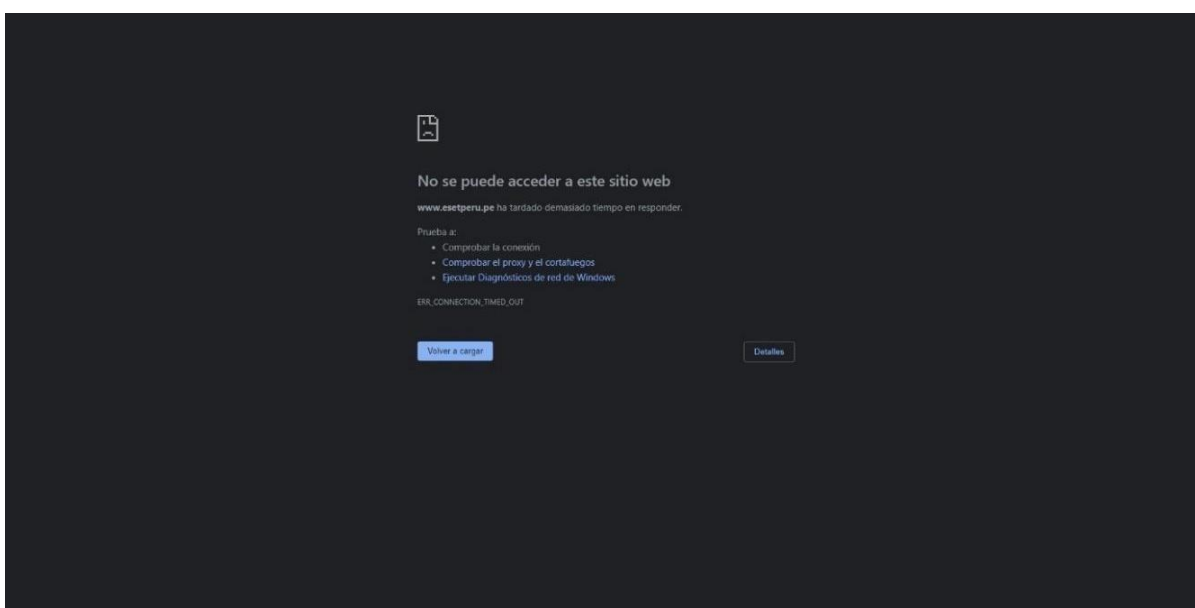


*Fuente: Elaboración propia*

## ATAQUE AL SERVIDOR EN A LOS 90 MINUTOS

Durante el transcurso de los 90 minutos del día 13 de octubre a las 10:30 am el servidor web seguía sin dar una respuesta a ninguna petición de los usuarios, por tal motivo es inaccesible

**Figura 7:** Sin acceso a la página web Durante el ataque DDoS de 90 minutos sin el sistema de seguridad

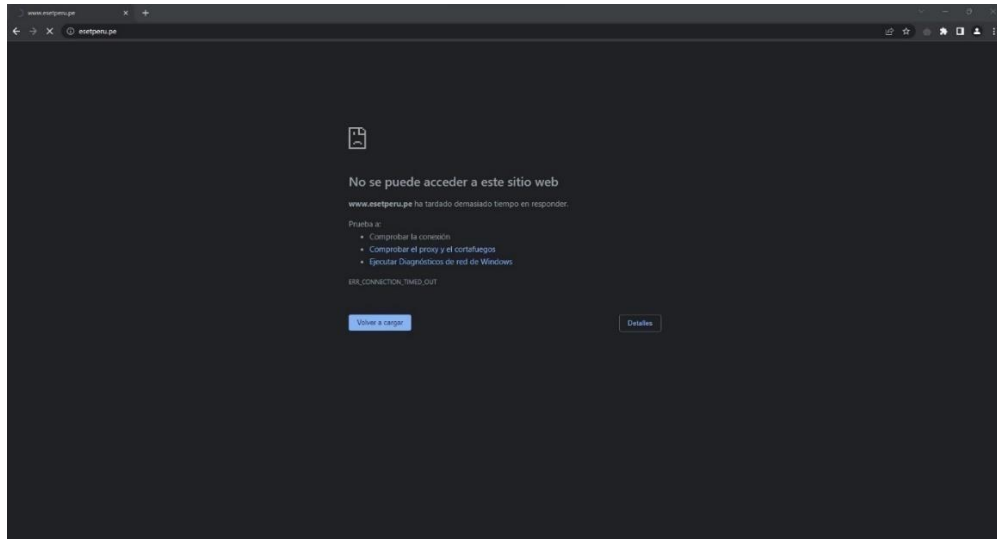


**Fuente:** Elaboración propia

## ATAQUE AL SERVIDOR EN A LOS 120 MINUTOS

Durante el transcurso de los 120 minutos del día 13 de octubre a las 10:59 am el servidor web seguía sin dar una respuesta a ninguna petición de los usuarios, por tal motivo es inaccesible

**Figura 8:** Sin acceso a la página web Durante el ataque DDoS de 120 minutos sin el sistema de seguridad



**Fuente:** Elaboración propia

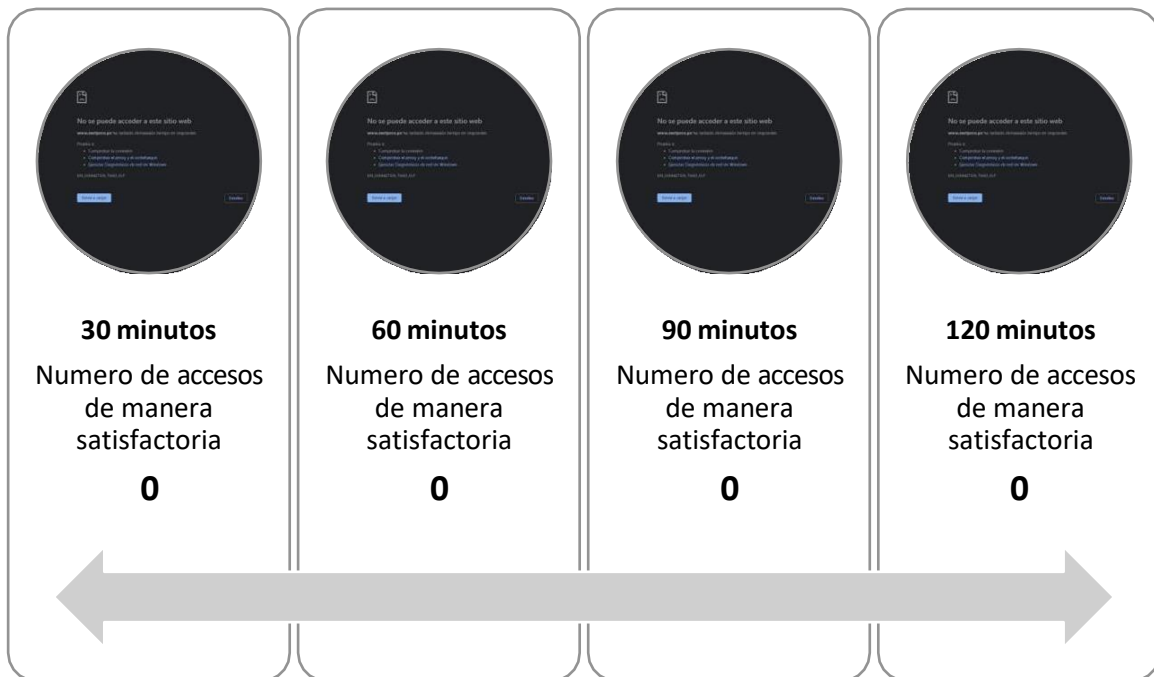
**Figura 9:** Datos de IP y fecha al momento de hacer el ataque

'194.149.73.237'	'13 Octubre 2022'	'11:02'	'/index.php'
'203.9.196.199'	'13 Octubre 2022'	'11:03'	'/index.php'
'188.47.67.134'	'13 Octubre 2022'	'11:04'	'/index.php'
'184.59.98.160'	'13 Octubre 2022'	'11:05'	'/index.php'
'16.54.63.132'	'13 Octubre 2022'	'11:06'	'/index.php'
'70.77.94.126'	'13 Octubre 2022'	'11:07'	'/index.php'
'19.178.50.124'	'13 Octubre 2022'	'11:08'	'/index.php'
'191.208.5.93'	'13 Octubre 2022'	'11:09'	'/index.php'
'117.165.204.9'	'13 Octubre 2022'	'11:10'	'/index.php'
'76.204.217.254'	'13 Octubre 2022'	'11:11'	'/index.php'
'116.246.169.162'	'13 Octubre 2022'	'11:12'	'/index.php'
'161.147.99.209'	'13 Octubre 2022'	'11:13'	'/index.php'
'13.77.206.187'	'13 Octubre 2022'	'11:14'	'/index.php'
'134.213.29.211'	'13 Octubre 2022'	'11:15'	'/index.php'
'204.238.251.67'	'13 Octubre 2022'	'11:16'	'/index.php'
'68.166.216.95'	'13 Octubre 2022'	'11:17'	'/index.php'
'203.97.163.39'	'13 Octubre 2022'	'11:18'	'/index.php'
'69.145.2.200'	'13 Octubre 2022'	'11:19'	'/index.php'
'49.179.106.179'	'13 Octubre 2022'	'11:20'	'/index.php'
'84.189.37.21'	'13 Octubre 2022'	'11:21'	'/index.php'
'89.7.210.131'	'13 Octubre 2022'	'11:22'	'/index.php'
'93.131.171.125'	'13 Octubre 2022'	'11:23'	'/index.php'
'61.106.133.105'	'13 Octubre 2022'	'11:24'	'/index.php'
'17.189.137.26'	'13 Octubre 2022'	'11:25'	'/index.php'
'155.175.207.180'	'13 Octubre 2022'	'11:26'	'/index.php'
'241.11.219.243'	'13 Octubre 2022'	'11:27'	'/index.php'

**Fuente:** Elaboración propia

Para concluir podemos visualizar que durante el envío de los ataques, no se presentan accesos de manera satisfactoria a la web.

**Figura 10:** Número de accesos de manera satisfactoria en cada tiempo del pre-Test



**Fuente:** Elaboración propia

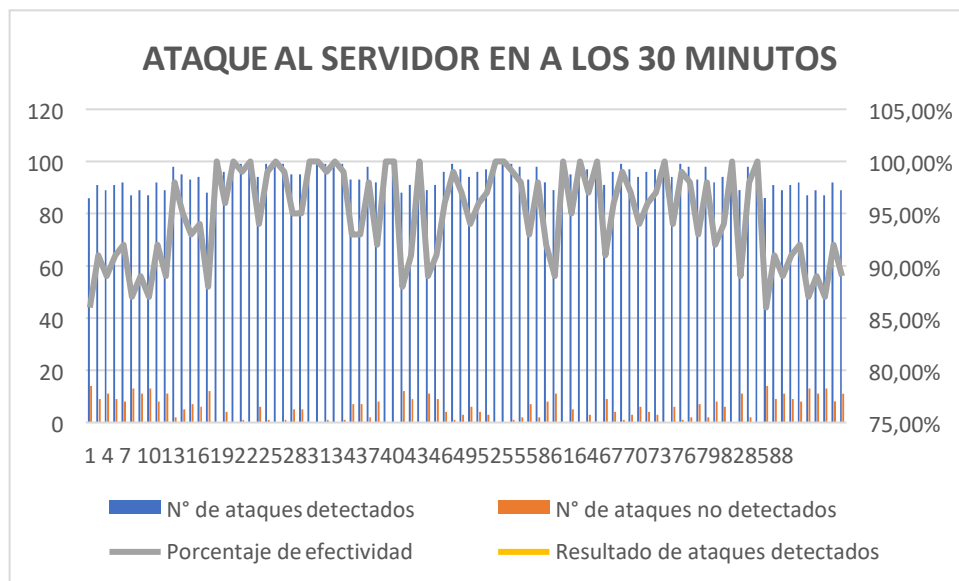
De esta manera podemos concluir que el sitio web no responde a ninguna solicitud enviada por los usuarios en el diseño del pretest, esto puede ser perjudicial si el sitio web no cuenta con un sistema de seguridad que garantice la disponibilidad de la información

## DISEÑO POST TEST

### ATAQUE DE LOS PRIMEROS 30 MINUTOS

A continuación, se visualiza los resultados que se obtuvo en el transcurso de los primeros 30 minutos de ataque

**Figura 11: Ataque Post-test de 30 minutos**



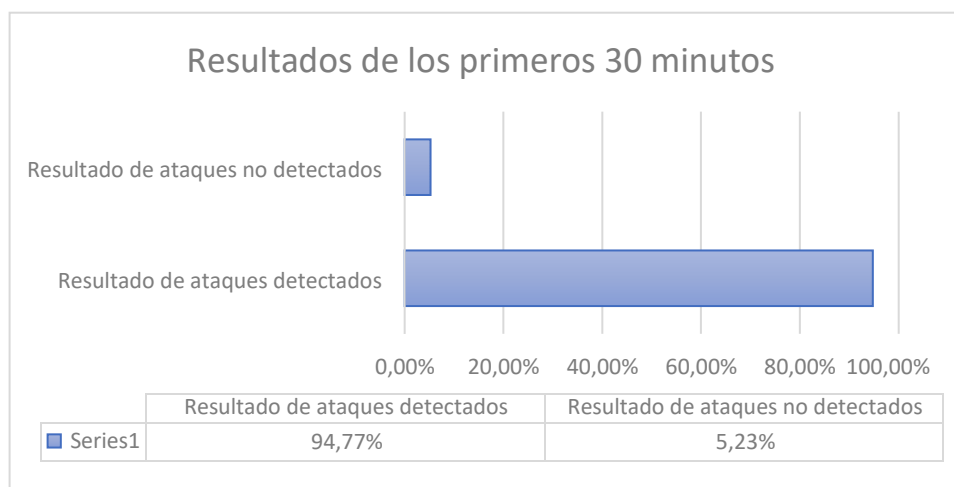
Fuente: Elaboración propia

De acuerdo a los resultados obtenidos en base a los indicadores se tendrá la siguiente interpretación

Durante el proceso de ataques DDoS en los primeros 30 minutos realizados se determinó que el porcentaje de ataques que no fueron identificados por el sistema de seguridad fueron 5.23%, por otra parte, los números de ataques que detecto el sistema de seguridad fue 94.77%.

A continuación, se visualiza los resultados en porcentajes

**Figura 12: Resultado Post-Test Ataque de 30 minutos**



Fuente: Elaboración propia

Visualizando el grafico podemos identificar que la tasa de resultados que fueron detectados en el transcurso de los 30 minutos de ataque fueron positivos dando como interpretación:

El porcentaje es superior al número de ataques no detectados demostrando la efectividad del sistema de seguridad

**Figura 13: Resultado Ataque post test de 30 minutos en el sistema de seguridad**

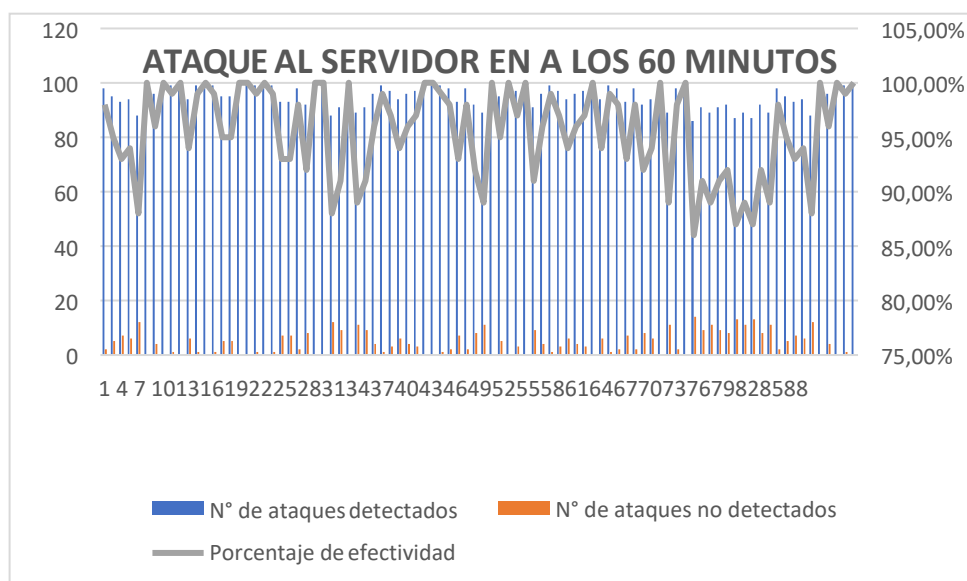
ID	Dirección IP	Acceso/Tipo de trafico	Fecha	País	peticiones	Tipo de Ataque
21	194.149.73.237	Detectado/Anomalia	14 Octubre 2022 a las 09:01	Peru	88	Mass Requests
22	203.9.196.199	Detectado/Anomalia	14 Octubre 2022 a las 09:01	United States	91	Mass Requests
23	188.47.67.134	Detectado/Anomalia	14 Octubre 2022 a las 09:01	United States	89	Mass Requests
24	184.59.98.160	Detectado/Anomalia	14 Octubre 2022 a las 09:01	Peru	91	Mass Requests
25	16.54.63.132	Detectado/Anomalia	14 Octubre 2022 a las 09:02	Peru	92	Mass Requests
26	70.77.94.126	Detectado/Anomalia	14 Octubre 2022 a las 09:02	Peru	87	Mass Requests
27	19.178.50.124	Detectado/Anomalia	14 Octubre 2022 a las 09:02	Peru	89	Mass Requests
28	191.208.5.93	Detectado/Anomalia	14 Octubre 2022 a las 09:02	Peru	87	Mass Requests
29	117.165.204.9	Detectado/Anomalia	14 Octubre 2022 a las 09:03	Peru	92	Mass Requests
30	78.204.217.254	Detectado/Anomalia	14 Octubre 2022 a las 09:03	Peru	89	Mass Requests
31	194.149.73.237	Detectado/Anomalia	14 Octubre 2022 a las 09:03	Peru	96	Mass Requests
32	203.9.196.199	Detectado/Anomalia	14 Octubre 2022 a las 09:03	Peru	95	Spammer
33	188.47.67.134	Detectado/Anomalia	14 Octubre 2022 a las 09:04	Peru	93	Spammer
34	184.59.98.160	Detectado/Anomalia	14 Octubre 2022 a las 09:04	Peru	94	Spammer
35	16.54.63.132	Detectado/Anomalia	14 Octubre 2022 a las 09:04	Peru	88	Spammer
36	70.77.94.126	Detectado/Anomalia	14 Octubre 2022 a las 09:04	Peru	100	Spammer
37	19.178.50.124	Detectado/Anomalia	14 Octubre 2022 a las 09:05	Peru	96	Spammer

Fuente: Elaboración propia

## ATAQUE DE LOS 60 MINUTOS

A continuación, se visualiza los resultados que se obtuvo en el transcurso de los primeros 60 minutos de ataque

**Figura 14: Ataque Post-test de 60 minutos**



Fuente: Elaboración propia

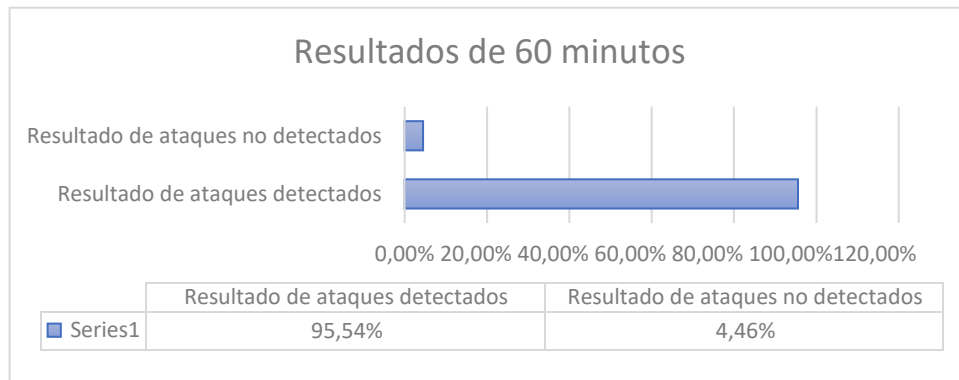
De acuerdo a los resultados obtenidos en base a los indicadores se tendrá la siguiente interpretación

Durante el proceso de ataques DDoS en los primeros 60 minutos realizados se determinó que el porcentaje de ataques que no fueron identificados por el sistema de seguridad fueron 4.46%, por otra parte, los números de ataques que detecto el sistema de seguridad fue 95.54%.

A continuación, se visualiza los resultados en porcentajes



**Figura 15: Resultado Post-Test Ataque de 60 minutos**



Fuente: Elaboración propia

Visualizando el grafico podemos identificar que la tasa de resultados que fueron detectados en el transcurso de los 60 minutos de ataque fueron positivos dando como interpretación:

El porcentaje es superior al número de ataques no detectados demostrando la efectividad del sistema de seguridad

**Figura 16: Resultado Ataque post test de 60 minutos en el sistema de seguridad**

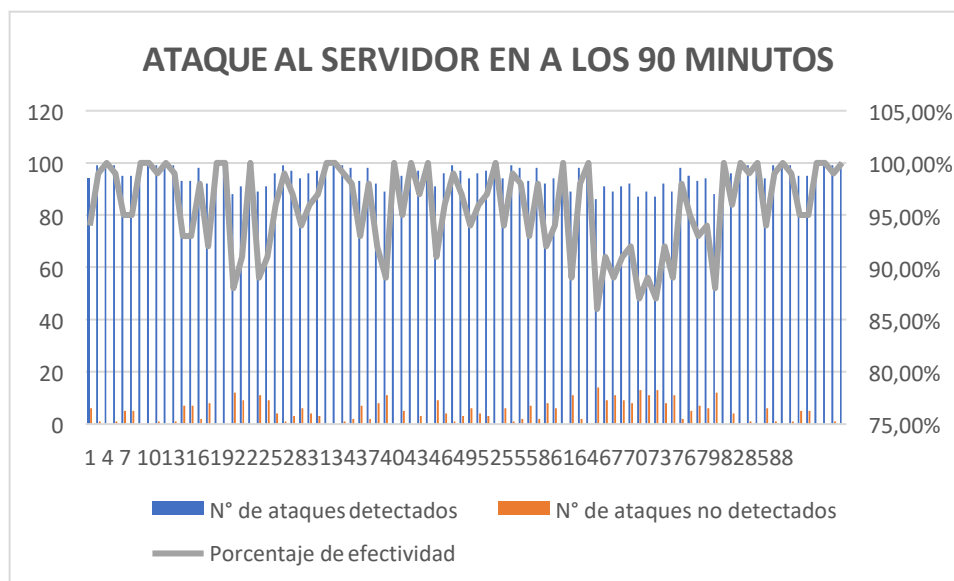
ID	Dirección IP	Acceso/Tipo de trafico	Fecha	País	peticiones	Tipo de Ataque
71	194.149.73.237	Detectado/Anomalía	14 Octubre 2022 a las 09:24	Peru	99	Spammer
72	203.9.196.199	Detectado/Anomalía	14 Octubre 2022 a las 09:25	Peru	96	Spammer
73	188.47.67.134	Detectado/Anomalía	14 Octubre 2022 a las 09:26	Peru	93	Spammer
74	184.59.98.160	Detectado/Anomalía	14 Octubre 2022 a las 09:27	Peru	98	Spammer
75	16.54.63.132	Detectado/Anomalía	14 Octubre 2022 a las 09:28	Peru	92	Spammer
76	70.77.94.126	Detectado/Anomalía	14 Octubre 2022 a las 09:29	Peru	89	Spammer
77	19.178.50.124	Detectado/Anomalía	14 Octubre 2022 a las 09:30	Peru	100	Spammer
78	191.208.5.93	Detectado/Anomalía	14 Octubre 2022 a las 09:31	Peru	95	Spammer
79	117.165.204.9	Detectado/Anomalía	14 Octubre 2022 a las 09:32	Peru	100	Spammer
80	76.204.217.2549	Detectado/Anomalía	14 Octubre 2022 a las 09:33	Peru	97	Spammer
81	194.149.73.237	Detectado/Anomalía	14 Octubre 2022 a las 09:33	Peru	100	Spammer
82	203.9.196.199	Detectado/Anomalía	14 Octubre 2022 a las 09:33	Peru	91	Spammer
83	188.47.67.134	Detectado/Anomalía	14 Octubre 2022 a las 09:33	Peru	96	Spammer
84	184.59.98.160	Detectado/Anomalía	14 Octubre 2022 a las 09:33	Peru	99	Spammer
85	16.54.63.132	Detectado/Anomalía	14 Octubre 2022 a las 09:33	Peru	97	Spammer
86	70.77.94.126	Detectado/Anomalía	14 Octubre 2022 a las 09:33	Peru	94	Spammer
87	19.178.50.124	Detectado/Anomalía	14 Octubre 2022 a las 09:33	Peru	96	Spammer
88	191.208.5.93	Detectado/Anomalía	14 Octubre 2022 a las 09:33	Peru	97	Spammer

Fuente: Elaboración propia

## ATAQUE DE LOS 90 MINUTOS

A continuación, se visualiza los resultados que se obtuvo en el transcurso de los primeros 90 minutos de ataque

**Figura 17: Ataque Post-test de 90 minutos**



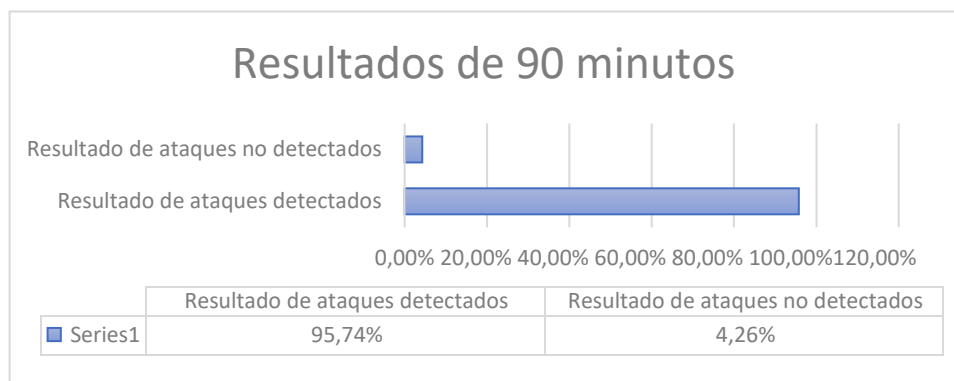
Fuente: Elaboración propia

De acuerdo a los resultados obtenidos en base a los indicadores se tendrá la siguiente interpretación

Durante el proceso de ataques DDoS en los primeros 90 minutos realizados se determinó que el porcentaje de ataques que no fueron identificados por el sistema de seguridad fueron 4.26%, por otra parte, los números de ataques que detecto el sistema de seguridad fue 95.74%.

A continuación, se visualiza los resultados en porcentajes

**Figura 18: Resultado Post-Test Ataque de 90 minutos**



Fuente: Elaboración propia

Visualizando el grafico podemos identificar que la tasa de resultados que fueron detectados en el transcurso de los 90 minutos de ataque fueron positivos dando como interpretación:

El porcentaje es superior al número de ataques no detectados demostrando la efectividad del sistema de seguridad

**Figura 19: Resultado Ataque post test de 90 minutos en el sistema de seguridad**

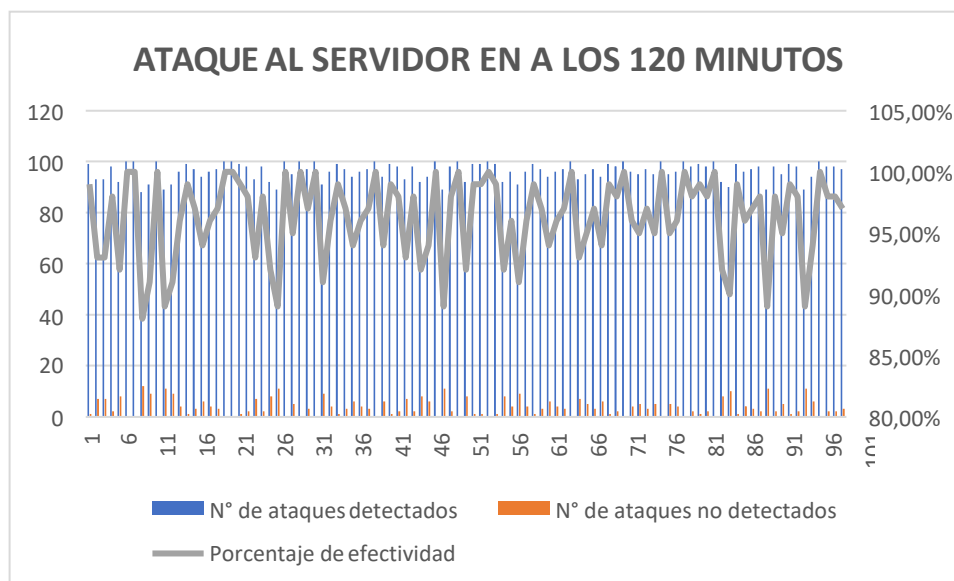
ID	Dirección IP	Acceso/Tipo de trafico	Fecha	País	peticiones	Tipo de Ataque
221	194.149.73.237	Detectado/Anomalía	14 Octubre 2022 a las 10:12	Peru	89	Spammer
222	203.9.196.199	Detectado/Anomalía	14 Octubre 2022 a las 10:12	Peru	91	Spammer
223	188.47.67.134	Detectado/Anomalía	14 Octubre 2022 a las 10:12	Peru	96	Spammer
224	184.59.98.160	Detectado/Anomalía	14 Octubre 2022 a las 10:13	Peru	99	Spammer
225	16.54.63.132	Detectado/Anomalía	14 Octubre 2022 a las 10:13	Peru	97	Spammer
226	70.77.94.126	Detectado/Anomalía	14 Octubre 2022 a las 10:13	Peru	94	Spammer
227	19.178.50.124	Detectado/Anomalía	14 Octubre 2022 a las 10:13	Peru	96	Spammer
228	191.206.5.93	Detectado/Anomalía	14 Octubre 2022 a las 10:13	Peru	97	Spammer
229	117.165.204.9	Detectado/Anomalía	14 Octubre 2022 a las 10:13	Peru	100	Spammer
230	76.204.217.2549	Detectado/Anomalía	14 Octubre 2022 a las 10:14	Peru	100	Spammer
231	194.149.73.237	Detectado/Anomalía	14 Octubre 2022 a las 10:14	Peru	99	Spammer
232	203.9.196.199	Detectado/Anomalía	14 Octubre 2022 a las 10:14	Peru	98	Spammer
233	188.47.67.134	Detectado/Anomalía	14 Octubre 2022 a las 10:14	Peru	93	Spammer
234	184.59.98.160	Detectado/Anomalía	14 Octubre 2022 a las 10:14	Peru	98	Spammer
235	16.54.63.132	Detectado/Anomalía	14 Octubre 2022 a las 10:14	Peru	92	Spammer
236	70.77.94.126	Detectado/Anomalía	14 Octubre 2022 a las 10:14	Peru	89	Spammer
237	19.178.50.124	Detectado/Anomalía	14 Octubre 2022 a las 10:14	Peru	100	Spammer

Fuente: Elaboración propia

## ATAQUE DE LOS 120 MINUTOS

A continuación, se visualiza los resultados que se obtuvo en el transcurso de los primeros 120 minutos de ataque

**Figura 20:** Ataque Post-test de 120 minutos



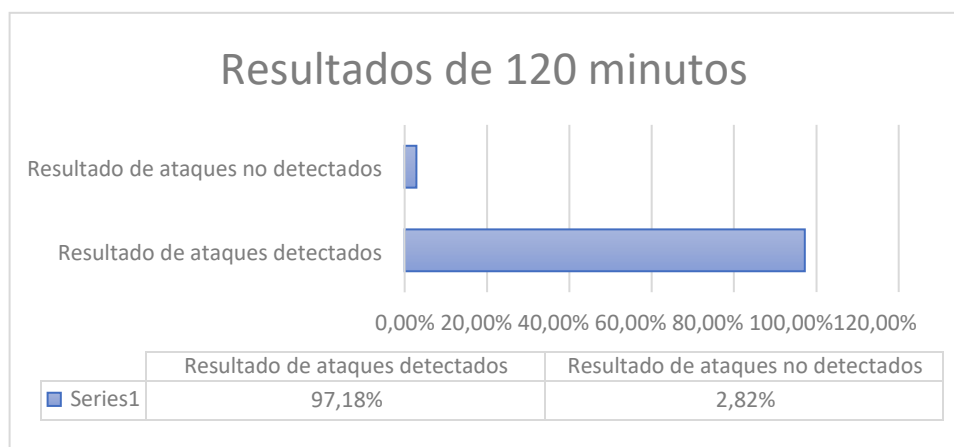
Fuente: Elaboración propia

De acuerdo a los resultados obtenidos en base a los indicadores se tendrá la siguiente interpretación

Durante el proceso de ataques DDoS en los primeros 120 minutos realizados se determinó que el porcentaje de ataques que no fueron identificados por el sistema de seguridad fueron 2.82%, por otra parte, los números de ataques que detecto el sistema de seguridad fue 97.18%.

A continuación, se visualiza los resultados en porcentajes

**Figura 21: Resultado Post-Test Ataque de 120 minutos**



Fuente: Elaboración propia

Visualizando el grafico podemos identificar que la tasa de resultados que fueron detectados en el transcurso de los 120 minutos de ataque fueron positivos dando como interpretación:

El porcentaje es superior al número de ataques no detectados demostrando la efectividad del sistema de seguridad

**Figura 22: Resultado Post-Test Ataque de 120 minutos con el sistema de seguridad**

ID	Dirección IP	Acceso/Tipo de trafico	Fecha	País	peticiones	Tipo de Ataque
321	194.149.73.237	Detectado/Anomalía	14 Octubre 2022 a las 10:41	Peru	100	Spammer
322	203.9.196.199	Detectado/Anomalía	14 Octubre 2022 a las 10:41	Peru	91	Spammer
323	188.47.67.134	Detectado/Anomalía	14 Octubre 2022 a las 10:41	Peru	96	Spammer
324	184.59.98.160	Detectado/Anomalía	14 Octubre 2022 a las 10:41	Peru	99	Spammer
325	16.54.63.132	Detectado/Anomalía	14 Octubre 2022 a las 10:41	Peru	97	Spammer
326	70.77.94.126	Detectado/Anomalía	14 Octubre 2022 a las 10:42	Peru	94	Spammer
327	19.178.50.124	Detectado/Anomalía	14 Octubre 2022 a las 10:43	Peru	96	Spammer
328	191.208.5.93	Detectado/Anomalía	14 Octubre 2022 a las 10:44	Peru	97	Spammer
329	117.165.204.9	Detectado/Anomalía	14 Octubre 2022 a las 10:45	Peru	100	Spammer
330	76.204.217.2549	Detectado/Anomalía	14 Octubre 2022 a las 10:46	Peru	94	Spammer
331	194.149.73.237	Detectado/Anomalía	14 Octubre 2022 a las 10:47	Peru	99	Spammer
332	203.9.196.199	Detectado/Anomalía	14 Octubre 2022 a las 10:47	Peru	98	Spammer
333	188.47.67.134	Detectado/Anomalía	14 Octubre 2022 a las 10:48	Peru	93	Spammer
334	184.59.98.160	Detectado/Anomalía	14 Octubre 2022 a las 10:48	Peru	98	Spammer
335	16.54.63.132	Detectado/Anomalía	14 Octubre 2022 a las 10:49	Peru	92	Spammer
336	70.77.94.126	Detectado/Anomalía	14 Octubre 2022 a las 10:49	Peru	94	Spammer
337	19.178.50.124	Detectado/Anomalía	14 Octubre 2022 a las 10:50	Peru	100	Spammer
338	191.208.5.93	Detectado/Anomalía	14 Octubre 2022 a las 10:50	Peru	89	Spammer

Fuente: Elaboración propia

## I. DISCUSIÓN

Esta presente investigación sintetiza y compara el estudio con varios estudios en la literatura científica actual. Continuaremos describiendo las ventajas y desventajas del método utilizado y detallando aspectos importantes relevantes al contexto en el que se ubica este estudio.

Con respecto al indicador detección de anomalías el resultado del Pre test y Post test del Indicador 1, se detalla que la de detección de anomalías reportadas en el pre test es del 6 %, y post test fue de 95%. Se llega a contestar que existe un alza en la detección de las anomalías del 89%.

Por otra parte, el indicador exhaustividad el resultado de Pre test y Post test del Indicador 2, se detalla que la exhaustividad reportada en el pre test es del 6.47 %, y post test fue de 90,42%. Se llega a contestar que existe un alza en la exhaustividad del 83,95%.

La investigación denota mucho en el nivel de variación que se puede obtener entre ambos escenarios pre y post se puede demostrar la importante diferencia en ambos; Así mismo en la tesis de Linarez (2017) El enfoque de su investigación fue detectar y prevenir ataques DDoS en servidores web mediante la implementación de módulos. Seguridad apache mod\_qos. Se decidió utilizar un diseño de pretest-postest de un grupo porque era el más apropiado para el tipo de estudio.

En la medición se obtuvo que el porcentaje de ataques no detectados era del 0,20 %, lo que a su vez daba el porcentaje de ataques detectados correctamente como 99,80%. Además, se concluye que el porcentaje de tráfico legítimo registrado, el porcentaje de tráfico identificado incorrectamente como ataque fue del 0 %, y el porcentaje de tráfico normal identificado correctamente como tráfico normal fue del 100 %.

## II. CONCLUSIONES

Se concluye que:

1. La detección de anomalías incrementó en un 89% a comparación de antes de implementar el sistema de seguridad, dando a entender que el sistema es eficiente, ya que mejoro la protección del servicio y ayudo a detectar las anomalías
2. La exhaustividad incrementó en un 83,95% a comparación de antes de implementar el sistema de seguridad, dando a entender que el sistema es eficiente, ya que mejoro la protección del servicio y ayudo a incrementar la exhaustividad.
3. De tal motivo se concluye que Sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web en la empresa SISTEC, 2022 influye de manera positiva con respecto a la Detección de ataques

### III. RECOMENDACIONES

- Considerando los buenos resultados del estudio, se recomienda a las futuras empresas planificar e implementar herramientas de seguridad para garantizar integridad y disponibilidad de su negocio.
  
- Se recomienda a los futuros personas que demuestren interés por el trabajo que continúen con este tipo de investigación para encontrar mejores soluciones al problema en cuestión, de modo que los resultados obtenidos puedan ser comparados.



## REFERENCIAS:

- **FEIJÓO Aguilar, Francisco.** *Los ataques informaticos y su incidencia en la seguridad de servidores con sistema operativo linux de entidades de gobierno local. Tesis (Maestría en Gerencia de Sistemas de Información).* Ambato: Universidad Tecnica de Ambato, 2019. 139pp.

Disponible en

[https://repositorio.uta.edu.ec/bitstream/123456789/30474/1/Tesis\\_t1645msi.pdf](https://repositorio.uta.edu.ec/bitstream/123456789/30474/1/Tesis_t1645msi.pdf)

- **ALCÁNTARA Ramirez, Ana.** *Desarrollo de un proceso de seguridad para la prevención de intrusiones en una red privada. Tesis (maestría).* Valle de chalco Solidaridad: Universidad Autónoma del Estado de Mexico, 2017. 92pp.

Disponible en

<http://ri.uaemex.mx/handle/20.500.11799/68050>

- **GARCÍA Cañola, Juan.** *Sistema preventivo contra ataques de denegación de servicio web utilizando Deep Learning. Tesis (Magister en Seguridad Informática).* Medellín: Instituto Tecnológico Metropolitano, 2020. 186pp.

Disponible en

[https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/4674/JuanCanola\\_2021.pdf?sequence=1](https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/4674/JuanCanola_2021.pdf?sequence=1)

- **MACÍAS Gómez, Sebastián.** *Sistema de Detección de Ataques de DDoS Basado en Modelos de Aprendizaje de Máquina para la Arquitectura SDN.*

Tesis (Magíster en Ingeniería de Telecomunicaciones). Medellín: Universidad de Antioquia, 2020. 82pp.

Disponible en

[https://bibliotecadigital.udea.edu.co/bitstream/10495/17420/4/GomezSebastian\\_2020\\_SistemaDeteccionAtaques.pdf](https://bibliotecadigital.udea.edu.co/bitstream/10495/17420/4/GomezSebastian_2020_SistemaDeteccionAtaques.pdf)

- **BUCHELI Guagua, Cynthia** *Algoritmos de seguridad para mitigar riesgos de datos en la nube: un mapeo sistematico. Tesis(Obtención de título de ingeniera de sistemas)*. Guayaquil : Universidad Politecnica Salesiana sede Guayaquil, 2021.

Disponible en

<https://dspace.ups.edu.ec/bitstream/123456789/20319/1/UPS-GT003220.pdf>

- **HERRANZ Andre, LORENZO Borja, RUIS Guillermo.** *Adaptacion y calibrado de algoritmos de predicción para la identificación de ataquesDDoS en redes de quinta generación. Tesis (Obtención de título de ingeniero de sistemas)*. Madrid: Universidad Complutense de Madrid, 2018. 129pp

Disponible en

<https://eprints.ucm.es/id/eprint/56245/1/003.pdf>

- **LIZARES Paul, LOPEZ Marco.** *Prevención y deteccion de ataques de denegación de servicio distribuido(DDoS) implementando el modulo QOS en el servidor web apache. Tesis (Obtención de título de ingeniero de sistemas)*. Lambayeque: Universidad Nacional Pedro Ruiz Gallo, 2017. 133pp.

Disponible en

[https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/10160/Lizares\\_Figuroa\\_y\\_López\\_Benavides.pdf?sequence=1&isAllowed=y](https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/10160/Lizares_Figuroa_y_López_Benavides.pdf?sequence=1&isAllowed=y)

- BAENA, Gera. Metodología de la Investigación, serie integral por competencias. México: Grupo Editorial Patria, 2017.
- TORRES, M. La investigación científica: cómo abordarla. México: Universidad Autónoma de Chihuahua, 1992.
- ARIAS, F. El proyecto de investigación, introducción a la metodología científica. Venezuela: Editorial Episteme, 2018.
- DE LA HOZ CORREA, E. Mapas auto-organizativos probabilísticos y análisis en componentes de conexiones para la detección de anomalías en redes de computadores (Tesis Doctoral). España: Universidad de Granada, 2016.
- HOYOS, M. Prototipo de detección de ataques distribuidos de denegación de servicios (DDOS) a partir de máquinas de aprendizaje (Tesis de Maestría). Colombia: Universidad Autónoma de Manizales, 2015.
- Álvarez, J. Modelo comparativo de plataformas Cloud y Evaluación de Microsoft Azure, Google App Engine y Amazon EC2. Valencia, España: Universidad Politécnica de València, 2018.
- **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. En ICEEG 2017: Proceedings of the 2017 International Conference on E-commerce, E-Business and E-Government (pp. 51-55).
- Balobaid, A., Alawad, W., & Aljasim, H. (2016). A study on the impacts of DoS and DDoS attacks on cloud and mitigation techniques. En 2016 International Conference on Computing, Analytics and Security Trends (CAST) (pp. 416-421).
- Bances Carlos, I. (2019). Revisión bibliográfica de técnicas de Deep learning para la detección de ataques distribuidos de denegación de servicios. Tesis de pregrado, Universidad Señor de Sipán, Pimentel.

- 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.
- 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.

- Cegarra, J. (2013). Metodología de la investigación científica y tecnológica. Barcelona: Diaz de Santos.
- Centro Criptológico Nacional de España. (2020). Ciber Amenazas 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/fasel/tesis/tecnicas1.pdf>
- Condor Untiveros, J., & Segura Ydiáquez, J. (2017). 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: Universidad Peruana de Ciencias Aplicadas.
- Conti, M., Somani, G., & Dargahi, T. (2018). Versatile Cybersecurity. Engelska: Springer.
- Costas, J. (2014). Seguridad y Alta Dispon

Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Escala de medición
Prevención de ataques	<p>Fitni y Ramli (2020)</p> <p>La prevención de ataques consta que unas buenas políticas de dispositivos perimetrales (firewalls), antivirus, sistemas de detección de intrusos combinados con una buena formación del personal son el arma perfecta para reducir el riesgo de incidentes maliciosos.</p>	<p>Para poder medir la variable usamos los instrumentos mecánicos o electrónicos y los de Observación, como instrumentos de recolección de datos. Para medir las variables identificadas vamos a utilizar los indicadores con sus respectivas fórmulas matemáticas</p> <p>(Hernández. S, 2013)</p>	<p>Detección de ataques DDoS</p> <p>Liyang L, Zhou J y Xiao N (2007)</p>	<p>Detección de anomalías</p> $H = - \sum_{i=1}^n p_i \log_2 p_i$ <p>Pi= Probabilidad de IP distinta n = Número total de paquetes H= entropía</p> <p>Liyang L, Zhou J y Xiao N (2007)</p>	ORDINAL
			<p>Rendimiento (Martinez (2020))</p>	<p>Exhaustividad</p> $= \frac{VP}{VP + FN}$ <p>VP=Verdaderos Positivos FN= Falsos Negativos Martinez (2020)</p>	

**Anexo 1: Matriz de operacionalización de variable**

## ANEXO 2: MATRIZ DE CONSISTENCIA

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES	METODOLOGÍA
Problema general	Objetivo general	Hipótesis General	<u>VARIABLE DEPENDIENTE</u>	ENFOQUE: Cuantitativo
¿De qué manera influye un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web en la empresa Sistec?	determinar de qué manera influye un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web en la empresa Sistec	el uso de un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web mejorara la seguridad de la empresa SISTEC, 2022	Prevenición de ataques	TIPO DE INVESTIGACIÓN:
			Indicadores Detección de anomalías $H = - \sum_{i=1}^n p_i \log_2 p_i$ Pi= Probabilidad de IP distinta n = Número total de paquetes H= entropía Liying L, Zhou J y Xiao N (2007)	Según la intervención: *Experimental Según la planificación: *Retrospectivo Según se mide: Longitudinal Según Variables de interés: Analítico NIVEL: Explicativo DISEÑO: pre Experimental
<b>Problemas específicos</b>	<b>Objetivos específicos</b>	<b>Hipótesis específicas</b>	<b><u>VARIABLE INDEPENDIENTE:</u></b>	<b>POBLACION Y MUESTRA</b>
PE1: ¿De qué manera influye un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web en la empresa Sistec en base a la Detección de anomalías?  PE2: ¿De qué manera influye un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web en la empresa Sistec en base a la exhaustividad?	OE1: Determinar de qué manera influye un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web en la empresa Sistec en base a la Detección de anomalías.  OE2: Determinar de qué manera influye un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web en la empresa Sistec en base a la exhaustividad.	H1: El uso de un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web aumentará la detección de anomalías en la empresa SISTEC  H2: El uso de un sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web aumentará la exhaustividad en la empresa SISTEC, 2022		Para el presente estudio tuvo una población 10,784 ataques de Denegación de servicio web en los últimos 2 meses de recibió la empresa. La finalidad de poder obtener resultados que puedan ser prolongados hacia toda la población. A continuación, se utilizó la siguiente fórmula para el respectivo cálculo de la muestra:  $n = \frac{N * (z^2) * p * q}{(e^2)(N - 1) + (z^2) * p * q}$ Donde: n= Tamaño de la muestra N= Tamaño de la población 100 z= Nivel de Confianza 95% p= Probabilidad de éxito 0,5% <del>q= Probabilidad de fracaso 0,5%</del> e= Error de estimación 5% $n = \frac{10784 * (1.96)^2 * 0.5 * 0.5}{(0.05^2)(10784 - 1) + (1.96^2) * 0.5 * 0.5}$ $n = \frac{10356.9536}{27.9179}$ $n = 371$ Con respecto a la Muestra Para realizar diferentes verificaciones con respecto a la mitigación de los ataques DDoS que estuvo constituida por 371 ataques que a su vez se dividirán en 4 tiempos  Dichos ataques tendrán una duración de 2 hora con periodos cortos de 30,60,90 y 120 minutos esto con la finalidad de poder comprobar y determinar la efectividad de sistema de seguridad mediante diversos periodos de tiempos efectivos



## ANEXO 3 FICHA DE OBSERVACIÓN

		Indicador: PERIODO DE TIEMPO			Indicador: Consumo de recursos			Indicador: Detección de ataques		
N° de ataques	fecha	Inicio de ataque	seguimiento	duración del ataque	IP del servidor	IP del atacante	Acceso/Tipo de trafico	N° de ataques detectados	N° de ataques no detectados	Porcentaje de efectividad
1	14-oct-22	09:00:00 a. m.	09:10:00 a. m.	00:30	88.99.30.217	194.149.73.237	Detectado/Anomalía	86	14	86.00%
2	14-oct-22			00:30	88.99.30.217	203.9.196.199	Detectado/Anomalía	91	9	91.00%
3	14-oct-22			00:30	88.99.30.217	188.47.67.134	Detectado/Anomalía	89	11	89.00%
4	14-oct-22			00:30	88.99.30.217	184.59.98.160	Detectado/Anomalía	91	9	91.00%
5	14-oct-22			00:30	88.99.30.217	16.54.63.132	Detectado/Anomalía	92	8	92.00%
6	14-oct-22			00:30	88.99.30.217	70.77.94.126	Detectado/Anomalía	87	13	87.00%
7	14-oct-22			00:30	88.99.30.217	19.178.50.124	Detectado/Anomalía	89	11	89.00%
8	14-oct-22			00:30	88.99.30.217	191.208.5.93	Detectado/Anomalía	87	13	87.00%
9	14-oct-22			00:30	88.99.30.217	117.165.204.9	Detectado/Anomalía	92	8	92.00%
10	14-oct-22			00:30	88.99.30.217	76.204.217.254	Detectado/Anomalía	89	11	89.00%
11	14-oct-22			00:30	88.99.30.217	194.149.73.237	Detectado/Anomalía	98	2	98.00%
12	14-oct-22			00:30	88.99.30.217	203.9.196.199	Detectado/Anomalía	95	5	95.00%
13	14-oct-22			00:30	88.99.30.217	188.47.67.134	Detectado/Anomalía	93	7	93.00%
14	14-oct-22			00:30	88.99.30.217	184.59.98.160	Detectado/Anomalía	94	6	94.00%
15	14-oct-22			00:30	88.99.30.217	16.54.63.132	Detectado/Anomalía	88	12	88.00%
16	14-oct-22			00:30	88.99.30.217	70.77.94.126	Detectado/Anomalía	100	0	100.00%
17	14-oct-22			00:30	88.99.30.217	19.178.50.124	Detectado/Anomalía	96	4	96.00%
18	14-oct-22			00:30	88.99.30.217	191.208.5.93	Detectado/Anomalía	100	0	100.00%
19	14-oct-22			00:30	88.99.30.217	117.165.204.9	Detectado/Anomalía	99	1	99.00%
20	14-oct-22			00:30	88.99.30.217	76.204.217.254	Detectado/Anomalía	100	0	100.00%
21	14-oct-22			00:30	88.99.30.217	194.149.73.237	Detectado/Anomalía	94	6	94.00%
22	14-oct-22			00:30	88.99.30.217	203.9.196.199	Detectado/Anomalía	99	1	99.00%
23	14-oct-22			00:30	88.99.30.217	188.47.67.134	Detectado/Anomalía	100	0	100.00%
24	14-oct-22			00:30	88.99.30.217	184.59.98.160	Detectado/Anomalía	99	1	99.00%
25	14-oct-22			00:30	88.99.30.217	16.54.63.132	Detectado/Anomalía	95	5	95.00%
26	14-oct-22			00:30	88.99.30.217	70.77.94.126	Detectado/Anomalía	95	5	95.00%
27	14-oct-22			00:30	88.99.30.217	19.178.50.124	Detectado/Anomalía	100	0	100.00%
28	14-oct-22			00:30	88.99.30.217	191.208.5.93	Detectado/Anomalía	100	0	100.00%
29	14-oct-22			00:30	88.99.30.217	117.165.204.9	Detectado/Anomalía	99	1	99.00%
30	14-oct-22			00:30	88.99.30.217	76.204.217.254	Detectado/Anomalía	100	0	100.00%

## Anexo 4: Arquitectura tecnológica para el usuario final

En la figura se visualiza como está constituida la arquitectura tecnológica para el usuario final es decir se muestra el resultado final desde la capa de ingreso al sistema, la conexión con la base de datos y los procesos que tiene que realizar el administrador para activar los módulos de seguridad



Figura 23. Arquitectura tecnológica para el usuario final

## Anexo 5: Arquitectura tecnológica para el desarrollo del Sistema

En la siguiente figura se muestra como está construida la arquitectura tecnológica para el desarrollo del sistema, desde el desarrollador, las plataformas utilizadas, la conexión y la base de datos

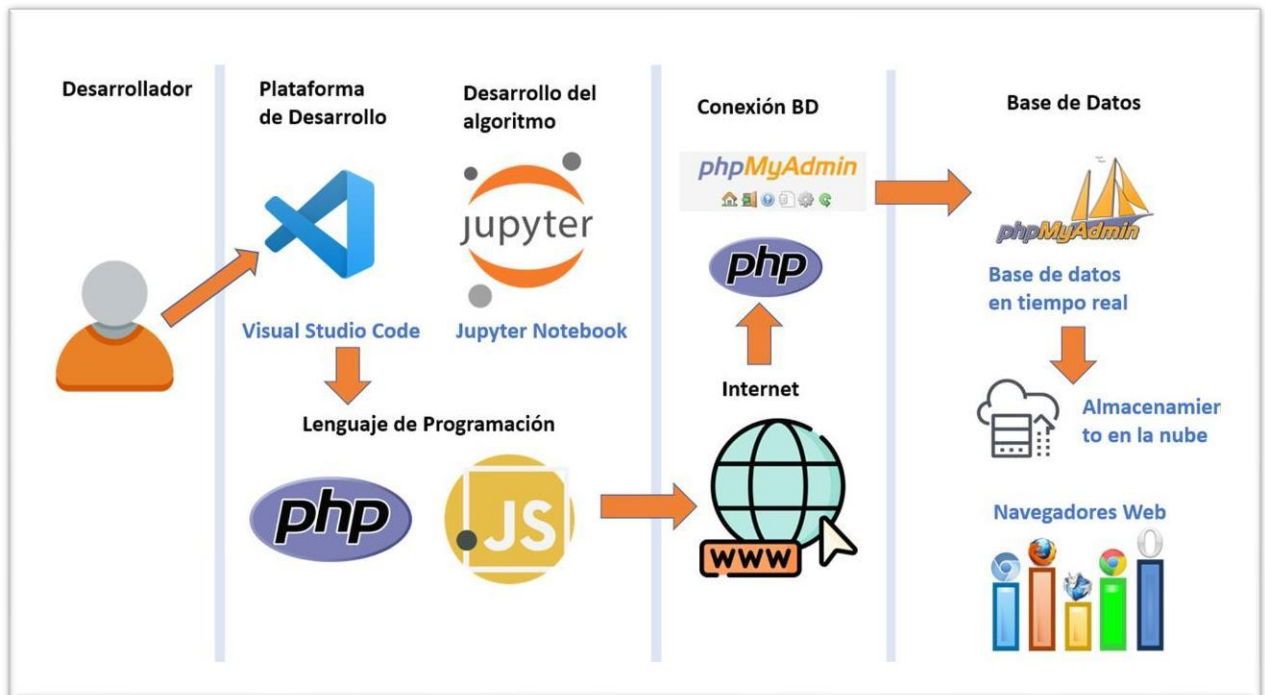


Figura 24. Arquitectura tecnológica para el desarrollo del Sistema

## Anexo 6: METODOLOGÍA DE DESARROLLO

Se realizo planes de trabajo bajo la metodología XP y se dividió en fases

### FASE I: PLANIFICACIÓN

Para esta fase denominada Planificación del Proyecto se utilizará Historias de Usuario, ya que estas permiten definir los requerimientos necesarios para el desarrollo del Sistema de Seguridad.

Historia de Usuario	
Código: H1	Usuario: Usuario final
Nombre historia: Login	
Prioridad en negocio: alta	Riesgo en desarrollo: alto
Puntos estimados: 2	Iteración asignada: 1
Programador responsable: Willians Rivera	
Descripción: Una vez el usuario ingrese al módulo de seguridad se visualizará el formulario Login	
Observaciones: El usuario deberá ingresar su usuario y contraseña posteriormente será validado por el sistema	

*Tabla 10: Historia de usuario Login*

<b>Historia de Usuario</b>	
Código: H2	Usuario: Usuario final
Nombre historia: Dashboard	
Prioridad en negocio: medio	Riesgo en desarrollo: medio
Puntos estimados: 3	Iteración asignada: 2
Programador responsable: Willians Rivera	
Descripción: El dashboard debe mostrar un resumen de la información registrada en el sistema	
Observaciones: El usuario puede previsualizar la información proveniente del dashboard	

*Tabla 11: Historia de usuario Dashboard*

<b>Historia de Usuario</b>	
Código: H3	Usuario: Usuario final
Nombre historia: Modulo de Mitigación DDoS	
Prioridad en negocio: Alta	Riesgo en desarrollo: Alto
Puntos estimados: 3	Iteración asignada: 3
Programador responsable: Willians Rivera	
Descripción: El módulo debe mostrar diferentes opciones donde el usuario puede activar o desactivar la protección contra ataques	

*Tabla 12: Historia de usuario Modulo de Mitigación DDoS*

<b>Historia de Usuario</b>	
Código: H4	Usuario: Usuario final
Nombre historia: Modulo protección contra spam	
Prioridad en negocio: Media	Riesgo en desarrollo: Medio
Puntos estimados: 2	Iteración asignada: 4
Programador responsable: Willians Rivera	
Descripción: El módulo debe mostrar diferentes opciones donde el usuario puede activar o desactivar la protección contra ataques de spam	

*Tabla 13: Historia de usuario Modulo protección contra spam*

<b>Historia de Usuario</b>	
Código: H5	Usuario: Usuario final
Nombre historia: Modulo protección contra bots	
Prioridad en negocio: Media	Riesgo en desarrollo: Medio
Puntos estimados: 2	Iteración asignada: 5
Programador responsable: Willians Rivera	
Descripción: El módulo debe mostrar diferentes opciones donde el usuario puede activar o desactivar la protección contra ataques de bots	

*Tabla 14: Historia de usuario Modulo protección contra bots*

<b>Historia de Usuario</b>	
Código: H6	Usuario: Usuario final
Nombre historia: Modulo de clasificación de ataques	
Prioridad en negocio: Media	Riesgo en desarrollo: Medio
Puntos estimados: 2	Iteración asignada: 6
Programador responsable: Willians Rivera	
Descripción: El módulo debe mostrar una lista de ataques capturados por el sistema y clasificarlos de acuerdo a su resultado	

*Tabla 15: Historia de usuario Modulo de clasificación de ataques*

<b>Historia de Usuario</b>	
Código: H7	Usuario: Usuario final
Nombre historia: Modulo de banear IP	
Prioridad en negocio: Media	Riesgo en desarrollo: Medio
Puntos estimados: 2	Iteración asignada: 7
Programador responsable: Willians Rivera	
Descripción: El módulo debe mostrar un apartado para banear ip manualmente y mostrar una lista de ip baneadas por el sistema.	

*Tabla 16: Historia de usuario Modulo de banear IP*

<b>Historia de Usuario</b>	
Código: H8	Usuario: Desarrollador
Nombre historia: Entrenamiento del algoritmo de detección	
Prioridad en negocio: Muy alta	Riesgo en desarrollo: Alto
Puntos estimados: 4	Iteración asignada: 8
Programador responsable: Willians Rivera	
Descripción: algoritmo de detección obligatoriamente debe ser entrenado con parámetros que identifiquen cuando una ip realiza una sobrecarga de paquetes al servidor.	
Observaciones: algoritmo de detección clasificara con falsos positivos, falsos negativos, verdaderos positivos y verdaderos negativos	

*Tabla 17: Historia de usuario Entrenamiento del algoritmo de detección*



## FASE II: DISEÑO

Para la realización de diseño del software, La metodología XP da como recomendación el uso de tarjetas CRC, a su vez estas permiten tener un diseño orientado a objetos de tal manera que da una representación clara de cada funcionalidad

### Tarjetas CRC

- Login

Modulo Login	
Responsabilidad	Colaboradores
Mostrar el formulario con las cajas de texto para el usuario y contraseña	Integración con el sistema
Observaciones: ninguna	

*Tabla 18: Tarjetas CRC Login*

- Dashboard

Modulo Dashboard	
Responsabilidad	Colaboradores
Visualizar parámetros que brinden información de manera resumida	Integración con el sistema
Observaciones: ninguna	

*Tabla 19: Tarjetas CRC Dashboard*

- Módulo de Mitigación DDoS

<b>Módulo de Mitigación DDoS</b>	
<b>Responsabilidad</b>	<b>Colaboradores</b>
Visualizar parámetros que permitan activar y desactivar la protección, flood.	Integración con el sistema
Observaciones: ninguna	

*Tabla 20: Tarjetas CRC Módulo de Mitigación DDoS*

- Módulo de Protección contra Spam

<b>Modulo protección contra spam</b>	
<b>Responsabilidad</b>	<b>Colaboradores</b>
Visualizar parámetros que permitan activar y desactivar la protección Spam	Integración con el sistema
Observaciones: ninguna	

*Tabla 21: Tarjetas CRC Módulo de Protección contra Spam*

- Módulo de protección contra Bots

<b>Modulo protección contra bot</b>	
<b>Responsabilidad</b>	<b>Colaboradores</b>
Visualizar parámetros que permitan activar y desactivar la protección contra bots	Integración con el sistema
Observaciones: ninguna	

*Tabla 22: Tarjetas CRC Módulo de Protección contra Bots*

- Módulo de clasificación de ataques

<b>Módulo de clasificación de ataques</b>	
<b>Responsabilidad</b>	<b>Colaboradores</b>
Visualizar una lista donde se muestren los ataques detectados por el sistema	Integración con el sistema
Observaciones: ninguna	

*Tabla 23: Tarjetas CRC Módulo de clasificación de ataques*

- Módulo de Banear IP

<b>Módulo de banear IP</b>	
<b>Responsabilidad</b>	<b>Colaboradores</b>
Visualizar un apartado para banear ip manualmente y mostrar una lista de ips baneadas por el sistema	Integración con el sistema
Observaciones: ninguna	

*Tabla 24: Tarjetas CRC Módulo de Banear IP*

- Entrenamiento de algoritmo de detección

<b>Entrenamiento de algoritmo de detección</b>	
<b>Responsabilidad</b>	<b>Colaboradores</b>
Obtener ip y evaluar mediante interacciones encontradas y retornar una respuesta	Entrenamiento de algoritmo de detección
Observaciones: ninguna	

*Tabla 25: Tarjetas CRC Entrenamiento de algoritmo de detección*

## Backend

El sistema de seguridad está desarrollado con la tecnología PHP, JavaScript, MySQL, bajo el uso de varias tecnologías actuales, además se utilizó herramientas como jupyter Notebook para el desarrollo del algoritmo

```
function getFromfile_source($type){
    $sad_check_file = 'check.txt';//
    $sad_all_file = 'all_ip.txt';//
    $sad_black_file = 'black_ip.txt';//
    $sad_white_file = 'white_ip.txt';//
    $sad_temp_file = 'ad_temp_file.txt';//
    $sad_dir = 'anti_ddos/files';//

    return ($type == "black") ? explode(',', implode(',',file("{$sad_dir}/{$sad_black_file}"))) : ( ($type == "white")
}

$sad_ip = "";
// if you'r working on your local machine, you can add these conditions
//and getenv(" HTTP_CLIENT_IP ") != '127.0.0.1'
//and getenv(" HTTP_X_FORWARDED_FOR") != '127.0.0.1'

$sad_ip = (getenv("HTTP_CLIENT_IP") and preg_match("/^\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}$/", getenv(" HTTP_CLIENT_IP

$sad_source = getFromfile_source('black');
if(in_array($sad_ip, $sad_source)) {die();}

$sad_source = getFromfile_source('white');
if(!in_array($sad_ip, $sad_source)) {

    $sad_source = getFromfile_source('temp');
    if(!in_array($sad_ip, $sad_source)) {
        $_SESSION['nbre_essai']=3;
        $sad_file = fopen("{$sad_dir}/{$sad_temp_file}", "a+");
        $sad_string = $sad_ip.',';
        fputs($sad_file, "$sad_string");
        fclose($sad_file);
        $array_for_nom = array('maN' 'hZ' 'E' 'S' 'i' 'D' 'u' '4' '4' 'Dc' 'En' 'EFGv' 'A' 'd' '98' '74cM');
```

Figura 25: Código del sistema de protección

```
// verificar ip repetidas por el servidor
$config_status .= (file_exists("{$sad_dir}/{$sad_check_file}") ? Create_File("{$sad_dir}/{$sad_check_file}") : "ERROR: Creating " . "{$sad_dir}/{$sad_check_file}<br>";
$config_status .= (file_exists("{$sad_dir}/{$sad_temp_file}") ? Create_File("{$sad_dir}/{$sad_temp_file}") : "ERROR: Creating " . "{$sad_dir}/{$sad_temp_file}<br>";
$config_status .= (file_exists("{$sad_dir}/{$sad_black_file}") ? Create_File("{$sad_dir}/{$sad_black_file}") : "ERROR: Creating " . "{$sad_dir}/{$sad_black_file}<br>";
$config_status .= (file_exists("{$sad_dir}/{$sad_white_file}") ? Create_File("{$sad_dir}/{$sad_white_file}") : "ERROR: Creating " . "{$sad_dir}/{$sad_white_file}<br>";
$config_status .= (file_exists("{$sad_dir}/{$sad_all_file}") ? Create_File("{$sad_dir}/{$sad_all_file}") : "ERROR: Creating " . "{$sad_dir}/{$sad_all_file}<br>";

if(!file_exists ("{$sad_dir}/../anti_ddos.php")){
    $config_status .= "anti_ddos.php does'nt exist!";
}

if (file_exists("{$sad_dir}/{$sad_check_file}") or
    !file_exists("{$sad_dir}/{$sad_temp_file}") or
    !file_exists("{$sad_dir}/{$sad_black_file}") or
    !file_exists("{$sad_dir}/{$sad_white_file}") or
    !file_exists("{$sad_dir}/{$sad_all_file}") or
    !file_exists ("{$sad_dir}/../anti_ddos.php")) {
    $config_status .= "Some files does'nt exist!";
    die($config_status);
}

// verificar sesion por ip
require ("{$sad_dir}/{$sad_check_file}");

if ($sad_end_defense and $sad_end_defense > $sad_date) {
    require ("{$sad_dir}/../anti_ddos.php");
} else {
    $sad_num_query = ($sad_sec == $sad_sec_query) ? $sad_num_query++ : '1';
    $sad_file = fopen ("{$sad_dir}/{$sad_check_file}", "w");
    $sad_string = ($sad_num_query >= $sad_ddos_query) ? '<?php $sad_end_defense'.safe_print($sad_date + $sad_defense_time).'; >': '<?php $sad_num_query=' . safe_print($sad_num_query)
```

Figura 26: Código del sistema de protección 2



○ Estructura de directorios y convenciones de nomenclatura de archivos

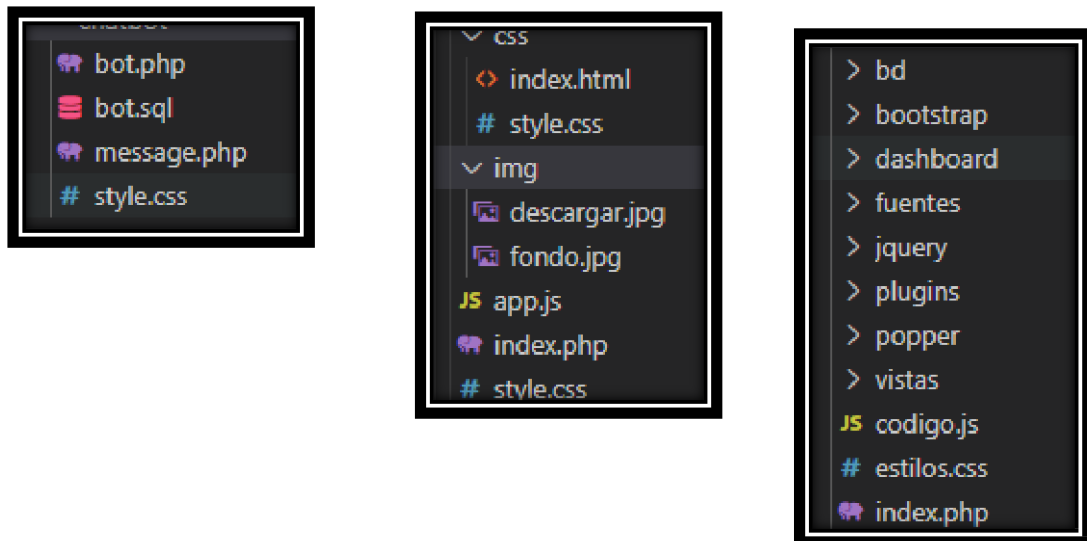


Figura 29: Estructura de directorios y convenciones de nomenclatura de archivos

Fuente: Elaboración Propia

**FASE IV: Pruebas de Funcionalidad**

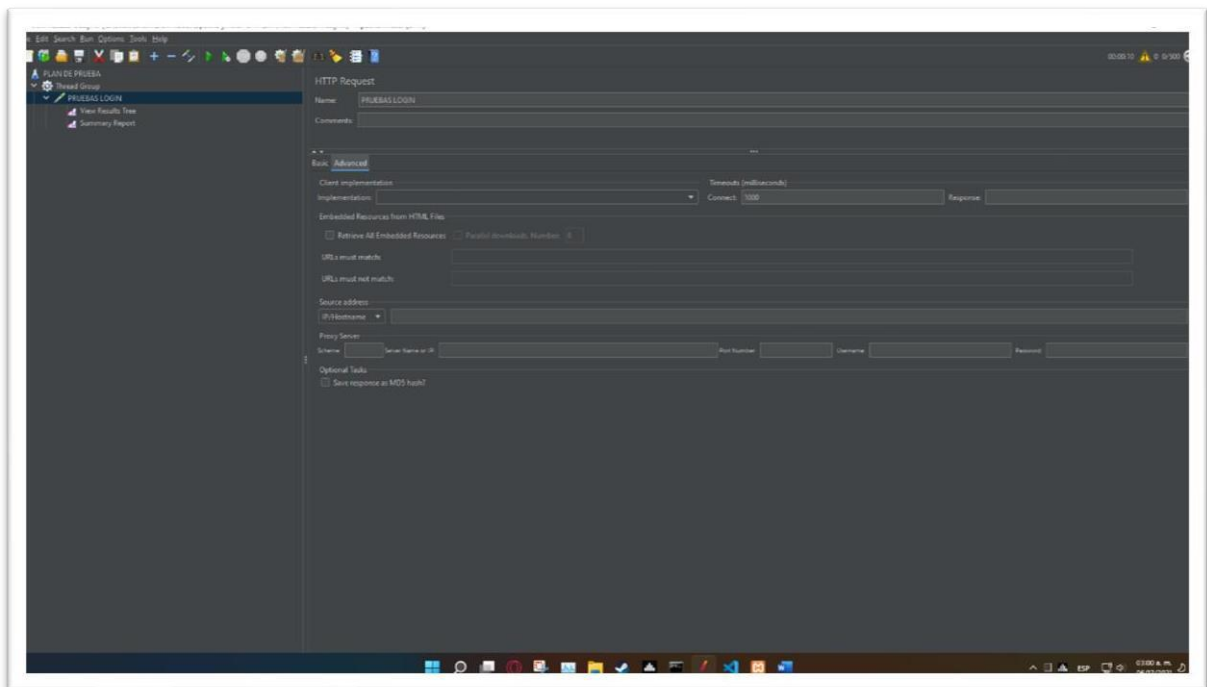
Prueba de Aceptación	
Código: P1	Código de historia: H1, Modulo Login
Descripción: Una vez ingresado al módulo de seguridad el administrador deberá logearse al sistema para poder activar la protección anti DDoS	
Condición de ejecución: El administrador deberá entrar al Login	
Entrada: -usuario y contraseña	
Resultados: credenciales correctas	
Evaluación de prueba: La prueba se realizó de forma satisfactoria.	

Tabla 26: Prueba de aceptación Login

Prueba de Aceptación	
Código: P2	Código de historia: H2, Modulo Dashboard
Descripción: El administrador tendrá acceso a módulos como el dashboard donde le permitirá poder visualizar los resúmenes y estadísticas del sistema	
Condición de ejecución: El usuario deberá estar autenticado exitosamente	
Resultados: información ordenada y precisa	
Evaluación de prueba: La prueba se realizó de forma satisfactoria.	

*Tabla 27: Prueba de aceptación Modulo Dashboard*

## PRUEBA DE CARGA UTILIZANDO LA HERRAMIENTA JMETER



*Figura 30: Prueba de Carga Utilizando la herramienta JMeter*



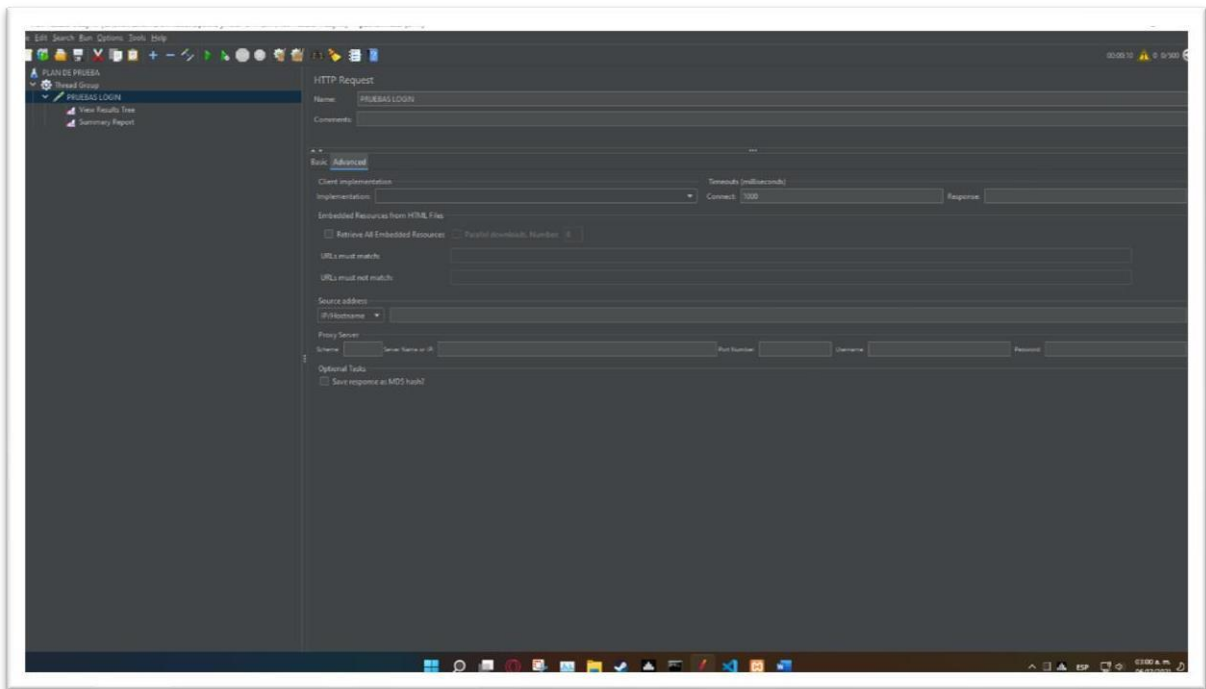


Figura 31: Prueba de Carga Utilizando la herramienta JMeter

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
PRUEBAS LOGIN	500	211	194	420	31.96	0.00%	48.21/sec	314.57	7.20	576
TOTAL	500	211	194	420	31.96	0.00%	48.21/sec	314.57	7.20	576

Figura 32: Prueba de Carga Utilizando la herramienta JMeter 3

## Anexo 7: Clasificación de algoritmos para evitar ataques de Denegación de servicio Web

### Estrategia de búsqueda de información

<b>Dialnet</b>	Algoritmos Shallow Learning, Cañola Garcia (2020)
<b>Google academic</b>	Algoritmos Shallow Learning No Supervisados, Gómez (2019)
<b>IAES</b>	Detección de ataques DDoS mediante algoritmos Deep Learning Supervisados, Thapanarath (2021).
<b>SALESIANA</b>	Algoritmos Deep Learning No Supervisados (Optimización de una red LAN después de un ataque DDoS detectado con técnicas de inteligencia artificial, Vizcaino (2020).
<b>CRAIUSTA</b>	Sistema preventivo contra ataques de denegación de servicio web utilizando Deep Learning, Cañola Garcia (2020)

*Tabla 28: Estrategia de búsqueda de información*

#### **Procedimientos:**

La recolección de información se extraerá de diferentes bases de datos considerando criterios de inclusión y exclusión, teniendo en cuenta el tema investigado en base a palabras clave. La siguiente tabla muestra una recopilación de información de varias bases de datos.

## Recolección de datos

Base de datos	Años		
	(2017-2018)	(2019-2020)	(2021-2022)
Dialnet	1	2	5
Google academic	3	2	4
IAES	0	0	2
SALESIANA	0	3	2
CRAIUSTA	0	2	1

*Tabla 29: Recolección de datos*

En el siguiente apartado se realizó una búsqueda de algoritmos de Deep Learning para evitar ataques de DDoS con mejor efectividad en los últimos años, Se seleccionan algoritmos que predominen por su efectividad.

*Tabla 30: Características de algoritmos para mitigar ataques de DDoS*

		Características			
Deep Learning	Algoritmo Supervisado	<b>Naïve Bayes (NB)</b>	Son clasificadores probabilísticos	Estos algoritmos son escalables	no requieren una gran cantidad de datos para su entrenamiento
		<b>Regresión logística (RL)</b>	Clasificadores	categoricos	adoptan un modelo discriminativo
		<b>Máquinas de vectores de soporte (SVM)</b>	son clasificadores no probabilísticos	muestra los datos en un espacio de función	Su escalabilidad limitada, podría llevar a largos tiempos de procesamiento
		<b>Red neuronal superficial (SNN)</b>	se basan en redes neuronales	organizadas en dos o más capas	utilizado para tareas de clasificación
	Algoritmo no Supervisado	<b>Clustering</b>	Algoritmo para fines de detección de anomalías		Reúne datos con características similares
		<b>Association</b>	identificar patrones desconocido entre todos los datos		Deben combinarse con combinaciones precisas

<b>Shadow Learning</b>	<b>Algoritmo Supervisado</b>	<b>Fully connected Feedforward Deep Neural Network (FNN)</b>	cada neurona está conectada a todas las neuronas	No supone datos de entrada	proporciona un propósito flexible y general	
		<b>Convolutional Feedforward Deep Neural Networks (CNN)</b>	cada neurona recibe su entrada	efectiva en analizar datos espaciales	rendimiento disminuye cuando se aplican a datos no espaciales	
		<b>Recurrent Deep Neural Networks (RNN)</b>	neuronas pueden enviar su salida	los hace más difícil de entrenar		
	<b>Algoritmo no Supervisado</b>	<b>Deep belief networks (DBN)</b>	redes neuronales sin capa de salida.	para tareas de preentrenamiento		
		<b>Stacked AutoEncoders (SAE)</b>	clase de redes neuronales	sobresale en tareas de preentrenamiento	mejores resultados en pequeños conjuntos de datos.	

Tabla 31: Características de algoritmos para mitigar ataques de DDoS 2

Tabla 32: Clasificación de algoritmos para evitar ataques de DDoS

		Detección de intrusos			Análisis de Malware	Spam Detectado
		Network	Botnet (conjunto de ordenadores, denominados bots)	DGA (Algoritmo de generación de dominio)		
Deep Learning	Algoritmo Supervisado	❖ RNN	❖ RNN	❖ NB	❖ FNN ❖ CNN ❖ RNN	SAE
	Algoritmo no Supervisado	❖ DBN ❖ SAE	❖ DBN	❖ NB	❖ DBN ❖ SAE	❖ DBN ❖ SAE
Shadow Learning	Algoritmo Supervisado	❖ RF ❖ NB ❖ SVM ❖ RL ❖ SNN	❖ RF ❖ NB ❖ SVM ❖ RL ❖ SNN	❖ RF	❖ RF ❖ NB ❖ SVM ❖ RL ❖ SNN	❖ RF ❖ NB ❖ SVM ❖ RL ❖ SNN
	Algoritmo no Supervisado	Agrupamiento asociado	Agrupamiento	Agrupamiento	Agrupamiento asociado	Agrupamiento asociado

## Anexo 8: Algoritmo que usa El Software

En la figura 33 se visualiza el algoritmo que utiliza el software para preparar los datos que serán enviados

```
# Import Dataset
balance_data = pd.read_csv('Data/final_dataset.csv')
balance_data
```

	Unnamed: 0	Flow ID	Src IP	Src Port	Dst IP	Dst Port	Protocol
0	624	192.168.4.118-203.73.24.75-4504-80-6	192.168.4.118	4504	203.73.24.75	80	6
1	625	192.168.4.118-203.73.24.75-4504-80-6	192.168.4.118	4504	203.73.24.75	80	6
2	626	192.168.4.118-203.73.24.75-4505-80-6	192.168.4.118	4505	203.73.24.75	80	6
3	627	192.168.4.118-203.73.24.75-4505-80-6	192.168.4.118	4505	203.73.24.75	80	6
4	628	192.168.4.118-203.73.24.75-4506-80-6	192.168.4.118	4506	203.73.24.75	80	6
...	...	...	...	...	...	...	...
12794622	1725894	172.31.67.50-209.85.203.113-53598-80-6	209.85.203.113	80	172.31.67.50	53598	6
12794623	5681778	172.31.69.17-108.174.10.14-54599-443-6	172.31.69.17	54599	108.174.10.14	443	6
12794624	6395326	172.31.0.2-172.31.65.49-53-61087-17	172.31.65.49	61087	172.31.0.2	53	17
12794625	4926899	172.31.0.2-172.31.67.58-53-61580-17	172.31.67.58	61580	172.31.0.2	53	17
12794626	7656685	169.254.169.254-172.31.65.89-80-49393-6	172.31.65.89	49393	169.254.169.254	80	6

Figura 33. Datos que serán enviados

En la figura 34 se visualiza el algoritmo que utiliza el software para Analizar los datos previamente enviados, se prueba la proporción de DDoS



Figura 34. Algoritmo Análisis de datos



En la figura 35 se visualiza que se obtuvieron los puntajes de precisión para los modelos de entrenamiento y prueba, y se analizó la distribución de etiquetas en el conjunto de prueba.

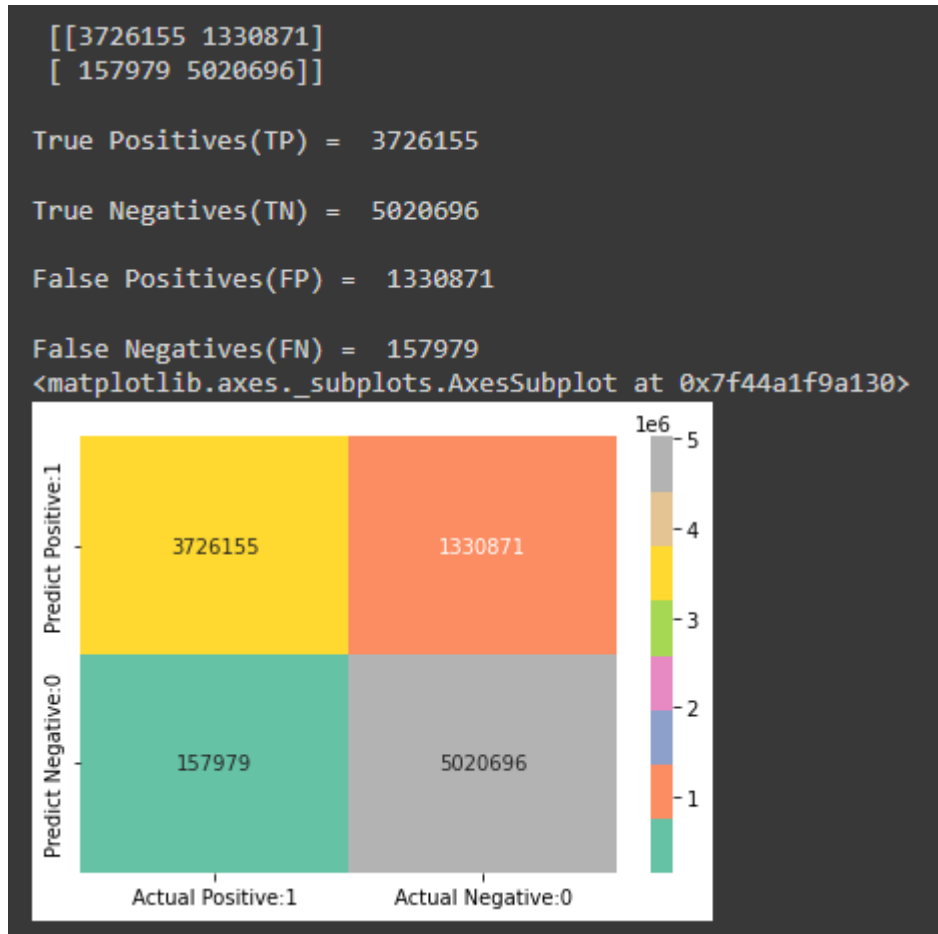


Figura 35. Algoritmo puntajes de precisión

En la figura 36 se visualiza resultados tanto para los modelos de entrenamiento como para los de prueba, se construyeron matrices de confusión y se ejecutaron medidas de precisión y recuperación en la división de prueba de los datos.

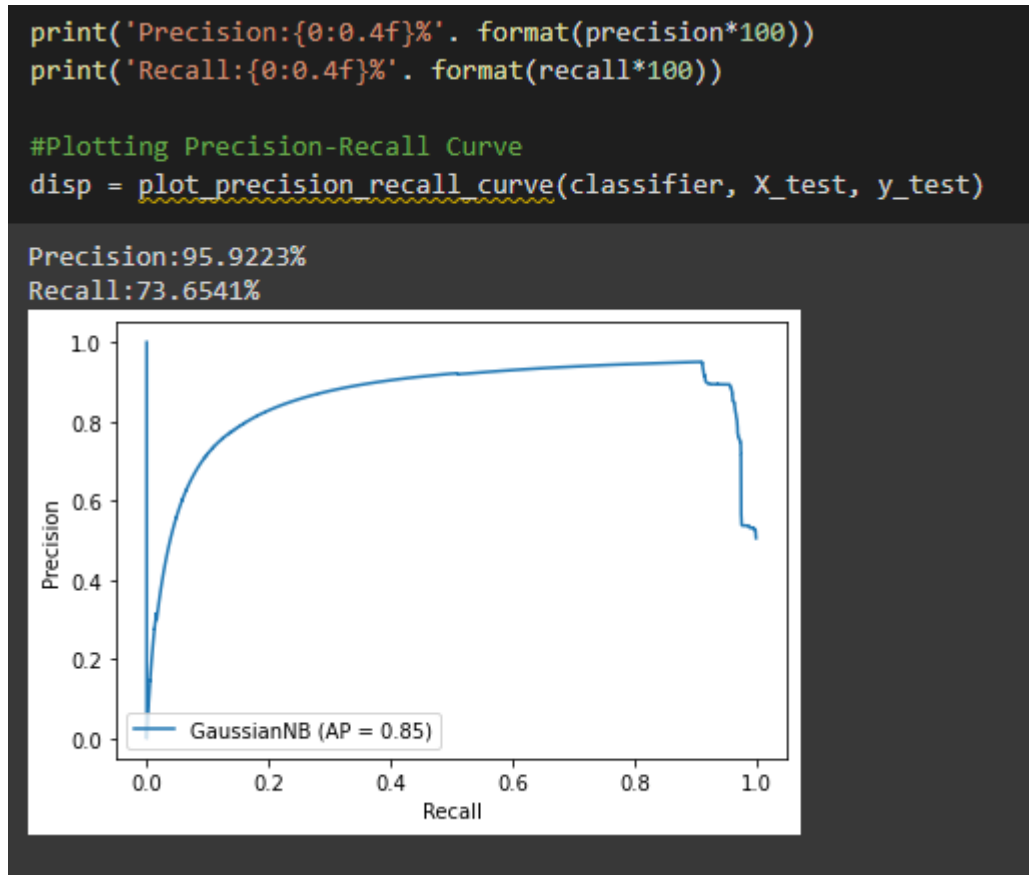
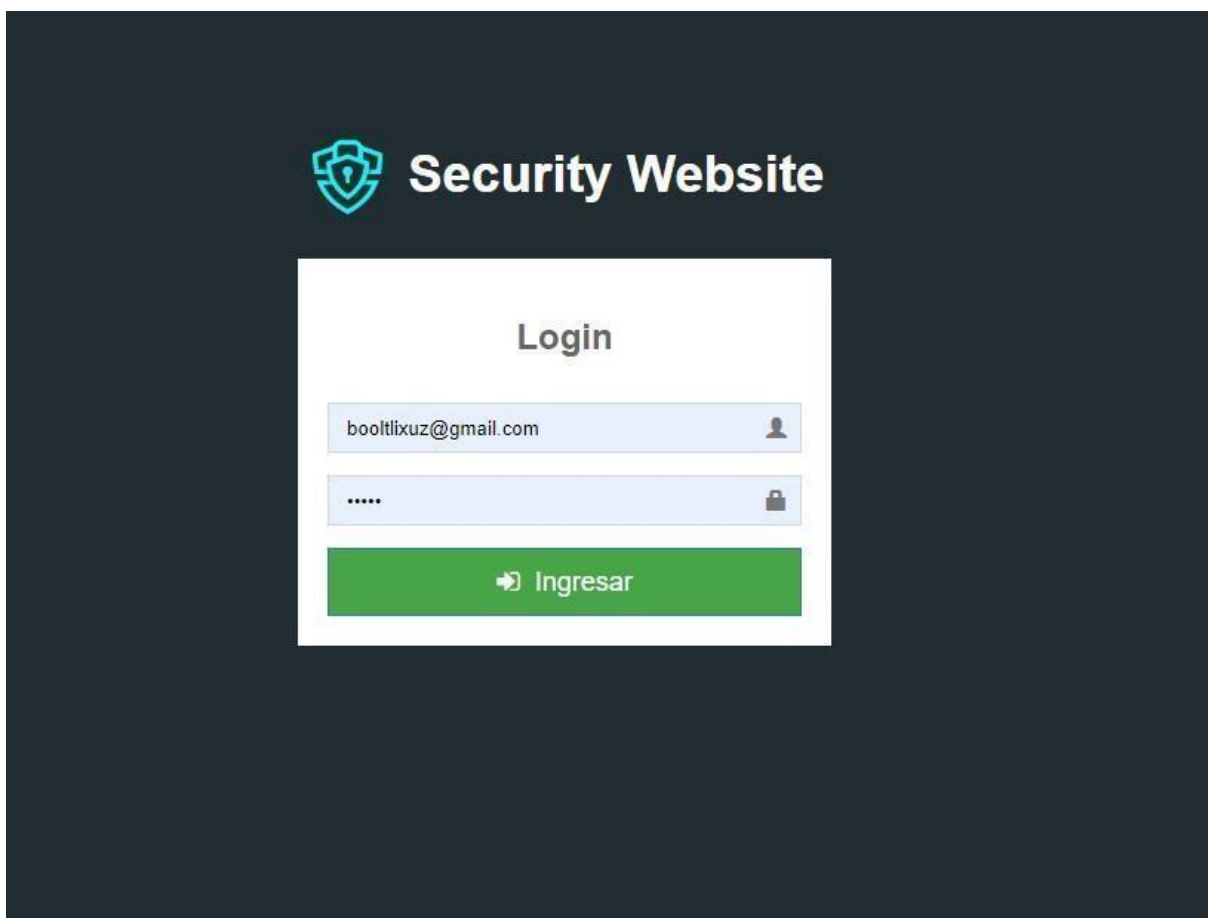


Figura 36. Algoritmo puntajes de Modelo de entrenamiento

## Anexo 9: Prototipos del Software

En la figura 37 podemos observar la interfaz de inicio de sesión para el administrador del sitio web.



*Figura 37. Interfaz de registro de login*

En la figura 38 se visualiza la interfaz principal que viene a contener el dashboard a la que podemos acceder a diferentes módulos y previsualizar las herramientas a la disposición.

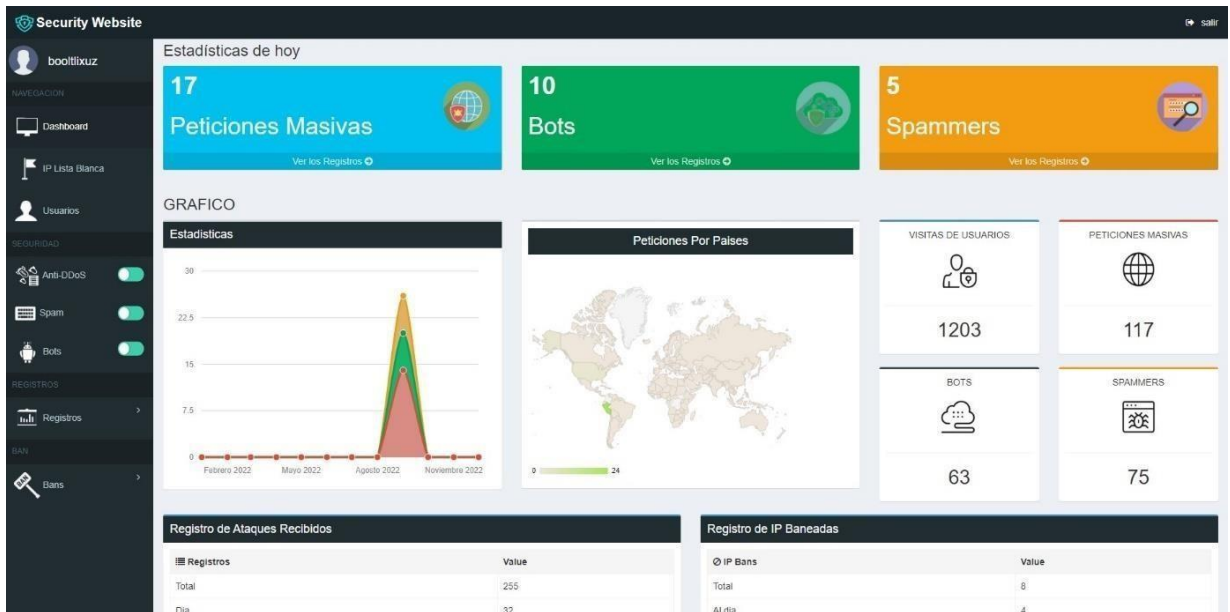


Figura 38. Interfaz de Dashboard

En la figura 39 se visualiza la interfaz del Módulo Protección contra ataques DDoS. Donde podemos activar y desactivar el módulo, de igual forma el módulo de CheKing DDoS que nos proporcionará más seguridad.

The screenshot displays the 'Security Website' management interface. On the left is a dark sidebar with navigation options: 'boottikuz', 'NAVIGACION' (Dashboard, IP Lista Blanca, Usuarios), 'SEGURIDAD' (Anti-DDoS, Spam, Bots), 'REGISTROS' (Registros), and 'HERR' (Bans). The main content area is divided into three panels:

- Peticiones Masivas - Modulo de Seguridad:** Shows a large green 'ACTIVADO' status. Below it, a configuration section includes 'Proteccion en tiempo Real' (On) and 'AutoBan' (Off). A 'Guardar' button is at the bottom.
- Modulo de protección contra Ataques DDoS:** Displays 'La protección Anti-DDoS Checking está Activada' and 'ANTIDDOS is checking...'. It also has an 'On' toggle and a 'Guardar' button.
- Ver Registros de amenazas Recientes:** Lists recent threats. The first entry is for IP 200.43.28.105, with a 'Proxy' threat type, dated 24 September 2022 at 23:02. The second entry is for IP 98.43.228.101, also with a 'Proxy' threat type and the same date. Each entry has 'Detalles', 'Status', and 'Eliminar' buttons.

Registros	Total de Ataques
Total	26
Dia	0
Al Mes	26
Al Año	26

Figura 39. Interfaz de Modulo Protección DDoS

En la figura 40 se visualiza la interfaz del Módulo Protección contra ataques DDoS Desactivado de tal forma que el sitio web se encuentra vulnerable ante posibles ataques.



Figura 40. Interfaz de Modulo Protección DDoS Desactivado

En la figura 41 se visualiza la interfaz del módulo de CheKing DDoS Desactivado.



*Figura 41. Interfaz de Modulo Protección Checking Desactivado*

En la figura 42 se visualiza la interfaz del Módulo Protección contra ataques de Spam

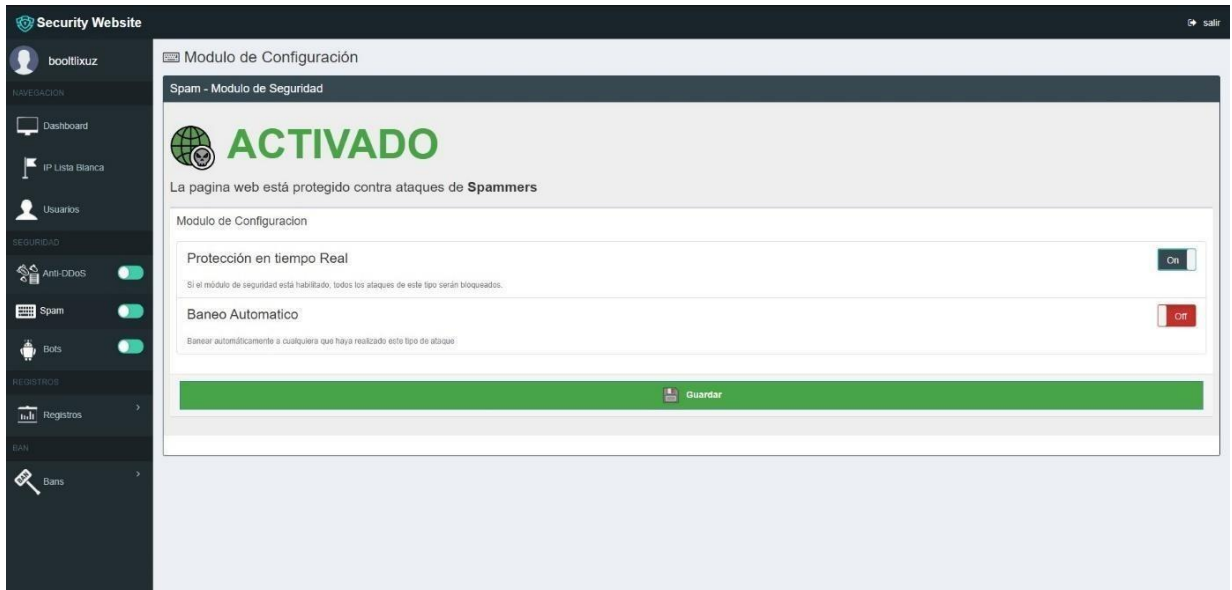


Figura 42. Interfaz de Modulo Protección contra Spam Activado

En la figura 43 se visualiza la interfaz del Módulo Protección contra ataques de Spam Desactivado



Figura 43. Interfaz de Modulo Protección contra Spam Desactivado



En la figura 44 se visualiza la interfaz del Módulo Protección contra ataques de Bots

The screenshot displays the 'Security Website' dashboard for user 'booltixuz'. The main content area is titled 'Security Module' and 'Modulo de Seguridad Proteccion Login'. A large green 'ACTIVADO' status is shown with a globe icon. Below this, a message states 'La pagina web está protegida contra ataques de Bots'. The 'Modulo de Configuración' section includes a toggle for 'Banear Automaticamente', which is currently set to 'Off'. A green 'Guardar' button is located at the bottom of the configuration area. The 'Registro de Ataques Recibidos' section contains a table with the following data:

Registros	Total de Ataques
Total	26
Dia	0
Al Mes	26
Al Año	26

Figura 44. Interfaz de Modulo Protección contra Bots

En la figura 45 se visualiza la interfaz del Módulo Protección contra ataques de Bots maliciosos, bots falsos y bots anónimos.

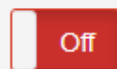
## Modulo de protección contra Bots

### La protección contra ataques de Bots está Desactivada

#### Bots Maliciosos



Ayuda a detectar **Bots Maliciosos** y bloquea el acceso a la pagina



#### Bots Falsos



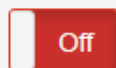
Ayuda a detectar **Bots Falsos** y bloquea el acceso a la pagina



#### Bots Anonymous



Ayuda a detectar **Bots Anonimos** y bloquea el acceso a la pagina



**Guardar**

*Figura 45. Interfaz de Modulo Protección contra bots falsos y bots anónimos*

En la figura 46 se visualiza la interfaz del Lista de los ataques DDoS que enviaron a la página web y se clasifican por tipos.

Security Website salir

boottikuz

NAVIGACION

- Dashboard
- IP Lista Blanca
- Usuarios

CONFIGURACION

- Anti-DDoS
- Spam
- Bots

REGISTROS

- Registros

BAN

- Bans

### Todos los Registros

Show 10 entries Search:

ID	Dirección IP	Fecha	Pais	Tipo de Ataque	Acciones
40	200.43.228.105	24 September 2022	Peru	Proxy	Detalles  Ban  Eliminar
39	98.43.228.101	24 September 2022	Peru	Proxy	Detalles  Ban  Eliminar
38	190.43.228.205	24 September 2022	Peru	Proxy	Detalles  Ban  Eliminar
37	190.43.228.205	24 September 2022	Peru	Proxy	Detalles  Ban  Eliminar
36	190.43.228.205	24 September 2022	Peru	Proxy	Detalles  Ban  Eliminar
35	193.43.228.205	25 September 2022	Peru	Spammer	Detalles  Ban  Eliminar
34	199.34.228.207	25 September 2022	Peru	Spammer	Detalles  Ban  Eliminar
33	190.43.228.206	25 September 2022	Peru	Spammer	Detalles  Ban  Eliminar
32	94.34.228.205	24 September 2022	Peru	Spammer	Detalles  Ban  Eliminar
31	190.43.228.201	24 September 2022	Peru	Spammer	Detalles  Ban  Eliminar

Showing 1 to 10 of 26 entries < 1 2 3 >

Figura 46. Interfaz de Lista de los ataques DDoS

En la figura 47 se visualiza la interfaz de búsqueda por palabra.



Figura 47. Interfaz de interfaz de búsqueda por palabra.

En la figura 48 se visualiza la interfaz de ban por IP

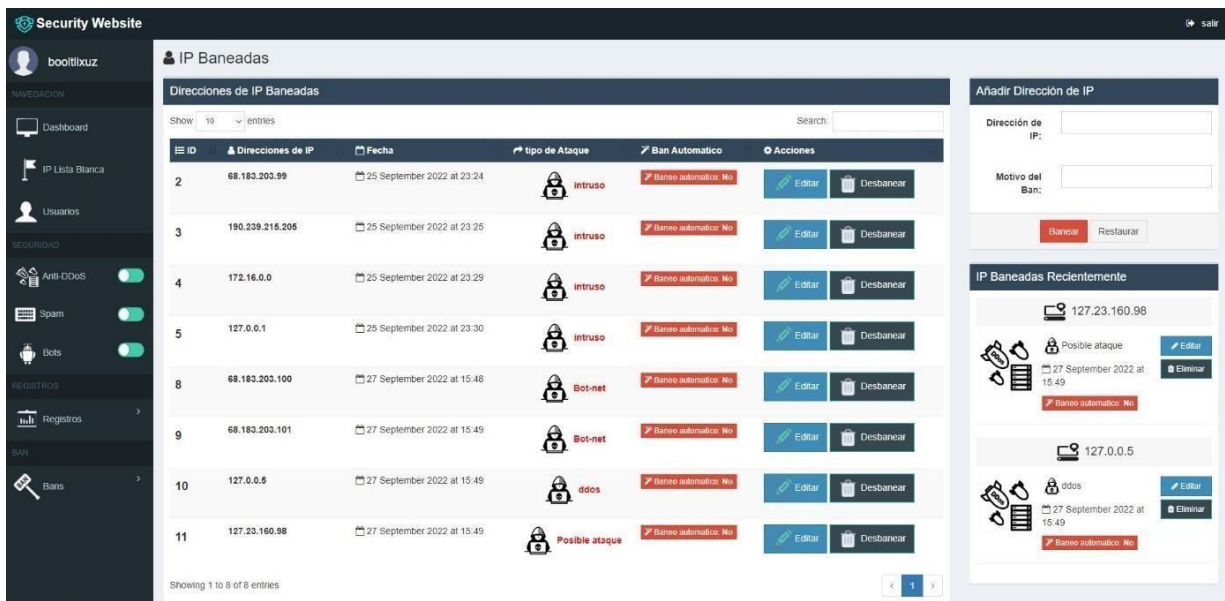


Figura 48. Interfaz de interfaz de ban por IP.

En la figura 49 se visualiza la interfaz de ban por país

The screenshot shows the 'Banear País' interface in a 'Security Website' dashboard. The sidebar on the left contains navigation links for 'Dashboard', 'IP Lista Blanca', 'Usuarios', 'Anti-DDoS', 'Spam', 'Bots', 'Registros', and 'Bans'. The main panel is titled 'Banear País' and features a table of 'Países Baneados' (Banned Countries). The table has columns for 'ID', 'Países', 'Redirecting', and 'Acciones'. The 'Acciones' column contains 'Editar' (Edit) and 'Eliminar' (Delete) buttons for each entry. Below the table, it indicates 'Showing 1 to 10 of 10 entries'. To the right of the table, there is a form to 'Añadir País' (Add Country) with a dropdown menu for 'País' (Country) set to 'Afghanistan' and buttons for 'Add' and 'Reset'. Below the form is a world map titled 'Mapa Países Baneados' (Banned Countries Map) showing highlighted regions in green and red.

ID	Países	Redirecting	Acciones
2	Albania	No	<a href="#">Editar</a> <a href="#">Eliminar</a>
3	Algeria	No	<a href="#">Editar</a> <a href="#">Eliminar</a>
4	American Samoa	No	<a href="#">Editar</a> <a href="#">Eliminar</a>
5	Andorra	No	<a href="#">Editar</a> <a href="#">Eliminar</a>
6	Armenia	No	<a href="#">Editar</a> <a href="#">Eliminar</a>
7	Bermuda	No	<a href="#">Editar</a> <a href="#">Eliminar</a>
8	Canary Islands	No	<a href="#">Editar</a> <a href="#">Eliminar</a>
9	Brazil	No	<a href="#">Editar</a> <a href="#">Eliminar</a>
10	Cayman Islands	No	<a href="#">Editar</a> <a href="#">Eliminar</a>
11	United States of America	No	<a href="#">Editar</a> <a href="#">Eliminar</a>

Figura 49. Interfaz de interfaz de ban por País.

En la figura 50 se visualiza la interfaz de lista de IP blanca

The screenshot displays the 'IP Lista Blanca' (IP Whitelist) interface within the 'Security Website' dashboard. The user 'boollixuz' is logged in. The interface includes a sidebar with navigation and security settings, and a main content area for managing the IP whitelist.

**Security Website**  
boollixuz

NAVEGACION

- Dashboard
- IP Lista Blanca
- Usuarios

SEGURIDAD

- Anti-DDoS
- Spam
- Bots

REGISTROS

- Registros >

BAN

- Bans >

IP Lista Blanca

IP Whitelist

Show 10 entries Search:

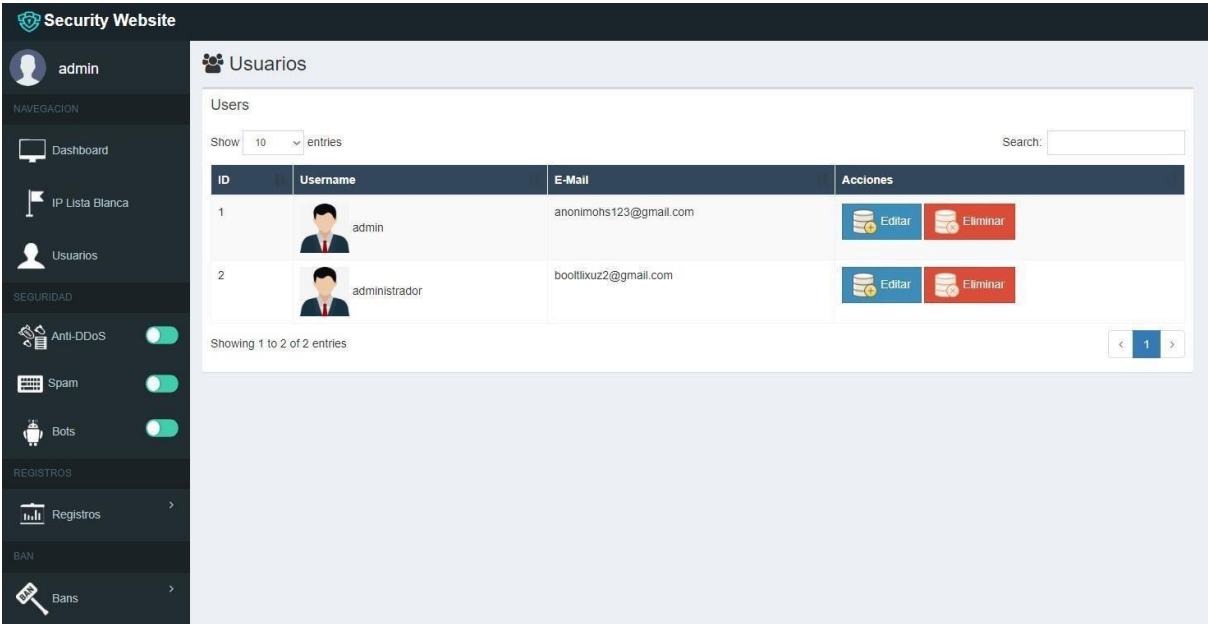
ID	Dirección IP	Acciones
1	192.168.1.23	<a href="#">Editar</a> <a href="#">Eliminar</a>
2	192.168.1.25	<a href="#">Editar</a> <a href="#">Eliminar</a>
3	192.168.1.26	<a href="#">Editar</a> <a href="#">Eliminar</a>
4	192.168.1.27	<a href="#">Editar</a> <a href="#">Eliminar</a>

Showing 1 to 4 of 4 entries

< 1 >

Figura 50. Interfaz de interfaz de lista Blanca

En la figura 51 se visualiza la interfaz de usuario

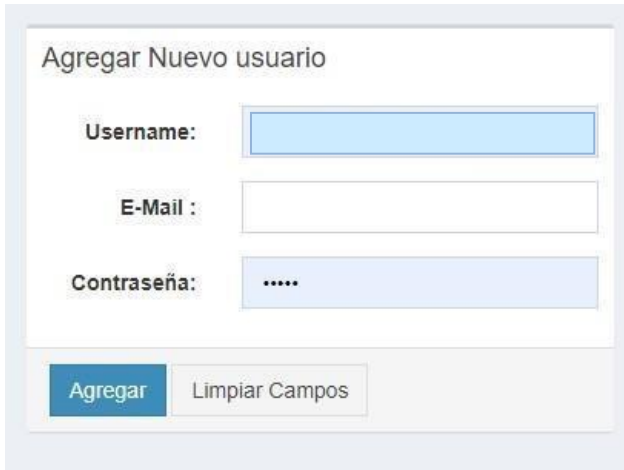


The screenshot shows the 'Security Website' user management interface. On the left is a dark sidebar with navigation and security options. The main content area is titled 'Usuarios' and displays a table of users. The table has columns for ID, Username, E-Mail, and Acciones. Two users are listed: 'admin' and 'administrador'. Below the table, there are pagination controls showing 'Showing 1 to 2 of 2 entries'.

ID	Username	E-Mail	Acciones
1	admin	anonymohs123@gmail.com	Editar Eliminar
2	administrador	boollitxuz2@gmail.com	Editar Eliminar

Figura 51. Interfaz de interfaz de usuario

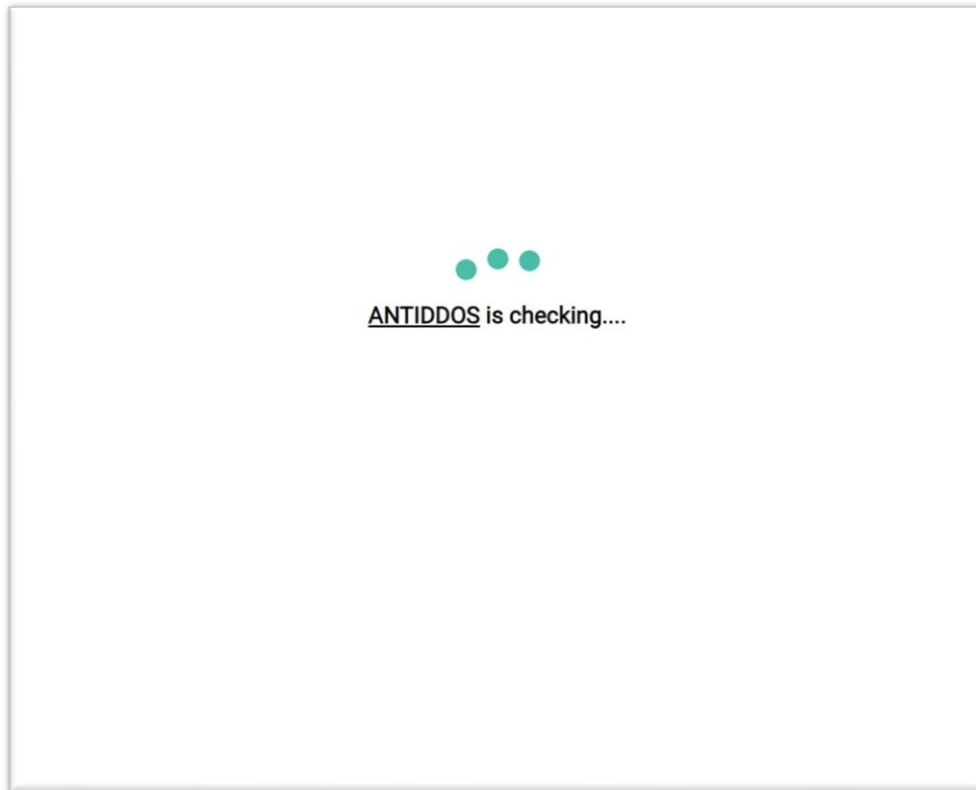
En la figura 52 se visualiza agregar usuario



The screenshot shows a form titled 'Agregar Nuevo usuario'. It contains three input fields: 'Username:', 'E-Mail:', and 'Contraseña:'. The 'Contraseña:' field is masked with dots. Below the fields are two buttons: 'Agregar' and 'Limpiar Campos'.

Figura 52. Interfaz de interfaz de agregar usuario

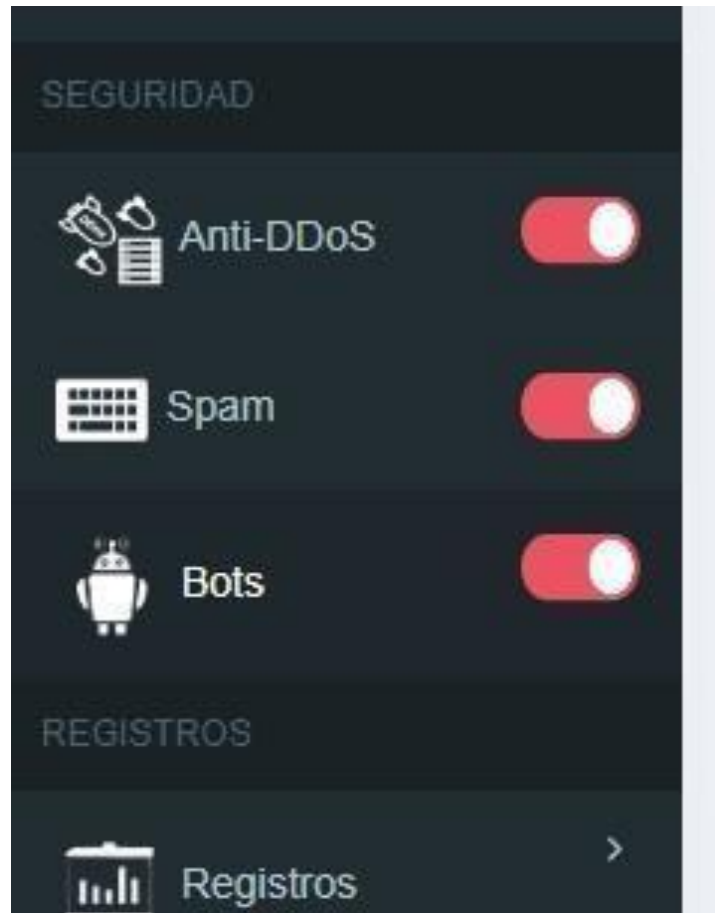
En la figura 53 se visualiza la interfaz principal de la página checking DDoS



*Figura 53. Interfaz de interfaz de Checking DDoS*



En la figura 54 se observa la interfaz del Core que previsualiza el estado de los módulos



*Figura 54. Interfaz de interfaz Core*



**UNIVERSIDAD CÉSAR VALLEJO**

**FACULTAD DE INGENIERÍA Y ARQUITECTURA  
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

### **Declaratoria de Autenticidad del Asesor**

Yo, COHELLO AGUIRRE ROGELIO GONZALO, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ATE, asesor de Tesis titulada: "Sistema de seguridad usando Deep Learning para la prevención de ataques de denegación de servicio web en la empresa SISTEC , 2022", cuyo autor es RIVERA MALLMA JUAN WILLIANS, constato que la investigación tiene un índice de similitud de 21.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 29 de Noviembre del 2022

<b>Apellidos y Nombres del Asesor:</b>	<b>Firma</b>
COHELLO AGUIRRE ROGELIO GONZALO <b>DNI:</b> 07634626 <b>ORCID:</b> 0000-0001-5526-5231	Firmado electrónicamente por: RCOHELLO el 13-12- 2022 18:33:25

Código documento Trilce: TRI - 0462135