“Implementación de una solución de Business Intelligence que permita analizar y mitigar ataques informáticos del tipo denegación de servicio (DoS) en un ISP de Ecuador”

Carrión Basantes, Santiago Andrés

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Maestría en Gestión de Sistemas de Información e Inteligencia de Negocios

Trabajo de titulación, previo a la obtención del título de Magíster en Gestión de Sistemas de Información e Inteligencia de Negocios

PhD. Gualotuña Alvarez, Tatiana Marisol

14 de Agosto de 2023

URKUND

Document Information

Analyzed document	TESIS_Carrion_Santiago_23.docx (D171142596)
Submitted	2023-06-22 17:38:00
Submitted by	Ramiro Delgado
Submitter email	pg.docenterdr@uniandes.edu.ec
Similarity	2%
Analysis address	pg.docenterdr.unia@analysis.urkund.com

Firmado electrónicamente por:
TATIANA MARISOL
GUALOTUNA ALVAREZ

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Certificación

Certifico que el trabajo de titulación: "**Implementación de una solución de Business Intelligence que permita analizar y mitigar ataques informáticos del tipo denegación de servicio (DoS) en un ISP de Ecuador**" fue realizado por el señor **Carrión Basantes, Santiago Andrés;** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 14 de agosto de 2023

Firmado electrónicamente por: TATIANA MARISOL GUALOTUÑA ALVAREZ

.....

PhD. Gualotuña Alvarez, Tatiana Marisol

Director

C.C.: 1711498418

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Responsabilidad de Autoría

Yo **Carrión Basantes, Santiago Andrés**, con cédula de ciudadanía n° 1722196233, declaro que el contenido, ideas y criterios del trabajo de titulación*:* **Implementación de una solución de Business Intelligence que permita analizar y mitigar ataques informáticos del tipo denegación de servicio (DoS) en un ISP de Ecuador** es de mí autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 14 de agosto de 2023

SANTIAGO ANDRÉS CARRIÓN BASANTES

.....

Carrión Basantes, Santiago Andrés

C.C.: 1722196233

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Autorización de Publicación

Yo **Carrión Basantes, Santiago Andrés**, con cédula de ciudadanía n° 1722196233, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Implementación de una solución de Business Intelligence que permita analizar y mitigar ataques informáticos del tipo denegación de servicio (DoS) en un ISP de Ecuador** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 14 de agosto de 2023

Firmado electrónicamente por:
SANTIAGO ANDRES
CARRION BASANTES

.....

Carrión Basantes, Santiago Andrés

C.C.: 1722196233

Dedicatoria

A Dios por guiarme, cuidarme y permitirme cumplir un objetivo más en mi vida.

A mi madre Margarita, por haberme inculcado la persistencia y fuerza en la vida, no dejarme desvanecer por los problemas, su cariño y poyo guían mi camino.

A mi grandiosa familia, mis hermanos Dave, Edy, Alexita y Diany que juntos hemos superado los obstáculos, adversidades y de igual forma compartimos los logros y momentos felices.

A mis amigos (as) y compañeros (as) de la maestría, por compartir momentos, recuerdos y gratas experiencias.

Agradecimientos

La culminación de este trabajo ha sido de suma importancia para mi carrera y formación profesional, una grata experiencia vivida, lo que empezó como una idea de volver a prepararme profesionalmente ya es una realidad, conocí personas valiosas con las que compartimos momentos memorables que, junto con su apoyo, concejos y ayuda son parte de este objetivo cumplido, a mi familia que me apoya en todo lo que hago, en fin, a todas las personas que directa o indirectamente me han aportado para la culminación de este logro.

Índice de contenido

Dedicatoria....6

Agradecimientos....7

Índice de contenido....8

Índice de tablas....11

Índice de figuras....12

Resumen....14

Abstract....15

Capítulo I....16

Problema de Investigación....16

Antecedentes....*16*

Planteamiento del problema....*17*

Objetivos de la Investigación....*18*

Objetivo General....18

Objetivos Específicos....18

Justificación, Importancia y Alcance....*19*

Preguntas de Investigación....*19*

Hipótesis....*20*

Señalamiento de las Variables de la Hipótesis....*20*

Capítulo II 20

Marco Teórico 20

Inteligencia de Negocios *21*

Inteligencia de Negocios Ágil *23*

Proveedor de servicios de Internet *23*

Redes definidas por software *24*

Máquina de vectores de soporte *25*

Ataques DDoS *27*

Tipos de ataques DDoS *28*

Ataques basados en volumen 29

Ataque basado en protocolo 30

Ataque basado en la capa de aplicación 30

Mecanismos de defensa ante ataques DDoS *30*

Prevención de ataques DDoS 30

Detección de ataques DDoS 30

Identificación de ataques DDoS 31

Mitigación de defensa ante ataques DDoS 32

Estado del arte *33*

Capítulo III 43

Metodología de Investigación 43

Metodología de Ralph Kimball *43*

Metodología Scrum *45*

Metodología.....*46*

Capítulo IV.....50

Desarrollo de la solución.....50

Inicio.....*50*

Análisis del problema.....50

Planificación y estimación.....*52*

Implementación.....*52*

Selección de la infraestructura.....52

PowerDesigner.....53

Microsoft SQL Server.....58

Pentaho Data integration.....65

Power BI.....68

Revisión y retrospectiva.....*69*

Validación de la solución.....*70*

Capitulo V.....73

Lanzamiento.....73

Conclusiones y recomendaciones.....78

Conclusiones.....78

Recomendaciones.....79

Referencias Bibliográficas.....80

Índice de tablas

Tabla 1 Clasificación de ataques distribuidos de denegación de servicios DDoS 29

Tabla 2 Listado de artículos del Grupo de control 34

Tabla 3 Construcción de la cadena de búsqueda 36

Tabla 4 Resumen de estudios candidatos 38

Tabla 5 Estudios primarios 39

Tabla 6 Nivel de granularidad Dim_flujo 54

Tabla 7 Descripción Dim_tiempo 56

Tabla 8 Descripción Dim_red 56

Tabla 9 Descripción DIM_puerto 57

Tabla 10 Descripción DIM_cliente 57

Tabla 11 Descripción DIM_protocolo 57

Tabla 12 Tabla de hechos Fac_flujo 58

Índice de figuras

Figura 1 Jerarquía de estudio 20
Figura 2 Arquitectura de Business Intelligence 22
Figura 3 Arquitectura SDN 24
Figura 4 Grafica de máquina de vectores de soporte 26
Figura 5 Estructura de un ataque DDoS 27
Figura 6 Artículos encontrados en los repositorios académicos 38
Figura 7 Metodología de Kimball 44
Figura 8 Fases de la metodología Scrum 46
Figura 9 Relación entre los procesos scrum y los objetivos 47
Figura 10 Diagrama lógico de la infraestructura de red del ISP 51
Figura 11 Herramientas seleccionadas para el modelo DWH 53
Figura 12 Descripción Dsa_flujo 54
Figura 13 Modelo dimensional físico DWH Fac_flujo 55
Figura 14 SQL Server, bases de datos 59
Figura 15 Script para la recolección de datos 60
Figura 16 Script para la recolección de datos flujo de datos 61
Figura 17 Script de entrenamiento del modelo para detección de ataques 62
Figura 18 Script algoritmo mitigación ataque DDoS 63
Figura 19 Script del algoritmo de machine learning basado en SVM 64
Figura 20 Resultado del controlador SDN para la detección y mitigación de ataques 64
Figura 21 Clasificador de regiones de decisión basado en SVM 65
Figura 22 Proceso de trasformación y carga para las dimensiones 66
Figura 23 Proceso de trasformación y carga para la dimensión tiempo 66

Figura 24 Proceso de trasformación y carga del DSA 67

Figura 25 Proceso de trasformación y carga del DSA y FAC_FLUJO 67

Figura 26 Proceso de trasformación y carga de la tabla de hechos y dimensiones 68

Figura 27 Modelo estrella Flujo de datos en Power BI..... 70

Figura 28 Reporte propuesto análisis datos históricos 71

Figura 29 Reporte propuesto análisis datos históricos tendencias de ataques..... 72

Figura 30 Correlación de parámetros del SVM..... 74

Figura 31 Clasificación de la máquina de vectores de soporte 74

Figura 32 Reporte propuesto análisis datos periodo año 2022 tendencias de ataques 75

Figura 33 Reporte mitigación de ataques en porcentaje por vector de ataque 76

Resumen

En la actualidad, la sociedad depende cada vez más del Internet, por lo que es extremadamente importante para las empresas garantizar que este servicio esté disponible en todo momento, el proveedor de servicios de Internet, debe asegurar el acceso al Internet cumpla con una eficiente gestión en la seguridad de la información para proteger la red y sus datos, el aumento de los ciberataques y de los ataques de denegación de servicio distribuidos, los cuales son extremadamente disruptivos al punto que logran interrumpir o colapsar la red de la víctima. Por esta razón, es imprescindible desarrollar medidas de seguridad que estén a la par de cualquier ataque denegación de servicio distribuidos. El presente estudio utiliza varias herramientas de inteligencia de negocios las cuales permiten analizar los datos históricos, identificar, medir, supervisar, detectar y mitigar ataques denegación de servicio distribuidos en la infraestructura del ISP, con la finalidad de mejorar la toma de decisiones en seguridad de la información a través de un prototipo que muestre visualizaciones en Dashboard. Se propone una metodología de gestión de proyectos ágil Scrum, como fase de inicio se analiza la situación actual, para las fases del diseño, construcción y validación de la solución se basaran en el modelo de Ralph Kimball, para el análisis de situación actual del proveedor de servicios de Internet, los datos se obtienen de un controlador de software definido por red que analiza el tráfico en tiempo real, para la detección de ataques de denegación de servicio distribuidos, mediante algoritmos de aprendizaje automático de una máquina de vectores de soporte, el tráfico se clasifica en anómalo y normal, logrando evidenciar la mitigación de ataques denegación de servicio distribuidos y la importancia de la inteligencia de negocios como una herramienta crucial en la prevención y buenas prácticas de seguridad lógica en la red.

Palabras clave: inteligencia de negocios, denegación de servicios distribuidos, proveedor de servicios de internet, software definido por red, máquina de vectores de soporte.

Abstract

Nowadays, society has increased its dependence on the Internet. For companies is indispensable to maintain the high availability of service, in order that, the Internet service provider must make ensure of Internet access complies with efficient information security management to protect the network and its data. Am increase in cyberattacks and distributed denial of service attacks are extremely disruptive to the point that they manage to interrupt or collapse the network of victims. For this reason, it is essential to develop security measures that are on distributed denial of service attacks. This research uses several business intelligence tools which allow analyzing historical data, identifying, measuring, monitoring, detecting, and attacking distributed denial of service attacks on the ISP infrastructure, in order to improve decision-making in Internet security the information through a prototype that shows visualizations in Dashboard. An agile Scrum project management methodology is proposed, as the start phase the current situation is analyzed, for the design, construction and validation phases of the solution they will be based on the Ralph Kimball model, for the analysis of the current situation of the Internet service provider, the data is obtained from a software controller defined by network that analyzes the traffic in real time, for the detection of distributed denial of service attacks, by means of automatic learning algorithms of a support vector machine, the traffic is classified into abnormal and normal, managing to demonstrate the mitigation of distributed denial of service attacks and the importance of business intelligence as a crucial tool in the prevention and good logical security practices in the network.

Keywords: business intelligence, distributed denial of service, internet service provider, network-defined software, support vector machine.

Capítulo I

Problema de Investigación

Antecedentes

Los ataques de denegación de servicio DoS[1], son un tipo de ciberataque que como principal objetivo inhabilitan la disponibilidad de un sistema, una aplicación o un servicio, con el fin de bloquear el acceso a los usuarios legítimos. Este ataque puede afectar, tanto a la infraestructura del proveedor de servicios de Internet, así como a una aplicación o el canal de transmisión.

El proveedor DYN DNS sufrió varios ataques del tipo denegación de servicios DDoS[2] que lograron afectar e incluso interrumpir el servicio de sitios tan relevantes como los medios de comunicación New York Times y Financial Times, de igual forma a plataformas como Playstation Network, Reddit, Twitter y Spotify. El ataque empleó entre 50.000 y 100.000 dispositivos IoT (Internet of Things) controlados mediante la botnet[3] en el 2016 (Obaid, Mohammad, & Chung-Horng, 2019).

Según el reporte de seguridad de infraestructura mundial, destacó que el 57% de las empresas y el 45% de los proveedores de servicios de Internet experimento que su ancho de banda se saturo debido a los ataques DDoS, los botnets se emplearon para lanzar ataques que afectaron a aplicaciones web, servicios y dispositivos de infraestructura al igual que para ataques volumétricos en el 2018 (Cisco Systems, Reporte Anual de Ciberseguridad de Cisco, 2020).

---

[1] DoS (Denial of Service) denegación de servicio es un ataque que impide la utilización correcta de ciertos servicios por parte de los usuarios autorizados y legítimos.

[2] DDoS (Destributed Denial of Service) denegación de servicio distribuido son ataques que se caracterizan por enviar varias solicitudes de varios orígenes hacia un mismo destino colapsando de esta forma el servicio.

[3] Botnet es el nombre técnico que denomina a cualquier grupo de red de robots informáticos, que se ejecutan de manera autónoma, para controlar ordenadores/servidores infectados.

El 59% de los proveedores de servicios de Internet y el 48% de las empresas experimentaron ataques de denegación de servicios distribuidos, un aumento del 20% con respecto al año 2019. Los proveedores de servicios de Internet experimentaron ataques volumétricos, mientras que las empresas informaron un aumento del 30% en ataques dirigidos a nivel de aplicaciones.

Los ataques de denegación de servicio distribuidos combinan inundaciones de gran cantidad de tráfico, ataques a nivel de aplicaciones y de agotamiento de recursos de protocolo TCP de manera constante, por lo tanto, aumenta la complejidad de la mitigación y la oportunidad de éxito del atacante, la cantidad de instituciones que confirmaron la pérdida de ingresos como un impacto en sus negocios ante los ataques DDoS representan el doble en el 2018 (Cisco Systems, Reporte de amenazas, 2019).

Planteamiento del problema

Los ataques de denegación de servicio distribuidos DDoS, son utilizados para bloquear por completo el funcionamiento normal del recurso o servicio ofrecido por un servidor, aprovechando sus vulnerabilidades pueden colapsar el sistema. La intensión primordial de los ciberdelincuentes es provocar un perjuicio, tanto a los usuarios, como al proveedor que lo ofrece (ISP), bloqueando su funcionalidad y provocando pérdidas, de prestigio como económicas.

El mayor ataque de denegación de servicio ocurrido se produjo, el 28 de febrero de 2018, a una conocida plataforma de proyectos colaborativos, la misma que dejo de funcionar durante 10 minutos de manera intermitente. A pesar de toda la seguridad de la que disponía la plataforma, no pudo afrontar el bombardeo de 1,35 Tbps. Este ataque fue realizado a través de una red botnet utilizando servidores de diversas entidades (Barrett, Ili, & Desmond, 2019).

En el caso de Ecuador en abril del 2019, se presentaron ataques a 300 entidades públicas con un promedio de 133 ataques cibernéticos por segundo cuando se produjo la

detención de Julian Assange, esto ubicó al país en el puesto 31 en el ranking mundial de las naciones más agredidas (El telegrafo, 2019).

Es Las empresas que han adoptado estrategias de transformación digital ahora, sufren un considerable aumento de ataques de denegación de servicio (DoS) cuyo costo por tiempo improductivo asociado a los cortes del servicio de Internet, pueden ser altos.

Para un ISP su prioridad es mantener y precautelar la disponibilidad, integridad y rendimiento de los servicios, el de los clientes y el de su infraestructura, si las vulnerabilidades no son mitigadas la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) puede bloquear o limitar los servicios del ISP con consecuencias mensurables como, pérdida de ingresos, daño a la reputación y marca (ARCOTEL, 2019).

Hay una alta tasa de vulnerabilidades del tipo DDoS en el ISP, los ataques de la capa de aplicación van en aumento mientras que los ataques de la capa de red están disminuyendo. La tendencia es preocupante porque la capa de aplicación es tan diversa y tiene tantos dispositivos conectados al Internet (Cisco Systems, Reporte Anual de Ciberseguridad de Cisco 2018, 2018), por lo tanto, es fundamental prevenir y mitigar los ataques cibernéticos altamente técnicos y de bajo nivel de software y hardware existentes hacia la infraestructura del ISP.

Objetivos de la Investigación

Objetivo General

Analizar los ataques informáticos que afectan a un ISP Ecuatoriano, mediante el estudio de los datos de vulnerabilidades de tipo denegación de servicio, para mitigar el impacto ante nuevos incidentes de seguridad.

Objetivos Específicos

OE.1: Realizar un análisis de literatura de los tipos de vulnerabilidades DoS existentes.

OE.2: Implementar una solución de Business Intelligence que permita mitigar los ataques informáticos hacia la infraestructura del ISP.

OE.3: Evaluar los resultados para determinar si el modelo ayude a mitigar el impacto de los incidentes de seguridad.

Justificación, Importancia y Alcance

Este proyecto contribuye a mantener la disponibilidad del servicio, mejorar la protección de la infraestructura del ISP de las nuevas y crecientes amenazas a las que están expuestas actualmente y que han surgido de la mano con las nuevas tecnologías.

Una solución de Business Intelligence que garantice una estrategia corporativa de competitividad, optimización y productividad, analizará los datos de vulnerabilidades DoS, que no solo permitirá mitigar los ataques informáticos, sino transformar la información en conocimiento.

El modelo desarrollado permitirá analizar los datos históricos, identificar el tipo de vulnerabilidad DoS, servicios, dispositivos de infraestructura y aplicaciones afectadas, generando una solución de mitigación de DoS que combina soluciones de seguridad del servicio, seguridad cibernética e inteligencia de negocios.

Preguntas de Investigación

En el presente trabajo de investigación se formulan las siguientes preguntas relacionadas con los objetivos específicos, por cada uno de ellos, se establecen dos preguntas:
OE1-RQ1: En la actualidad, ¿cuáles son los estudios existentes sobre los tipos de vulnerabilidades DoS?
OE1-RQ2: ¿Cuáles son las técnicas que ocupan los ciberatacantes para la generación de DDoS?
OE2-RQ1: ¿Cuáles son las soluciones de Business Intelligence que permiten analizar las vulnerabilidades DoS y que mitiguen ataques informáticos en la actualidad?
OE2-RQ2: ¿Los datos históricos de vulnerabilidades DoS se podrán acoplar al algoritmo de inteligencia de negocios?

OE3-RQ1: ¿Cuáles son las acciones que se pueden tomar ante la detección de las amenazas?

OE3-RQ2: ¿Cuál es el nivel de confianza con el que se va a trabajar para el análisis de los resultados?

Hipótesis

El desarrollo de una solución de Business Intelligence que analice los datos de vulnerabilidades DoS permitirá mitigar los ataques informáticos hacia la infraestructura del ISP a corto, mediano o largo plazo.

Señalamiento de las Variables de la Hipótesis

Variable Dependiente (VD): El impacto de incidentes de seguridad.

Variable Independiente (VI): Análisis de vulnerabilidades del tipo denegación de servicio.

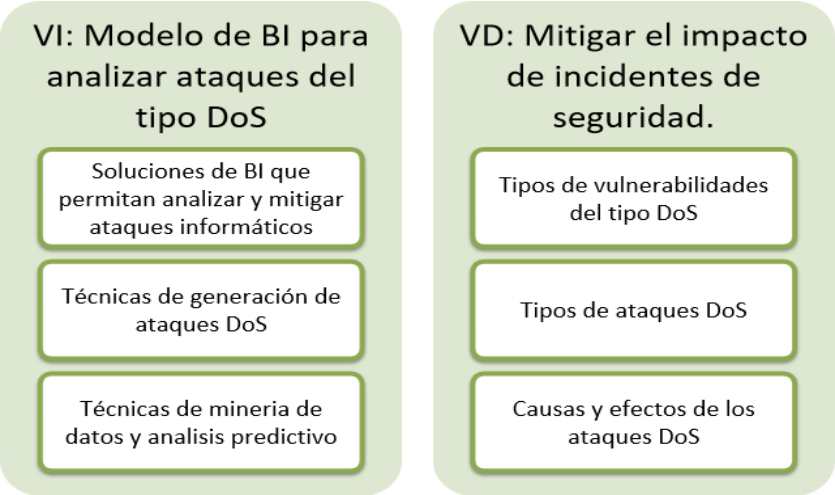
Capítulo II

Marco Teórico

La fundamentación teórica busca la congruencia con la hipótesis, para esto se realiza un análisis de la teoría usando las variables del problema como se muestra en la Figura 1, con la finalidad de investigar jerárquicamente cada categoría hasta llegar a la categoría que comprende y explica las variables dependientes e independientes del tema de estudio, para esto se propone la siguiente jerarquía de estudio:

Figura 1

Jerarquía de estudio



Nota. Representa las categorías de las variables independiente y dependiente

Fundamentación de la Variable Independiente

Inteligencia de Negocios

Se considera Business Intelligence (BI) como el método científico para resolver problemas de negocios, las herramientas tecnológicas y procesos, permiten gestionar los datos para obtener conocimientos que aporten satisfactoriamente al modelo de negocio de las organizaciones para la toma de decisiones en tiempo real, con criterios racionales, abarca la integración de datos, almacenamiento de datos y las herramientas de análisis e informes.

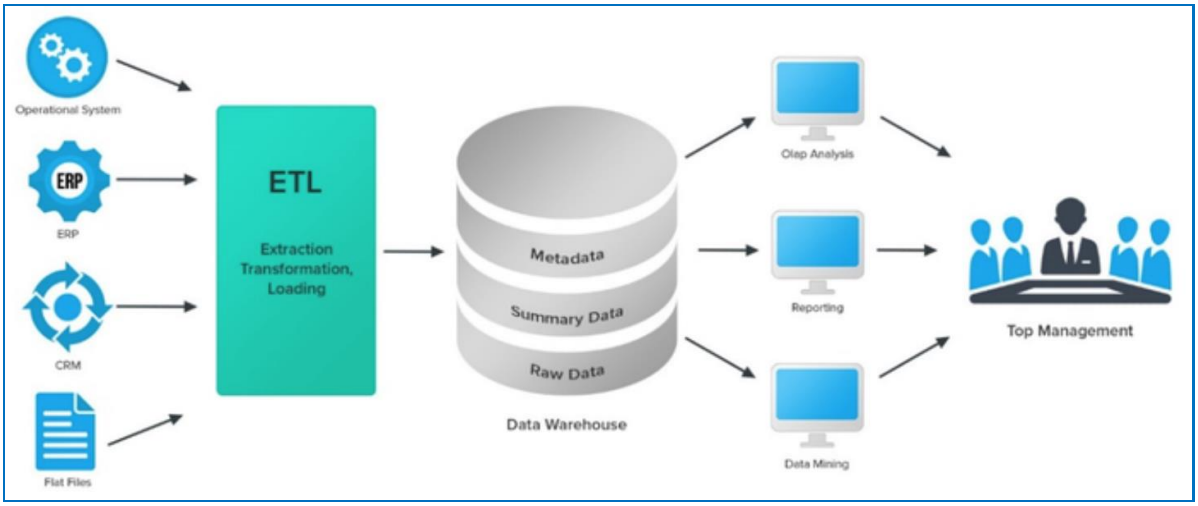
La explotación de información que genere volúmenes de datos son la base del negocio digital, es así que su uso se basa en el estudio, integración, depuración y el procesamiento de información para la toma de decisiones, se consideran como hitos históricos para la implementación de soluciones integrales en las empresas como instrumento esencial que genere valor en el capital financiero y humano (Wang, 2015).

Arquitectura de Business intelligence

Los sistemas tradicionales de BI utilizan una pequeña fracción de todos los datos disponibles. Los componentes centrales de la arquitectura de BI tradicional son: herramientas ETL, un almacén de datos empresarial con repositorio de metadatos y análisis empresarial, como se muestra en la Figura 2.

Figura 2

Arquitectura de Business Intelligence



Nota. Representa los componentes de DWH (Wayner, 2018)

Los sistemas de BI, utilizan herramientas ETL para extraer datos de múltiples fuentes y almacenar esos conjuntos de datos en un área de preparación temporal. Las organizaciones utilizan data warehouse para agregar datos estructurados y limpios.

Las herramientas de BI incluyen herramientas de informes empresariales, herramientas de consulta ad hoc, herramientas de análisis estadístico, herramientas OLAP[4], dashboards, scorecards y análisis avanzado. Los análisis avanzados se refieren a: herramientas de minería

[4] OLAP (Online Analytical Processing) Tecnología que se usa para administrar base de datos empresariales con procesamiento analito en línea, Inteligencia de negocios.

de datos, herramientas de minería de texto, análisis predictivo, inteligencia artificial y procesamiento de lenguaje natural.

Inteligencia de Negocios Ágil

Inteligencia de negocios ágil, es un proceso rápido, flexible y adaptable que incorpora metodologías, estructura organizacional, herramientas y tecnologías que permiten a los tomadores de decisiones estratégicos, tácticos y operativos ser más flexibles y más receptivos al rápido ritmo de cambios en los requisitos comerciales y regulatorios. (Muñoz, Osorio, & Zuñiga, 2016). Según el Data Warehousing Institute, el BI ágil "aborda una necesidad amplia de permitir la flexibilidad al acelerar el tiempo que lleva entregar valor con los proyectos de BI. Puede incluir opciones de implementación de tecnología como BI de autoservicio, BI basado en la nube y paneles de control de descubrimiento de datos que permiten a los usuarios comenzar a trabajar con datos más rápidamente y adaptarse a las necesidades cambiantes" (Tovar, 2017). En conclusión, una solución de ágil BI debe proporcionar acceso a información precisa en el formato correcto a la persona adecuada en el momento adecuado. A continuación, se identifican los componentes clave que demuestran una solución de BI ágil: desarrollo ágil, análisis empresarial ágil e infraestructura de información ágil.

Proveedor de servicios de Internet

Mantener a los usuarios de Internet protegidos de los ciberataques y otras amenazas es uno de los desafíos de seguridad de un proveedor de servicios de Internet (ISP) de ofrecer a sus clientes. Para contrarrestar las amenazas como: pérdidas de reputación por parte de los clientes hacia el ISP y pérdidas económicas, el ISP debe prepararse ante cualquier escenario y tomar las medidas necesarias para prevenir que su infraestructura sea víctima de estos ataques.

Por ejemplo, existen diferentes escenarios que los ciberatacantes pretenden colapsar la red como: saturación de servicios online, mediante la inundación de peticiones y el

aprovechamiento de vulnerabilidades de programas o servicios, que dejan de funcionar de forma total o parcial, los atacantes usan una gran variedad de técnicas y herramientas que les permita ocultar su identidad, por lo que resulta imposible capturar a los responsables.

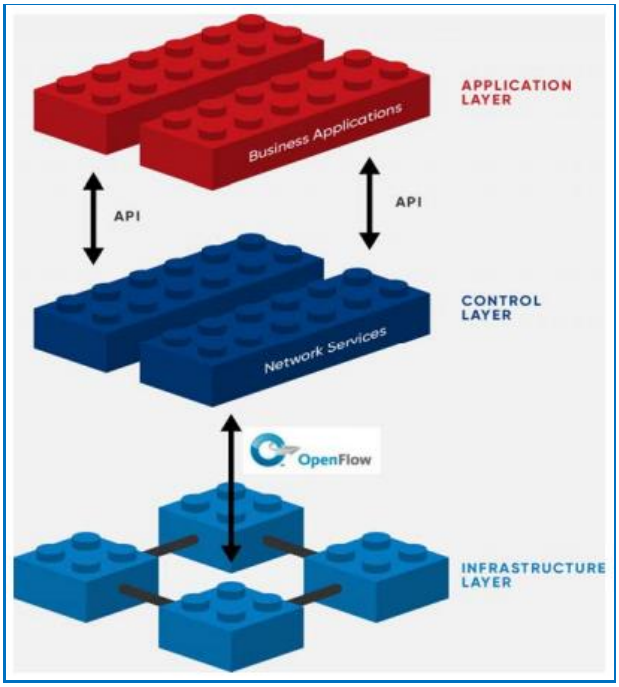
Redes definidas por software

Software defined networking (SDN) son una arquitectura de red ágil que describe un enfoque en el que las redes utilizan controladores basados en software, interfaces de programación de aplicaciones para dirigir el tráfico en la red y comunicarse con la infraestructura de hardware subyacente (Pachés, 2020).

La tecnología SDN se basa en la separación del plano de control, es decir la red de inteligencia, del plano de datos que es el reenvío de paquetes como se ve muestra a continuación:

Figura 3

Arquitectura SDN



Nota. En este trabajo se considera esta arquitectura SDN (Pachés, 2020)

Esta arquitectura es distinta al de las redes tradicionales que utilizan dispositivos de hardware dedicados como enrutadores y switchs para controlar el tráfico en la red. Una SDN de hardware puede ser manejada mediante el software para crear y controlar dicha red virtual y el enrutamiento de los paquetes de datos mediante un servidor centralizado.

El plano de control está supervisado por un controlador centralizado que toma todas las decisiones de reenvío de flujo en la red, la comunicación entre los dos planos es analizado a través del protocolo OpenFlow[5]. Como fases de prueba en una SDN se puede desplegar toda una infraestructura con el uso de un software virtualizado mininet[6] para emular su rendimiento cuando se implementa en la red real. (Cueto Altahona, 2019).

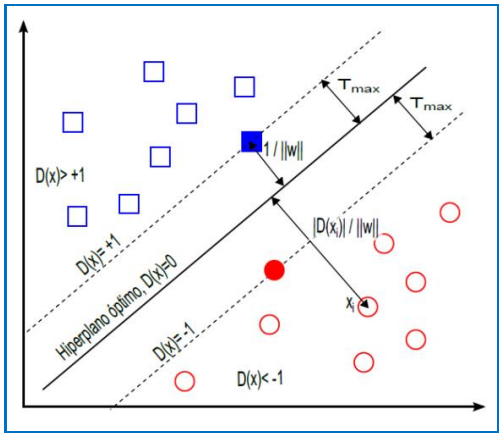
Máquina de vectores de soporte

Support Vector Machine (SVM) es una técnica de clasificación basada en algoritmo de aprendizaje automático, implica el trazado de datos como puntos en un espacio n-dimensional, donde 'n' denota el número de características, representa los puntos de muestreo en el espacio, separando las clases a dos espacios lo más amplios posibles mediante un hiperplano, en el cual las dos clases más cercanos se llama vector soporte que es el vector entre los dos puntos. El modelo construido por SVM es capaz de predecir si un punto nuevo pertenece a una clase o a otra (Campo, 2018).

[5] OpenFlow es un protocolo abierto de comunicaciones que permite a un servidor de software determina por donde renviar paquetes.
[6] Mininet es un emulador para el despliegue de redes definidas por software.

Figura 4

Grafica de máquina de vectores de soporte



Nota. Representa el margen de un hiperplano de un SVM (Campo, 2018)

Los ataques de denegación de servicio distribuido DDoS, son un tipo de ataque informático cuyo objetico es reducir o anular la capacidad de los servidores o recursos informáticos de ofrecer su servicio. Es decir, viola o afecta la propiedad de disponibilidad que todo sistema debe poseer (INCIBE-CERT, 2020).

Los ataques pueden colapsar a un servidor donde la cantidad de paquetes que se envían para crear la interrupción de un servicio a usuarios legítimos privando a organizaciones de los servicios informáticos indispensables, como el acceso a Internet, servicios de correo electrónico que están alojados en las instalaciones o en la nube (Sims J. S., 2017).

Los ataques de denegación de servicios se han desarrollado y ejecutado sobre todas las capas del modelo OSI[7], empezando por ataques en la capa de red hasta la capa de aplicaciones, esta diversidad de ataques en las diferentes capas del modelo OSI incrementa la capacidad de detectar ataques (Gupta, 2013).

Fundamentación de la Variable Dependiente

[7] OSI (Open System Interconnection) es el modelo de referencia para los protocolos de la red conformado por 7 capas o niveles.

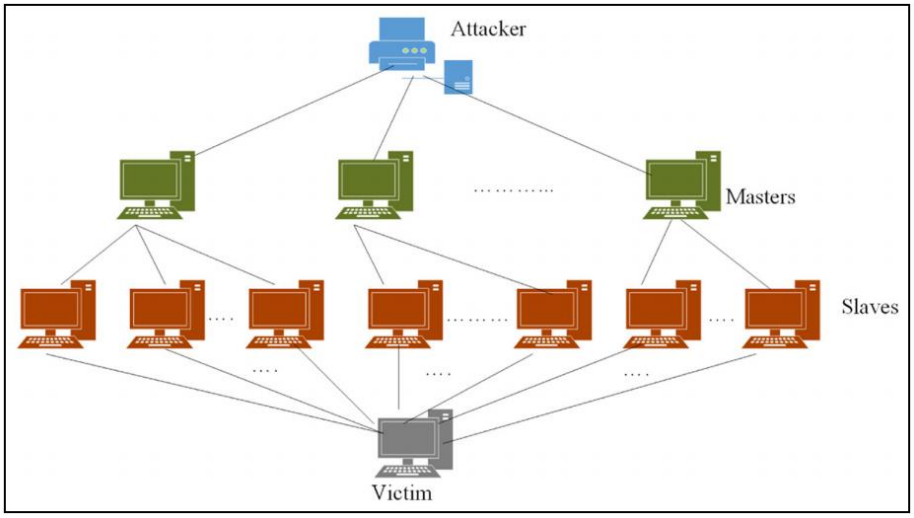
Ataques DDoS

Los ataques DDoS tiene como objetivo inundar una red con una gran cantidad de paquetes desde varios destinos. Los ataques DDoS pueden inundar la red de la víctima en varias formas: TCP, UDP, ataque de inundación ICMP, inundación de IP aleatoria y el uso de redes de botnets.

Un bot es un intruso que toma el control de una dispositivo o computadora en la infraestructura de una red. En general, en un ataque DDoS, un atacante comienza explotando una vulnerabilidad en un sistema informático, convirtiéndolo en el bot maestro DDoS. El sistema atacante principal identifica otros sistemas vulnerables y obtiene el control sobre ellos ya sea infectando los sistemas con malware o evitando los controles de autenticación denominados bots esclavos DDoS, para que el atacante crea un servidor de comando para controlar la red de bots, conocida como botnet. El atacante usa el tráfico generado por los dispositivos comprometidos para inundar el objetivo y hacer que sus servicios caigan como se muestra en la estructura de un ataque DDoS (Tasnuva Mahjabin, 2020).

Figura 5

Estructura de un ataque DDoS



Nota. Representa un ataque DDoS en una red (Graham-Cumming, 2014)

Las razones o motivos detrás de los ataques DDoS pueden ser específicos. Pero, en general, las principales causas de los ataques DDoS son las siguientes:

- Competencia: los ataques DDoS pueden estar destinados a paralizar las operaciones de una empresa, dañar la reputación que pueden beneficiar directamente a los competidores y generar pérdidas económicas a la víctima.
- Ganancias financieras: los ataques DDoS pueden utilizarse para lograr ganancias financieras. Los atacantes pueden ser contratado, bien pagado o incluso pueden pedir rescate.
- Política: los ataques DDoS tienen el potencial de silenciar digitalmente a los partidos de la oposición. Pueden ser utilizado por partidos políticos y terroristas.
- Venganza: empleados actuales, ex empleados, clientes enojados o cualquier persona con una disputa puede tener un motivo para un ataque DDoS (Tasnuva Mahjabin, 2020).

Tipos de ataques DDoS

Los ataques de denegación de servicios distribuidos se clasifican en: ataques volumétricos, ataques basados en protocolos y ataques basados en capas de aplicación. Los ataques basados volumétricos se concentran en enviar grandes cantidades de tráfico, generalmente medidos en Gigabits por segundo (Gbps), para saturar el ancho de banda de la víctima, estos no requieren gran conocimiento o habilidad y son los más comunes. En la siguiente tabla, se muestra la clasificación detallada de los ataques DDoS (Isha, 2013).

Tabla 1

Clasificación de ataques distribuidos de denegación de servicios DDoS

Categoría de ataque DDoS	Ataque	
Ataque basado en volumen	Inundación	ICMP
		UDP
	Amplificación	DNS
		NTP
Ataque basado en protocolo	Inundación TCP SYN	
	Inundación HTTP	
	Ping de la muerte	
Ataque basado en la capa de aplicación	Zero-day	
	Slowloris	

Nota. Tomado en resumen de (Isha, 2013)

Ataques basados en volumen

La finalidad de este tipo de ataques es generar enormes volúmenes de tráfico saturando el ancho de banda y cortando el tráfico legítimo de entrada y salida, es decir, los usuarios pierden acceso a sus aplicaciones o servicios, la interrupción del tráfico legítimo significa que usuarios no puedan ejecutar transacciones en línea, bloquear el acceso de usuarios a un servicio online con impactos negativos.

Los ataques volumétricos utilizan botnets creados y controlados por los atacantes de forma individual en los dispositivos infectados con malware. Los bots, se utilizan para provocar el colapso de la red, en general con tráfico malintencionado que satura todo el ancho de banda disponible, los bots asumen el control de dispositivos legítimos para amplificar los ataques DDoS que consumen un gran ancho de banda, normalmente sin que los usuarios se percaten

de ello, es difícil para la organización detectar el tráfico malintencionado (K. Mallikarjunan Narasimha, 2016).

Ataque basado en protocolo

Los protocolos en Internet se basan en conjuntos de reglas para el intercambio de información en una comunicación de red, dichas reglas pueden ser explotadas de forma indebida por un atacante que intenta abrumar y agotar la capacidad informática de diversos recursos de la infraestructura de red, como servidores o firewalls, a través de solicitudes que vulneren las comunicaciones del protocolo (US-CERT, 2021).

Ataque basado en la capa de aplicación

Los ataques a la capa de aplicación o ataques DDoS de capa 7 hacen referencia al comportamiento malintencionado para dirigirse a la capa de 7 del modelo OSI, donde se producen las solicitudes comunes de Internet como HTTP GET y HTTP POST y están dirigidos a consumir recursos del servidor y de la red (Graham-Cumming, 2014).

Mecanismos de defensa ante ataques DDoS

Existen múltiples técnicas de defensa ante intentos de ataques de denegación de servicio distribuidos que se pueden clasificar según el momento del proceso de intrusión en que actúan. A continuación, se resumen brevemente algunos tipos de mecanismos de defensa:

Prevención de ataques DDoS

Como mecanismos de prevención se entiende a aquellos que actúan antes de que el ataque suceda e independientemente de su detección. Su propósito es minimizar el impacto causado por los atacantes, cuanto menos expuestos estén los servicios, sistemas y equipos, menores serán las oportunidades de que sean atacados.

Detección de ataques DDoS

Para la detección de los ataques es importante que actúen todos los elementos defensivos. Su eficacia depende de la proporción de ataques reales que son capaces de

detectar sin fallar. La mayor parte de trabajos de investigación opta por el desarrollo de sistemas basados en el estudio de anomalías porque el sistema de detección de patrones dificulta la detección de nuevas amenazas. El reconocimiento de anomalía simplifica el modelado del comportamiento habitual y legítimo de un sistema, con el fin de identificar eventos que difieran de las acciones legítimas. De este tipo de detecciones han sido propuestas diferentes técnicas que se describen a continuación:

Se propone utilizar diversas medidas de la capa 4 en el nivel de red (TCP/IP) con el objetivo de detectar ataques en el borde de la red y clasificarlos mediante el uso de una red neuronal. Para lograr esto, se lleva a cabo un proceso de aprendizaje automático en el cual se entrena a una red neuronal multicapa utilizando estadísticas recolectadas, específicamente diseñada para detectar ataques basados en el tráfico UDP (Siaterlis & Maglaris, 2010).

Además, se emplea la teoría del caos para identificar diferencias entre el tráfico legítimo y el malicioso. Se observa que el tráfico generado por un ataque sigue un patrón específico, lo que permite desarrollar un algoritmo capaz de detectar ataques y proporcionar una estimación aproximada de su inicio (Chonka, Jaipal, & Zhou, 2013).

Se utilizan técnicas de inteligencia artificial para identificar ataques. En este proceso, se recopila el tráfico y se emplea una red neuronal como sistema de detección. Las pruebas envían los datos a un servidor central, el cual analiza los datos recibidos y genera filtros y herramientas para facilitar la detección de los ataques (Seufert & O'Brien, 2011).

Identificación de ataques DDoS

Durante el proceso de determinar el origen del ataque, la persona afectada intenta desvelar la ruta tomada por el atacante para poder identificar al responsable. Sin embargo, esto suele resultar muy difícil en la mayoría de los casos, ya que el atacante utiliza diversas técnicas para ocultar su rastro. Estas técnicas incluyen una variedad de métodos de suplantación de identidad y el uso de redes anónimas. Por lo tanto, lograr identificar todo el recorrido hasta llegar al responsable es una situación ideal que rara vez se consigue.

Mitigación de defensa ante ataques DDoS

Posterior a determinar la existencia de una amenaza, es necesario llevar a cabo acciones para reducir su impacto, lo cual implica implementar una serie de medidas y técnicas destinadas a disminuir los daños ocasionados y, si es posible, restaurar los servicios del sistema afectado. A continuación, se mencionan diversas soluciones y enfoques de mitigación propuestos por diferentes autores.:

Se propone una estrategia en los Routers de borde que posibilita la detección de direcciones IP de origen falsificadas, con el fin de determinar la validez del segmento TCP SYN-ACK. Para lograr esto, se utiliza una tabla de estados que establece la relación entre los segmentos TCP SYN y los SYN-ACK. Si un segmento SYN-ACK no es considerado válido, el Router borde reinicia la conexión TCP. Esto tiene como resultado la liberación de la cola de solicitudes del servidor, conocida como Backlog Queue, permitiendo al servidor atender a clientes legítimos (Giralte & Conde, 2013).

Se presentan dos sistemas de protección perimetral para los Proveedores de Servicios de Internet (ISPs) que no requieren intervención en los routers externos o internos del ISP. Estos sistemas permiten bloquear ataques mediante la colaboración de los routers de borde, los cuales identifican los flujos de los atacantes y aplican limitación de velocidad, bloqueo de puertos o nodos comprometidos. En caso de un ataque, se conecta un nuevo nodo de respaldo en la ubicación del nodo atacado (Chen & Song, 2012).

En los próximos capítulos se describirá el proceso completo de un mecanismo de defensa contra ataques de denegación de servicio, utilizando una arquitectura SDN y aprovechando las funcionalidades propuestas por los autores Stefanet, Siaterlis en la detección y Chen para la mitigación. Este enfoque se basa en el uso de algoritmos basados en Maquinas de Vectores de Soporte (SVM) para la detección y mitigación de estos ataques.

Estado del arte

Para realizar el estado del arte se empleó la técnica de revisión sistemática de literatura, iniciamos con analizar el problema definido en el planteamiento del problema, los criterios de inclusión y exclusión; seguidos por la estrategia de búsqueda.

El enfoque estará dado para encontrar estudio relacionados con la investigación que necesitamos, quiere decir que según el resultado del estado del arte se determinan las propuestas necesarias para identificar la mejor alternativa de solución justificada por los estudios identificados.

Definición del objetivo

Identificar en la literatura científica las propuestas relacionadas que permitan proponer e implementar la metodología y herramienta apropiada de inteligencia de negocios que ayude a mejorar la toma de decisiones gerenciales antes ataques del tipo DDoS.

Definición de los criterios de inclusión y exclusión

Definición de los criterios de inclusión y exclusión: Las búsquedas en las bases digitales dependiendo del tema retornan una gran cantidad de artículos relacionados por lo cual es importante definir las características idóneas de los artículos a ser tomados en cuenta, para el presente análisis, se tomaron en cuenta los siguientes criterios:

Criterios de Inclusión

- Con el fin de analizar metodologías utilizadas en la actualidad, se tomarán en cuenta artículos a partir del 2014.
- Se tomaron en cuenta solamente artículos científicos publicados en el idioma inglés.
- Artículos que contengan información referente al uso de metodologías de inteligencia de negocios para sistemas aplicados al análisis de datos de vulnerabilidades del tipo denegación de servicio.

Se tomarán en cuenta mayormente artículos científicos y documentos de conferencias.

- Criterios de Exclusión
- Artículos que tengan temas de inteligencia de negocios no relacionados con el análisis de datos de vulnerabilidades del tipo denegación de servicio.
- Artículos que no estén en el idioma inglés.
- Grupo de control

El grupo de control está conformado por estudios que cumplen con los criterios de inclusión y exclusión, para lo cual se inicia con un análisis del título de los estudios, su introducción, conclusiones y palabras claves. Los estudios que son seleccionados para el grupo de control son los siguientes:

Tabla 2

Listado de artículos del Grupo de control

Grupo de Control	Titulo	Palabras Clave
EC1	Cloud Computing Vulnerability: DDoS as its main Security Threat, and Analysis of IDS as a Solution Model	Cloud, DDoS, IDS, Security, Vulnerability, ISP
EC2	A survey of Distributed Denial of Service attack	DDoS, Botnets, UDP, TCP, Server, Resources
EC3	An Adversary-Centric Behavior Modeling of DDoS Attacks	DDoS, Computer crime, Analytical models, Feature extraction, Predictive models, Malware, ISP

Grupo de Control	Titulo	Palabras Clave
EC4	DDoS Attack Detection and Mitigation Techniques in Cloud Computing Environment	Cloud computing, DDoS, Detection, Mitigation, Security, Vulnerability
EC5	A Novel Algorithm for DoS and DDoS attack detection in Internet Of Things	Internet of Things, Security, DoS, DDoS, Constrained
EC6	A New Machine Learning-based Collaborative DDoS Mitigation Mechanism in Software-Defined Network	DDoS attacks, SDN, Machine Learning, Security
EC7	FlowTrApp: An SDN Based Architecture for DDoS Attack Detection and Mitigation in Data Centers	DDoS, SDN, Data Center, sFlow-RT, OpenFlow
EC8	Feature dynamic deep learning approach for DDoS mitigation within the ISP domain	IoT, DDoS mitigation, Deep learning, SOM, Network security, Cyber security, Machine learning attacks, ISP, Self organizing map
EC9	Unsupervised learning with hierarchical	DDoS mitigation, cyber security, Internet service providers (ISP), mitigations

Grupo de Control	Titulo	Palabras Clave
	feature selection for DDoS mitigation within the ISP domain	
EC10	A lightweight DDoS attack mitigation system within the ISP domain utilising self-organizing map	Artificial Neural Network, DDoS attack, ISP, Machine learning, Intrusion detection, Security

Construcción de la cadena de búsqueda

En la elaboración de la cadena de búsqueda, se usan las palabras que más se repiten en cada contexto definido a partir de los estudios del grupo de control como se describe en la Tabla 3.

Tabla 3

Construcción de la cadena de búsqueda

PALABRA CLAVE	EC1	EC2	EC3	EC4	EC5	EC6	EC7	EC8	EC9	EC10	NUMERO DE REPETICIONES
DDoS	X	X	X	X	X	X	X	X	X	X	8
Detection				X						X	2
Mitigation				X		X		X	X		4
Security	X			X				X	X	X	4
Vulnerability	X			X				X		X	3
IOT(Internet of Things)					X			X			2
Attacks								X		X	2

PALABRA CLAVE	EC1	EC2	EC3	EC4	EC5	EC6	EC7	EC8	EC9	EC10	NUMERO DE REPETICIONES
SDN						X	X				2
ISP								X	X	X	3

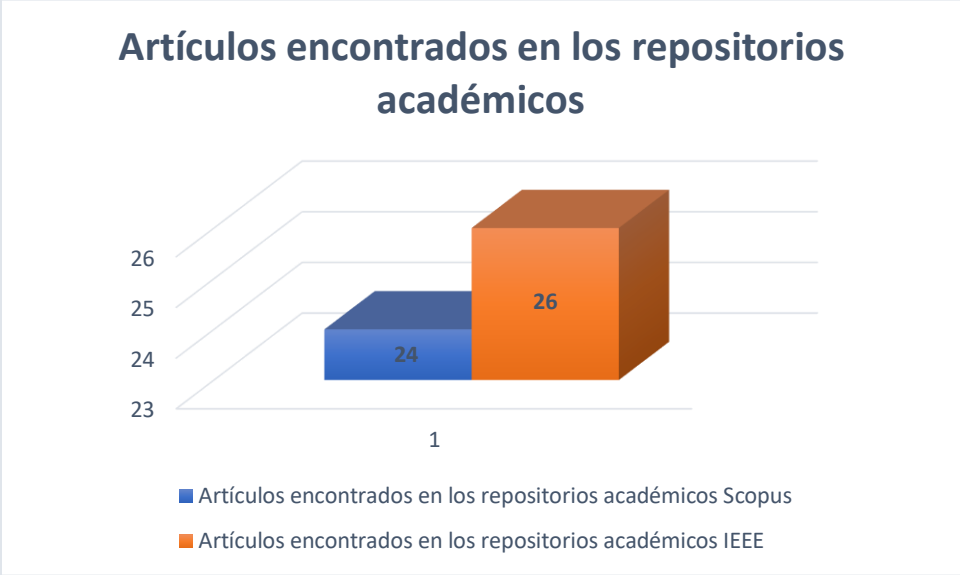
La cadena de búsqueda está estructurada por la unión de las palabras claves que más se repiten en cada contexto, los conectores usados son OR para las palabras que están dentro del mismo contexto y el conector AND para las palabras que están en contextos distintos, de esta manera se establece la siguiente cadena de búsqueda.

((DDoS)OR(Security)OR(Vulnerability))AND(Mitigation)AND(ISP)

Una vez armada la cadena de búsqueda se procede a aplicar la cadena de búsqueda en los repositorios académicos seleccionados para el estudio, para esto se procede a filtrar solo los documentos que estén en el idioma inglés, cuya fecha de publicación sea mayor al 2014 y que sean artículos científicos o documentos de conferencias, a continuación, se obtienen los siguientes resultados.

Figura 6

Artículos encontrados en los repositorios académicos



Nota. Resultado de la cadena de búsqueda obtenida de las bases digitales

Selección de estudios

De los estudios candidatos se detalla 26 artículos de la librería IEEE y 24 de Scopus, se realizó la lectura de los artículos, palabras claves y abstract, tomando en cuenta criterios de inclusión y exclusión se obtienen los 10 estudios candidatos.

Tabla 4

Resumen de estudios candidatos

Cantidad	Rechazados	Aceptados	Motivo
50	40	10	Titulos, palabras clave y abstract no cumplen con los criterios de inclusión y exclusion

Estudios primarios

De los resultados de los estudios candidatos, se descartan 4 artículos que no ayudarían a dar respuesta a las preguntas de investigación, de esta manera se seleccionan 6 artículos como estudios primarios cuyos títulos están relacionados con el tema de investigación.

Tabla 5

Estudios primarios

Estudios
A lightweight DDoS attack mitigation system within the ISP domain utilising self-organizing map
Unsupervised learning with hierarchical feature selection for DDoS mitigation within the ISP domain
Feature dynamic deep learning approach for DDoS mitigation within the ISP domain
A survey of Distributed Denial of Service attack
An Adversary-Centric Behavior Modeling of DDoS Attacks

Nota: Esta tabla muestra el listado de los estudios seleccionados para dar respuesta a las preguntas de investigación

Extracción de la información

Una vez obtenidos los resultados se realizó la revisión de los documentos encontrados los cuales se listan a continuación:

A lightweight DDoS attack mitigation system within the ISP domain utilising self-organizing map (Chambers & Barrett, 2018)

El presente estudio propone un sistema de mitigación de ataques DDoS que utiliza un algoritmo de mapa autoorganizado para clasificar los datos de flujo de red casi en tiempo real recopilados por el ISP. La mayoría de los enfoques actuales ofrecen detección y mitigación centralizadas. Sin embargo, pocas propuestas se centran en implementar sistemas de defensa y mitigación DDoS dentro del dominio del ISP, que tiene el potencial de proporcionar soluciones escalables y distribuidas para estos ataques cuyo objetivo principal es privar a los usuarios de los servicios de red agotando el ancho de banda o los recursos de hardware de la víctima.

Unsupervised learning with hierarchical feature selection for DDoS mitigation within the ISP domain (Ili, Desmond, & Barrett, 2019)

La presente investigación desarrolla mejores sistemas de mitigación de DDoS en comparación con la mayoría de los modelos existentes que proporcionan soluciones centralizadas, ya sea mediante la implementación del sistema con servidores adicionales en el sitio host, en la nube o en ubicaciones de terceros, lo que puede causar latencia. Dado que los proveedores de servicios de Internet (ISP) usan enlaces entre el Internet y los usuarios, la implementación del sistema de defensa dentro del dominio de ISP es la panacea para ofrecer una solución eficiente. Para hacer frente a la naturaleza dinámica de los nuevos ataques DDoS, utiliza una red neuronal artificial sin supervisión para desarrollar un mapa jerárquico de autoorganización de dos capas equipado con una doble selección de características para la mitigación DDoS dentro del dominio ISP.

Feature dynamic deep learning approach for DDoS mitigation within the ISP domain (Barrett, Ili, & Desmond, 2019)

En el documento el autor tiene como propósito explicar los tipos de ataques DDoS, su impacto y mitigación, propone un enfoque dinámico de aprendizaje profundo que utiliza datos de la red recopilados por el ISP para combatir la naturaleza dinámica de los nuevos ataques DDoS. Muchos investigadores se esfuerzan por desarrollar sistemas de mitigación para mantenerse al día con las crecientes amenazas de seguridad. No obstante, la mayoría de los modelos presentados ofrecen soluciones ineficientes, ya sea mediante el uso de servidores auxiliares en el sitio host, en la nube o en centros de depuración de datos dedicados. Dado que los proveedores de servicios de Internet (ISP) conectan Internet con los usuarios, el sistema de mitigación debe implementarse dentro del dominio del ISP para ofrecer una solución más eficiente.

A survey of Distributed Denial of Service attack (Narasimha & Mercy, 2016)

Este artículo presenta una descripción general del estado del arte en las estrategias de detección de ataques DDoS, que pueden ser usados para agrandar el ataque en caso de denegación de servicio distribuida para que el efecto del ataque sea alto. Los ataques distribuidos de denegación de servicio tienen como objetivo agotar la comunicación y el poder computacional de la red al inundar los paquetes a través de la red y generar tráfico malicioso en la red. Para ser un servicio eficaz, el ataque DDoS debe detectarse y mitigarse rápidamente antes de que el usuario legítimo acceda al objetivo del atacante. La seguridad de la información se ocupa de una gran cantidad de temas como la detección de mensajes falsos, el procesamiento de audio, la vigilancia por video y las detecciones de ataques cibernéticos. Los sistemas interconectados, como el servidor de bases de datos, el servidor web, los servidores de computación en la nube, etc., ahora están bajo hilos de atacantes de red. La denegación de servicio es un ataque común en Internet que causa problemas tanto para el usuario como para los proveedores de servicios.

An Adversary-Centric Behavior Modeling of DDoS Attacks (An, Aziz, & Songqing, 2017)

En este documento, se adopta un enfoque basado en el análisis de los datos que contempla diseñar y validar tres modelos de ataque DDoS, desde la perspectiva temporal; es decir, magnitudes de ataque, espaciales respecto al origen del atacante y espacio-temporales que evidencia el tiempo de lanzamiento de ataque. Se diseña los modelos basados en el análisis de trazas que consisten en más de 50,000 ataques DDoS, analizados desde las operaciones de mitigación industrial. Cada modelo también se valida probando su efectividad para predecir con precisión futuros ataques DDoS. Las comparaciones con modelos intuitivos simples muestran que nuestros modelos pueden capturar con mayor precisión las características esenciales de los ataques DDoS.

La técnica sobre el análisis del comportamiento de los atacantes a menudo se divide en dos aspectos: supone que los adversarios son estáticos y hace ciertas suposiciones simplificadoras sobre su comportamiento, que a menudo no son compatibles con los datos

reales del ataque, esto puede proporcionar información para revelar patrones y estrategias utilizadas por los atacantes.

Resultados de la revisión

Después de completar el análisis de los artículos principales, se recopiló la información necesaria para abordar las preguntas de investigación que se detallan a continuación:

Para responder a la pregunta OE1-RQ1: Hay varios estudios sobre vulnerabilidades DDoS, los cuales se pueden clasificar según las capas del modelo de interconexión de sistemas abiertos (OSI). Estas vulnerabilidades son más comunes en las capas de red, transporte, presentación y aplicación, según se presenta en los estudios realizados en (Ili, Desmond, & Barrett, 2019) y (Narasimha & Mercy, 2016).

Según (Chambers & Barrett, 2018) y (An, Aziz, & Songqing, 2017) en el caso de OE1-RQ2, se señala que los atacantes emplean una estrategia en la cual generan una gran cantidad de paquetes o solicitudes con el fin de sobrecargar el sistema objetivo. Esta técnica se basa en utilizar múltiples fuentes vulnerables o controladas para llevar a cabo el ataque. Algunos de los vectores de ataque más comúnmente utilizados incluyen el uso de botnets en la capa de red, así como las inundaciones SYN y UDP.

Conclusión del estado del arte

Al realizar la revisión de literatura se identifica que todos los servicios en la nube dependen de la infraestructura de un ISP, quien debe garantizar la seguridad y privacidad de los datos a sus usuarios, una detección en tiempo real de los ataques de denegación de servicio distribuido (DDoS) en la red y un método de control basado en la tecnología de mitigación puede garantizar un control total de las vulnerabilidades.

Es por este motivo que para mitigar los ataques del tipo DDoS hacia la infraestructura de un ISP de Ecuador, se describe la implementación de una solución de inteligencia de negocios que permita analizar la información histórica de los datos de las vulnerabilidades y permita mitigar la naturaleza dinámica de los nuevos ataques DDoS.

Capítulo III

Metodología de Investigación

En el presente capítulo, se describe la metodología a usarcé basada en técnicas y procedimientos bien estructurados que nos proporcionará un adecuado desarrollo de las actividades, a continuación, se describen las metodologías a usar para el cumplimiento de los objetivos planteados en este trabajo.

Metodología de Ralph Kimball

Esta metodología se basa en lo que Kimball denomina Ciclo de Vida Dimensional del Negocio Business (Kimball, 2008). Este ciclo de vida del proyecto se emplea para la construcción de un Data Warehouse como una colección de datos de un determinado ámbito, se basa en los siguientes principios:

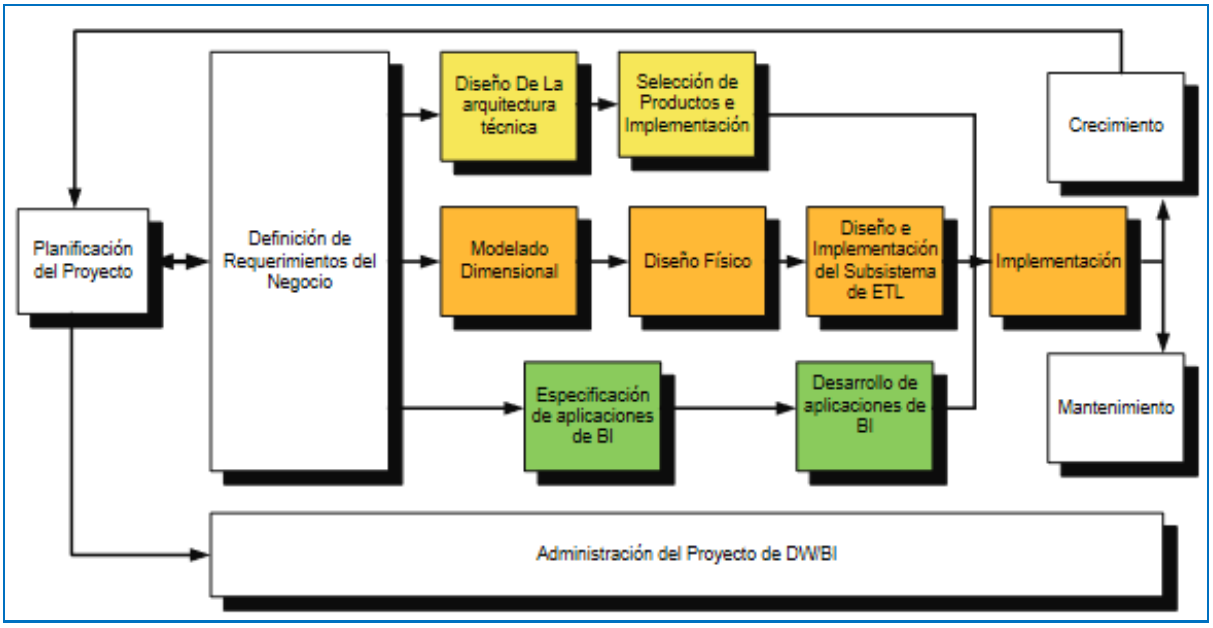
- Enfocarse en el negocio: Se concentra en la identificación de los requerimientos del negocio por ser el núcleo del ciclo de vida del Data Warehouse para el proyecto.
- Construir una infraestructura de información adecuada: Se describe el diseño de una base de información única, para cumplir con los requisitos que sea fácil de usar, integra y de alto rendimiento.
- Realizar entregas en incrementos significativos: Se crea el Data Warehouse en incrementos entregables en plazos de 6 a 12 meses, acorde con la metodología ágil de BI.
- Ofrecer la solución completa: Se proporciona los elementos necesarios para entregar valor a los usuarios de negocios. Para ofrecer un Data Warehouse sólido, bien diseñado y accesible, incluyendo herramientas de consulta con la herramienta de inteligencia de negocios, aplicaciones para informes y análisis avanzado, capacitación, soporte y documentación.

El enfoque que representa el ciclo de vida del Data Warehouse (Kimball, 2008) se describe en la Figura ***7***, donde se resalta el rol principal de la tarea de definición de requerimientos que son el soporte inicial de las tareas subsiguientes y su influencia en la planificación del proyecto. A continuación, se muestra las tres rutas que se enfocan en:

- Tecnología: Donde muestra el camino superior que implica tareas relacionadas con software específico.
- Datos: Muestra el camino del medio con tareas que se encargaran del diseño del modelo dimensional y el subsistema de Extracción, Transformación y Carga ETL en el Data Warehouse.
- Aplicaciones de Inteligencia de Negocios: El camino inferior, muestra la ruta con tareas que se diseñan y desarrollan las aplicaciones de negocios para los usuarios finales, estas rutas se combinan cuando se instale el sistema.

Figura 7

Metodología de Kimball



Nota. Representa la metodología de Kimbal y sus procesos (Kimball, 2008)

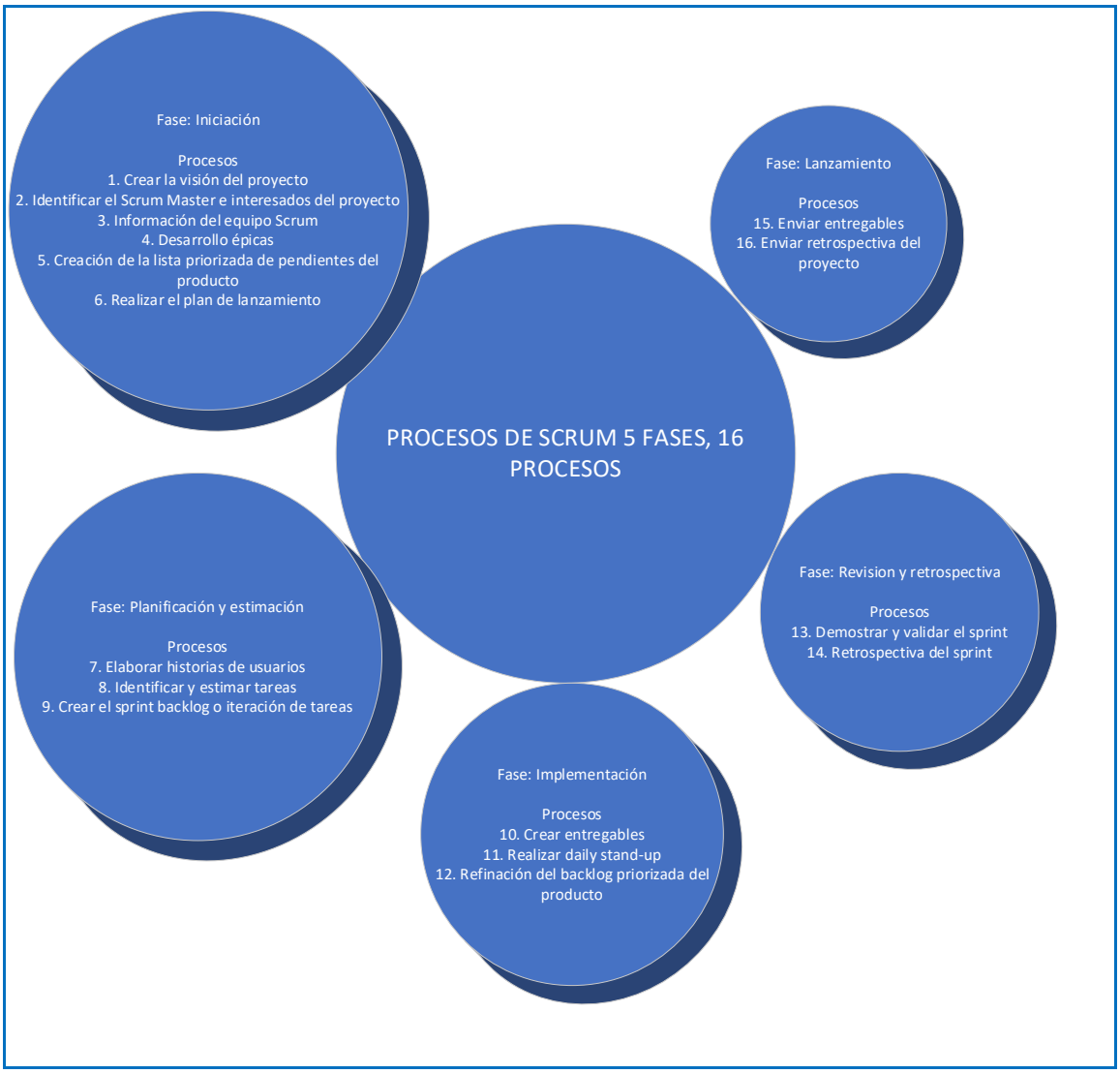
Metodología Scrum

El desarrollo de las metodologías agiles abarcan métodos para la gestión de proyectos de forma rápida y flexible, scrum contempla diferentes procesos y técnicas para obtener mejores resultados con entregas parciales para obtener resultados con prontitud, donde la innovación, flexibilidad y productividad son fundamentales para el soporte y gestión de este proyecto de BI.

Los procesos scrum contempla roles, eventos y fases que se cumplirán con el equipo de desarrollo que define tareas necesarias para conseguir el Srpint. A continuación, se representa las fases de la metodología scrum.

Figura 8

Fases de la metodología Scrum



Nota. Representa las fases y sprint de la metodología scrum

Metodología

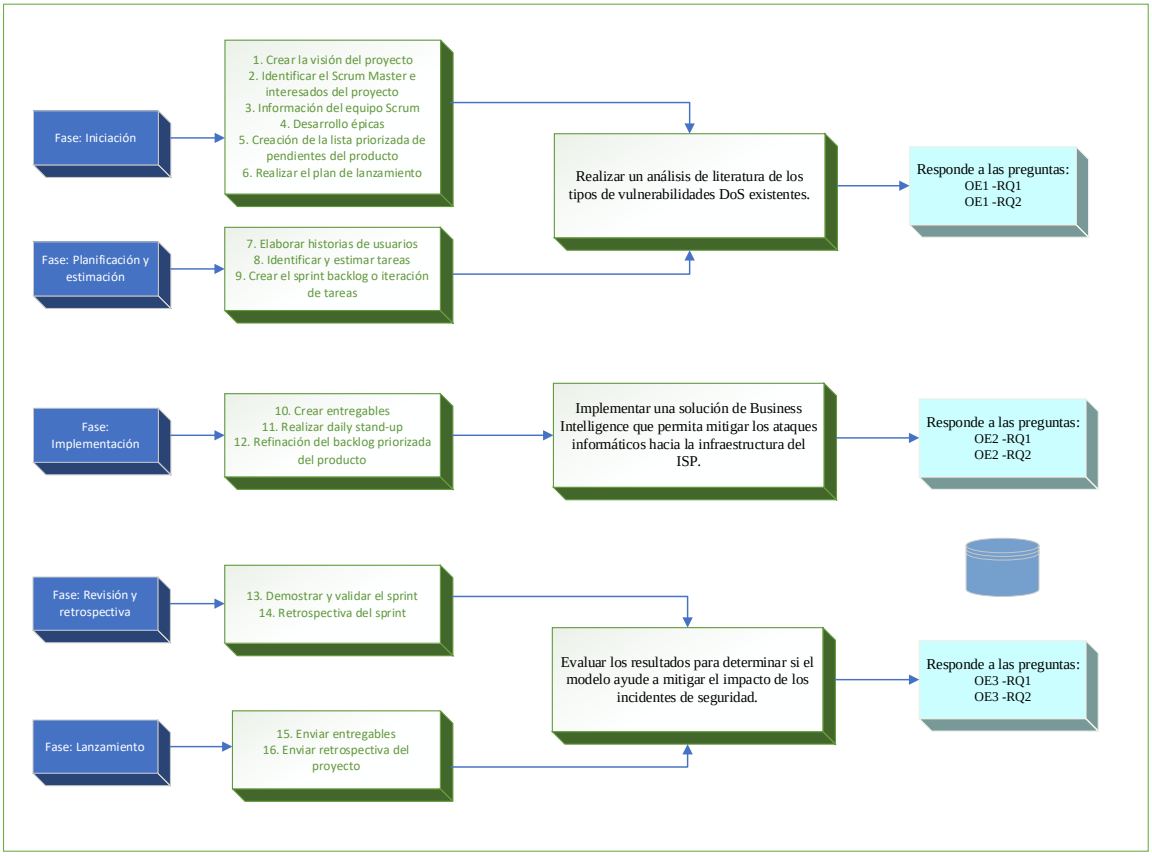
Las metodologías descritas definen los procesos, propósito y alcance, que constituyen una secuencia de actividades para producir un resultado que debe ser probado, en el estudio se describe las fases de la metodológica ágil Scrum y la metodología de Ralph Kimball en la implementación del diseño y desarrollo del modelo, forma la solución de la herramienta de

inteligencia de negocios que permita mitigar ataques de denegación de servicios en la infraestructura del ISP.

Se usará un método cuantitativo en el cual con el análisis de la situación actual en la recolección de datos se probará la hipótesis mediante técnicas de aprendizaje automático, se establecerán patrones de comportamiento, es decir, se realizará un análisis histórico de las fuentes de datos para obtener un análisis predictivo junto con la herramienta de inteligencia de negocios, apoyados con una metodología ágil para que los resultados sean eficaces y flexibles a lo largo del estudio, a continuación, se muestra la relación entre los objetivos y las fases de la metodología planteada.

Figura 9

Relación entre los procesos Scrum y los objetivos



Nota. Representa una relación entre objetivos, preguntas de investigación y fases

La revisión de literatura revela una serie de pasos que abordan las preguntas de investigación relacionadas con el primer objetivo y engloban las siguientes fases:

1. Iniciación: Durante esta etapa se establece la visión del proyecto, se identifican los roles clave y los interesados o stakeholders, se definen las prioridades, se elabora el plan de lanzamiento y se establece el alcance de cada sprint o mini proyecto.

Al analizar la literatura existente, se encontró que tanto en las fuentes primarias como en las secundarias no hay datos sobre inteligencia de negocios que ayuden a contrarrestar los ataques DDoS. Por lo tanto, se tomaron en cuenta algoritmos de detección de ataques y sistemas de mitigación para abordar cuestiones relacionadas con este tipo de ataques.

2. Planificación y estimación: En esta etapa se establecen las funcionalidades y tareas a llevar a cabo, con plazos claramente definidos, con el fin de cumplir los objetivos mediante la asignación prioritaria de las tareas. En resumen, se trata de la planificación del proyecto.

Durante esta fase, se identificó el problema que enfrenta el ISP de Ecuador con respecto a la alta cantidad de ataques DDoS que afectan tanto su infraestructura como la de sus clientes. Para abordar esta situación, se propone desarrollar una solución de Business Intelligence que analice los datos de vulnerabilidades DoS. Esta solución permitirá mitigar los ataques cibernéticos dirigidos a la infraestructura del ISP en un período de tiempo corto, mediano o largo.

En la siguiente etapa, se enfoca en cumplir el segundo objetivo, donde se llevará a cabo un análisis cuantitativo de las fuentes de datos con el objetivo de detectar y mitigar los ataques DDoS.

3. Implementación: En esta etapa se ejecutan las tareas y entregables establecidos en la planificación. Se llevan a cabo reuniones breves en las que el equipo informa sobre el estado de las actividades diarias y se actualiza la lista de prioridades. Se identifican dependencias, se realiza el análisis y diseño técnico de las soluciones, y se llevan a cabo pruebas de aceptación.

El experimento se llevará a cabo definiendo las variables a analizar y las relaciones entre estos elementos para detectar ataques. Se establecerán medidas y análisis en los datos históricos con el fin de obtener resultados que prevengan la afectación en la disponibilidad del servicio proporcionado por el ISP.

Las fases siguientes se enfocan en el objetivo tres, que permitirá la selección de la herramienta para el proceso de inteligencia de negocios.

4. Revisión y retrospectiva: En esta fase del proyecto en la que ya está en marcha la implementación, se llevará a cabo una revisión del proceso, junto con una evaluación interna del trabajo realizado. Esto nos permitirá obtener opiniones constructivas y lecciones aprendidas que se podrán aplicar en futuros ciclos de trabajo. Con el fin de apreciar claramente los resultados, una vez que dispongamos de los datos en las herramientas de inteligencia de negocios, utilizaremos las funcionalidades de estas para presentar los resultados e indicadores de acuerdo a lo definido a lo largo de este estudio.

5. Lanzamiento: Durante esta etapa, se lleva a cabo el proceso de generar los productos entregables y se realizan actividades de reflexión para identificar mejoras y lecciones aprendidas del proyecto.

Utilizando una herramienta de inteligencia de negocios, se generará automáticamente un informe con la información necesaria para la toma de decisiones de la gerencia. Se propone establecer un nivel de confianza para aceptar o rechazar la hipótesis planteada. Se realizará un análisis exhaustivo de las metodologías a implementar en el trabajo actual y se aplicarán para resolver el problema propuesto.

En el siguiente capítulo se describe de manera práctica cómo se utilizan las fases mencionadas.

Capítulo IV

Desarrollo de la solución

Inicio

En este capítulo se explica la propuesta de solución, se evalúa la herramienta de integración, se analizan y se presentan visualmente los datos. Se proporciona información detallada sobre cómo funciona actualmente el ISP frente a los incidentes de DDoS. Además, se plantea la utilización de la metodología Scrum para identificar, medir y controlar los ataques DDoS en la infraestructura del ISP para los clientes finales en un lapso de 7 meses.

Análisis del problema

El ISP desempeña un papel crucial como colaborador estratégico para empresas en Ecuador al ofrecer servicios de Internet que garanticen seguridad, rendimiento y confiabilidad. Cuando las organizaciones buscan proteger sus redes contra ataques DDoS, el departamento de TI del ISP recurre a hardware o proveedores en la nube para contrarrestar estos ataques. Sin embargo, las soluciones convencionales no están diseñadas para satisfacer las necesidades fundamentales de Internet debido a sus altos costos o retrasos en la respuesta.

Infraestructura

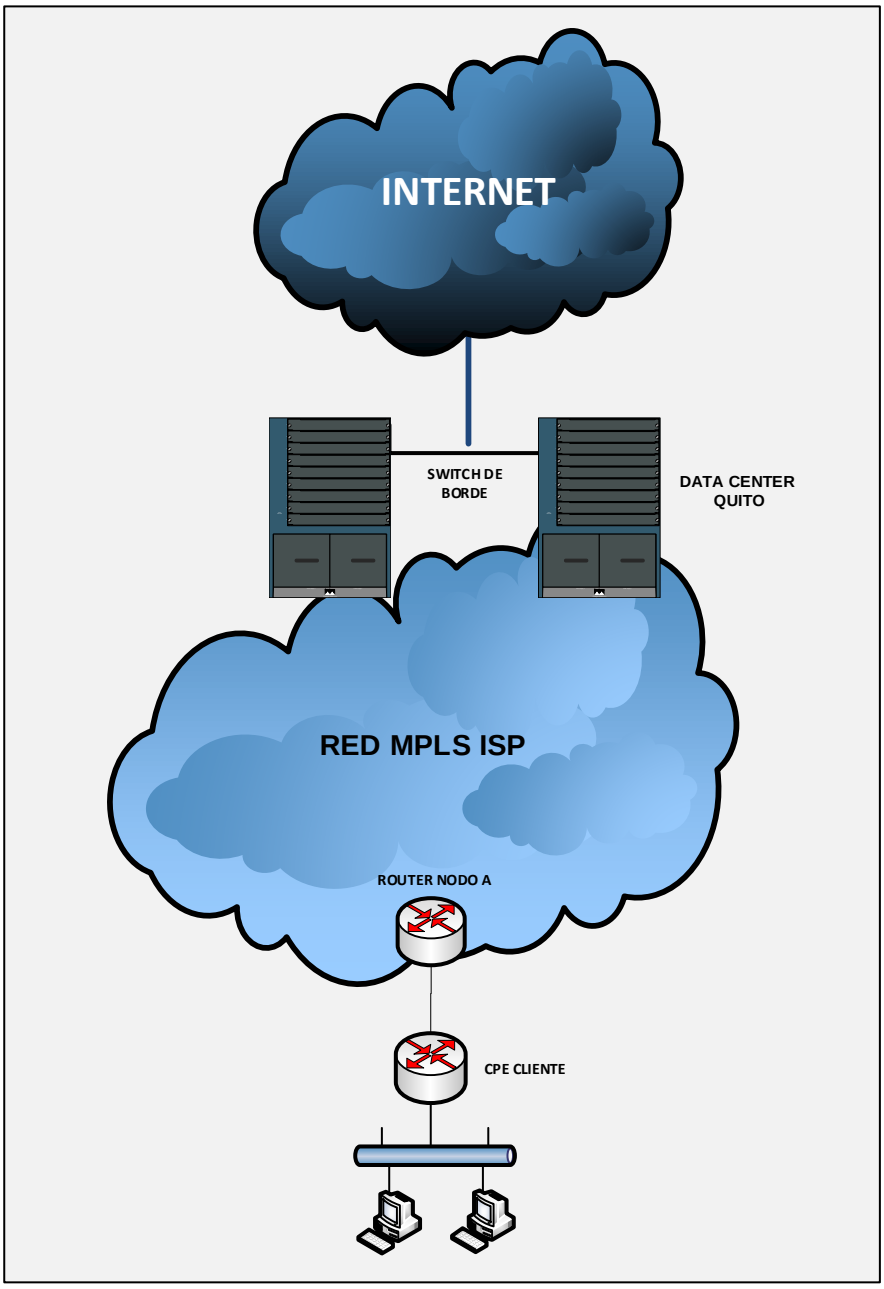
Para el producto de Internet dedicado que es contratado por el cliente se le instala: una última milla de fibra óptica desde el nodo, un CPE (router), se configura un ancho de banda específico y se asigna una subred publica al CPE, dicha IP sirve para publicar los servicios, sus redes locales, alcanzar servicios alojadas en la nube e hibridas o proporcionar la navegación libre de sus equipos.

La IP publica es propagada por la salida internacional que el ISP contrata con el proveedor internacional, en la figura a se describe un diagrama lógico de la topología de red de la infraestructura del ISP, donde se describe los equipos de borde que se interconectan a la salida internacional ubicados en el Data Center de Quito, los routers ubicados en cada nodo de

la red MPLS y estos a su vez, se conectan hacia la Ultima Milla del cliente en la infraestructura interna.

Figura 10

Diagrama lógico de la infraestructura de red del ISP



Nota. Representa el equipamiento básico para el servicio de un cliente

Una vez presentado en resumen el entorno del ISP, se busca contar con mecanismos que faciliten de manera inmediata los resultados a las métricas planteadas que son propias del giro del negocio, pues esto permitirá evaluar, medir, supervisar y controlar los riesgos ante ataque de denegación de servicio y tomar de forma oportuna decisiones que ayuden a mitigar los ataques y cumplir con los acuerdos de nivel de servicios.

Planificación y estimación

Una vez que se establece y se alinea lo que genera valor para la empresa, se llega a la conclusión de que la inteligencia de negocios es de gran importancia para el ISP. La preparación de la información, los procesos ETL, la carga, la validación y el uso permitirán tener un esquema organizado de datos para automatizar el proceso de mitigación de ataques de denegación de servicios. Para lograr esto, se estima que tomará aproximadamente 30 días desarrollar la herramienta de detección de ataques DDoS y alrededor de 6 meses para desarrollar el modelo de inteligencia empresarial, los tableros y los informes que respaldarán la toma de decisiones.

Implementación

Para el proceso de implementación en base a los requerimientos definidos, se procede a describir las herramientas de BI, proceso de extracción de datos, detección y mitigación de ataques DDoS, que permitan cumplir con los objetivos de la investigación.

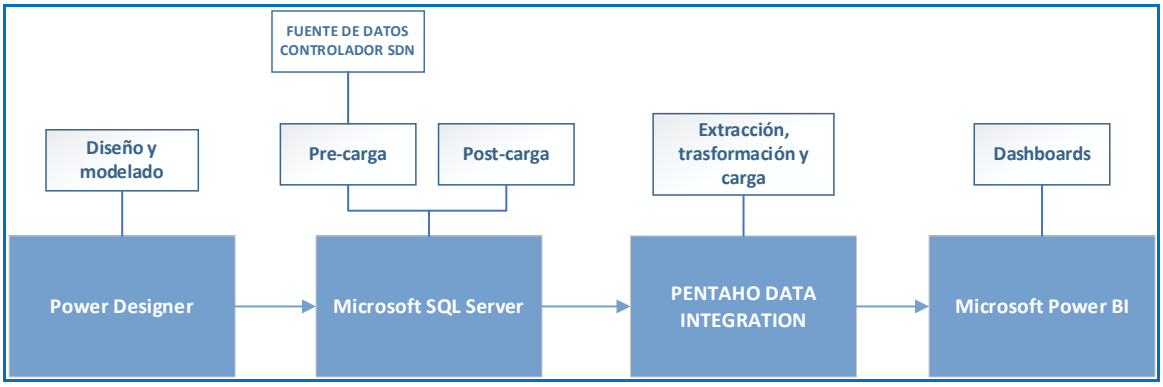
Selección de la infraestructura

El propósito principal de esta investigación es presentar una solución que salvaguarde tanto la red del proveedor de servicios de Internet (ISP) como la de los clientes contra ataques DDoS en tiempo real. Esta solución se basa en la utilización de una máquina de vectores de soporte integrada con un controlador SDN, el cual estará alojado en una Máquina Virtual situada en el Data Center de Quito.

La siguiente ilustración representa la conexión entre las herramientas y las etapas en las que se emplearían durante el proceso de implementación del modelo, según lo analizado en los capítulos previos.

Figura 11

Herramientas seleccionadas para el modelo DWH



Nota. Representa la relación de las herramientas y fases que se usaran en el proyecto de Business Intelligence.

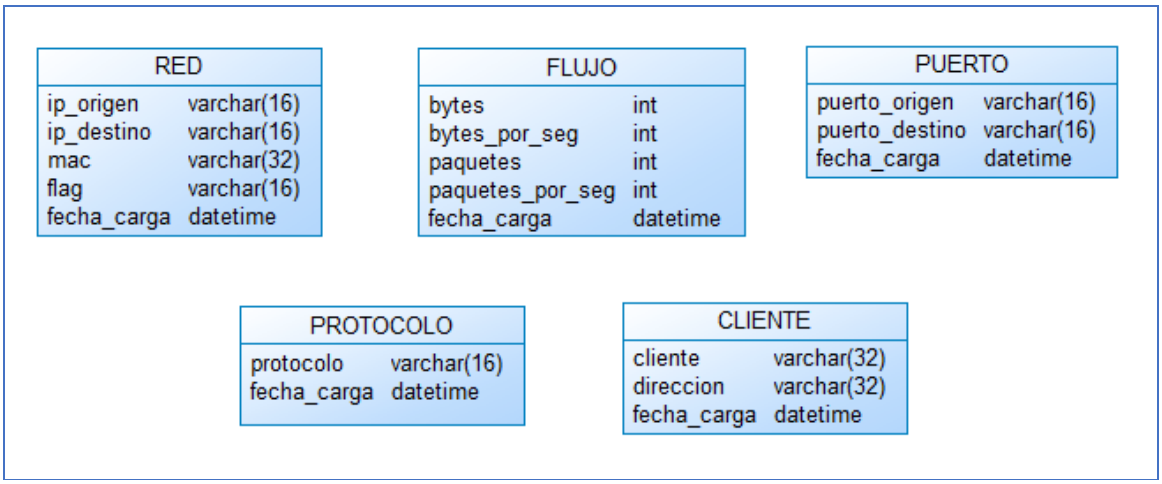
PowerDesigner

Para la construcción de la solución, se selecciona el software de modelado de datos que permite visualizar, analizar y manipular los metadatos para obtener una arquitectura eficaz, su versión gratuita por 15 días, facilita el mapeo de la información y su sincronización con otros programas, PowerDesigner cumple con estas especificaciones, en la herramienta se crean dos modelos, para el proceso de Data Warehouse y otro del DSA.

El DSA es un área temporal donde se recogen los datos que se necesitan de las fuentes origen, se recogen los datos estrictamente necesarios para las cargas, no se aplican restricciones de integridad ni se utilizan claves, los datos se analizan de forma de ficheros planos. Estos datos no van a dar servicio a ninguna aplicación de reportaría, son datos temporales que una vez hayan cumplido su objetivo serán eliminados (MSDN, 2022).

Figura 12

Descripción Dsa_flujo



Nota. Elaboración propia como parte del modelo DSA.

El esquema que se utiliza para el modelamiento del Data Warehouse es tipo estrella, el modelo dimensional físico está confirmado de la tabla de hechos, tabla de dimensiones, en la tabla de hechos se identifica los datos que deben responder a las preguntas de negocios.

Considerando el nivel de granularidad en cada dimensión, representa el detalla al que se desea guardas los datos, para esto se considerando la Dim_ flujo.

Tabla 6

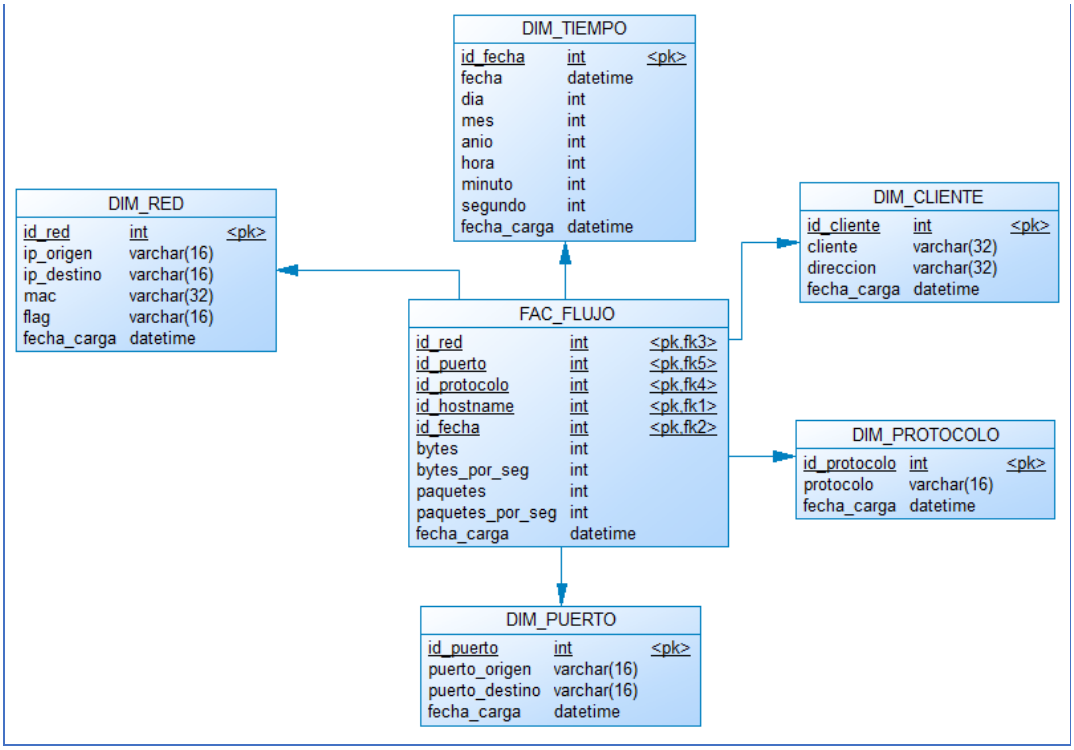
Nivel de granularidad Dim_flujo

Dimensión	Nivel de granularidad
dim_tiempo	id_tiempo
dim_red	id_red
dim_puerto	id_puerto
dim_protocolo	id_protocolo
dim_cliente	id_cliente

Una vez elaborado el DSA, a continuación, se elabora el modelo dimensional físico, el cual está conformado por la tabla de hechos, tablas de dimensiones y medidas, como se muestra en:

Figura 13

Modelo dimensional físico DWH Fac_flujo



Nota. Elaboración propia esquema estrella del modelo DWH

La tabla Dim_tiempo, tiene información del tiempo, el nivel de granularidad, permite elegir la frecuencia de carga de datos, colocar algo respecto al intervalo de muestreo.

Tabla 7

Descripción Dim_tiempo

Descripción campo	Campo	Tipo de dato
id_fecha	ID_FECHA	Int
Fecha	FECHA	Datetime
Dia	DIA	Int
Mes	MES	Int
Anio	ANIO	Int
Hora	HORA	Int
Minuto	MINUTO	Int
Segundo	SEGUNDO	Int
fecha_carga	FECHA_CARGA	Datetime

La tabla Dim_red, tiene información que corresponde a la red del usuario final, esto quiere decir, IP origen IP destino, dirección física y flag que es la etiqueta del paquete de red.

Tabla 8

Descripción Dim_red

Descripción campo	Campo	Tipo de dato
id_red	ID_RED	Int
ip_origen	IP_ORIGEN	varchar(16)
ip_destino	IP_DESTINO	varchar(16)
Mac	MAC	varchar(32)
Flag	FLAG	varchar(16)
fecha_carga	FECHA_CARGA	datetime

La tabla Dim_puerto, contiene información acerca del puerto que se establece en la comunicación de red.

Tabla 9

Descripción DIM_puerto

Descripción campo	Campo	Tipo de dato
id_puerto	ID_PUERTO	Int
puerto_origen	PUERTO_ORIGEN	varchar(16)
puerto_destino	PUERTO_DESTINO	varchar(16)
fecha_carga	FECHA_CARGA	datetime

La tabla Dim_cliente, tiene información del cliente final como el identificativo o nombre y dirección.

Tabla 10

Descripción DIM_cliente

Descripción campo	Campo	Tipo de dato
id_cliente	ID_CLIENTE	Int
Cliente	CLIENTE	varchar(32)
Dirección	DIRECCION	varchar(32)
fecha_carga	FECHA_CARGA	datetime

La tabla Dim_protocolo contiene información acerca del protocolo de comunicación que se establece en la comunicación de red.

Tabla 11

Descripción DIM_protocolo

Descripción campo	Campo	Tipo de dato
id_protocolo	ID_PROTOCOLO	Int
Protocolo	PROTOCOLO	varchar(16)
fecha_carga	FECHA_CARGA	Datetime

Finalmente se crea la tabla de hechos, que consta de las claves externas que provienen de las dimensiones.

Tabla 12

Tabla de hechos Fac_flujo

Descripción campo	Campo	Tipo de dato
id_red	ID_RED	Int
id_puerto	ID_PUERTO	Int
id_protocolo	ID_PROTOCOLO	Int
id_hostname	ID_HOSTNAME	Int
id_fecha	ID_FECHA	Int
Bytes	BYTES	Int
bytes_por_seg	BYTES_POR_SEG	Int
Paquetes	PAQUETES	Int
paquetes_por_seg	PAQUETES_POR_SEG	Int
fecha_carga	FECHA_CARGA	Datetime

Microsoft SQL Server

El gestor de base de datos seleccionado es SQL Server, edición gratuita ya que permite almacenar y gestionar los datos de forma eficiente y estructurada.

Se crean dos bases de datos con sus respectivas tablas, esta herramienta controla el procesamiento, ejecuta consultas, comandos y almacena los archivos, tablas manteniendo su integridad.

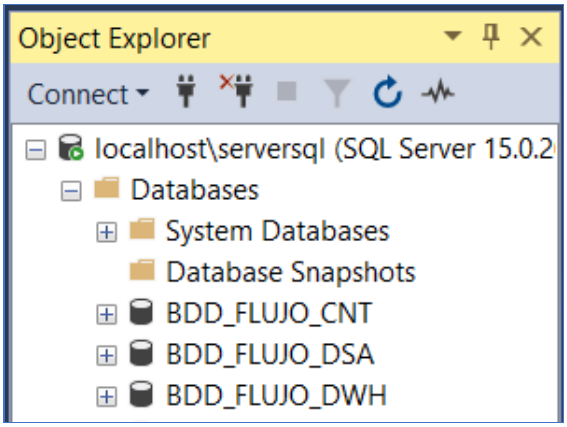
La base de datos multidimensional BDD_FLUJO_DWH es responsable de consolidar y almacenar los flujos de IP recopilados y preprocesados del controlador SDN. Para ello se utilizó el modelo estrella propuesto. En el modelo desarrollado, el objeto de análisis es la Fac_flujo, en el que las dimensiones brindan métricas para evaluar el comportamiento de la red, principalmente, en escenarios de ataque.

La BDD_FLUJO_DSA almacena los archivos originales de la fuente de datos desde el controlador SDN, los mismos serán almacenados de manera temporal, en la

BDD_FLUJO_DWH, se realiza el proceso de ETL extracción, trasformación y carga, la BDD_FLUJO_CNT es una base de control temporal.

Figura 14

SQL Server, bases de datos



Controlador SDN

Dentro del proceso de desarrollo del modelo, previo a la implementación del modelo DWH, basados en los estudios del autor (Siaterlis & Maglaris, 2010), como fase de pruebas de la herramienta de detección de ataques DDoS se emula la red SDN y se lanzó ataques DDoS en tiempo real desde múltiples hosts comprometidos hacia un objetivo en la red del ISP con el objetivo de abrumar los recursos de la red y evaluar el proceso de detección. El sistema descrito se implementó asegurando su funcionalidad y confiabilidad sobre la red del ISP y esta evaluado sobre la capa 3 de red. Los resultados obtenidos en esta sección de pruebas muestran que el sistema propuesto detecta y mitiga los ataques DDoS, los resultados y script se muestran a continuación.

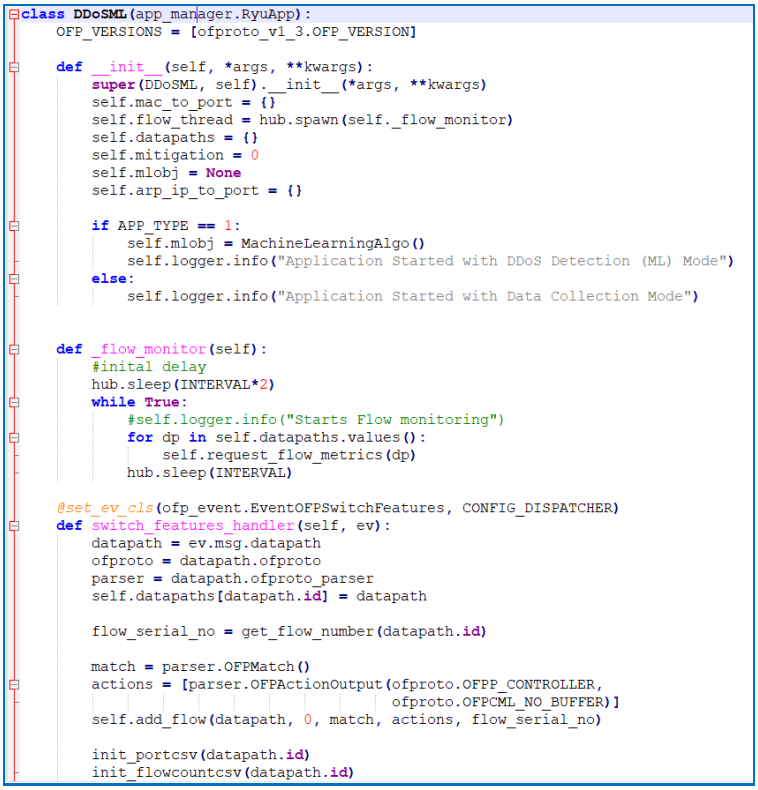
Figura 15

Script para la recolección de datos

```
from ryu.base import app_manager
from ryu.controller import ofp_event
from ryu.controller.handler import CONFIG_DISPATCHER, MAIN_DISPATCHER
from ryu.controller.handler import set_ev_cls
from ryu.ofproto import ofproto_v1_3
from ryu.lib.packet import packet
from ryu.lib.packet import ethernet
from ryu.lib.packet import ether_types

from ryu.lib.packet import in_proto
from ryu.lib.packet import ipv4
from ryu.lib.packet import icmp
from ryu.lib.packet import tcp
from ryu.lib.packet import udp
from ryu.lib.packet import arp

from ryu.lib import hub
import csv
import time
import math
import statistics
from datetime import datetime

from ml import MachineLearningAlgo

#------------------------------------------------------------#
APP_TYPE = 0
#0 datacollection, 1 deteccion ddos
PREVENTION = 0
# prevension ddos


#0  normal, 1 attack
TEST_TYPE = 0


#intervalo coleccion datos
INTERVAL = 5
#------------------------------------------------------------#

BLOCKED_PORTS = {}
```

Figura 16

Script para la recolección de datos flujo de datos

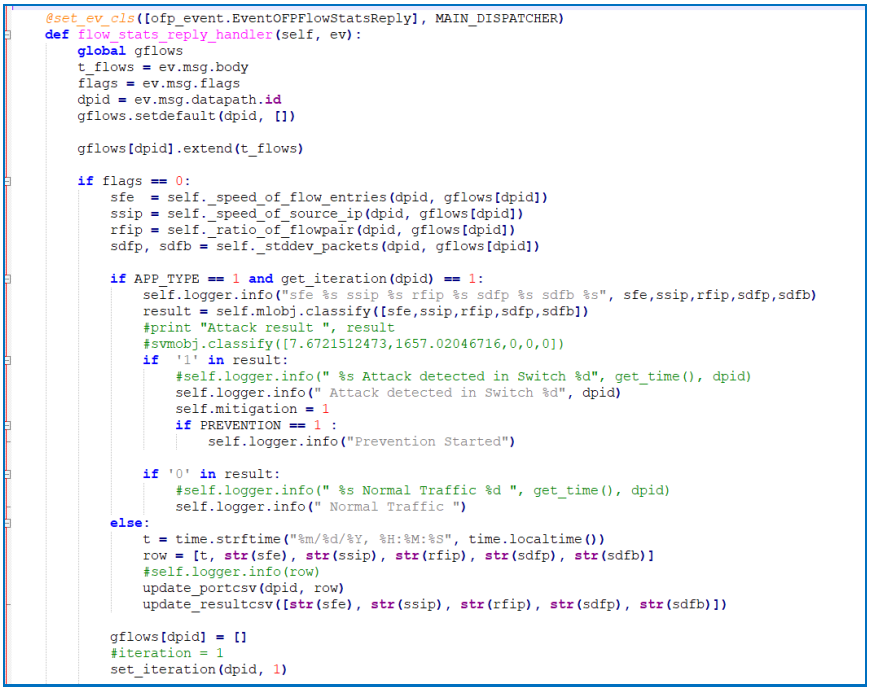


```
class DDoSML(app_manager.RyuApp):
    OFP_VERSIONS = [ofproto_v1_3.OFP_VERSION]

    def __init__(self, *args, **kwargs):
        super(DDoSML, self).__init__(*args, **kwargs)
        self.mac_to_port = {}
        self.flow_thread = hub.spawn(self._flow_monitor)
        self.datapaths = {}
        self.mitigation = 0
        self.mlobj = None
        self.arp_ip_to_port = {}

        if APP_TYPE == 1:
            self.mlobj = MachineLearningAlgo()
            self.logger.info("Application Started with DDoS Detection (ML) Mode")
        else:
            self.logger.info("Application Started with Data Collection Mode")


    def _flow_monitor(self):
        #inital delay
        hub.sleep(INTERVAL*2)
        while True:
            #self.logger.info("Starts Flow monitoring")
            for dp in self.datapaths.values():
                self.request_flow_metrics(dp)
            hub.sleep(INTERVAL)

    @set_ev_cls(ofp_event.EventOFPSwitchFeatures, CONFIG_DISPATCHER)
    def switch_features_handler(self, ev):
        datapath = ev.msg.datapath
        ofproto = datapath.ofproto
        parser = datapath.ofproto_parser
        self.datapaths[datapath.id] = datapath

        flow_serial_no = get_flow_number(datapath.id)

        match = parser.OFPMatch()
        actions = [parser.OFPActionOutput(ofproto.OFPP_CONTROLLER,
                                          ofproto.OFPCML_NO_BUFFER)]
        self.add_flow(datapath, 0, match, actions, flow_serial_no)

        init_portcsv(datapath.id)
        init_flowcountcsv(datapath.id)
```

La SDN gestiona el tráfico de red buscando las entradas de la tabla de flujo. La extracción de valores característicos está relacionada con el ataque DDoS de la tabla de flujo de las interfaces de entrada de los switchs de borde, la información de valores característicos analizados se clasifica utilizando un algoritmo basado en SVM para distinguir entre tráfico normal y tráfico de ataque.

Figura 17

Script de entrenamiento del modelo para detección de ataques



```
    @set_ev_cls([ofp_event.EventOFPFlowStatsReply], MAIN_DISPATCHER)
    def flow_stats_reply_handler(self, ev):
        global gflows
        t_flows = ev.msg.body
        flags = ev.msg.flags
        dpid = ev.msg.datapath.id
        gflows.setdefault(dpid, [])

        gflows[dpid].extend(t_flows)

        if flags == 0:
            sfe  = self._speed_of_flow_entries(dpid, gflows[dpid])
            ssip = self._speed_of_source_ip(dpid, gflows[dpid])
            rfip = self._ratio_of_flowpair(dpid, gflows[dpid])
            sdfp, sdfb = self._stddev_packets(dpid, gflows[dpid])

            if APP_TYPE == 1 and get_iteration(dpid) == 1:
                self.logger.info("sfe %s ssip %s rfip %s sdfp %s sdfb %s", sfe,ssip,rfip,sdfp,sdfb)
                result = self.mlobj.classify([sfe,ssip,rfip,sdfp,sdfb])
                #print "Attack result ", result
                #svmobj.classify([7.6721512473,1657.02046716,0,0,0])
                if  '1' in result:
                    #self.logger.info(" %s Attack detected in Switch %d", get_time(), dpid)
                    self.logger.info(" Attack detected in Switch %d", dpid)
                    self.mitigation = 1
                    if PREVENTION == 1 :
                        self.logger.info("Prevention Started")

                if '0' in result:
                    #self.logger.info(" %s Normal Traffic %d ", get_time(), dpid)
                    self.logger.info(" Normal Traffic ")
            else:
                t = time.strftime("%m/%d/%Y, %H:%M:%S", time.localtime())
                row = [t, str(sfe), str(ssip), str(rfip), str(sdfp), str(sdfb)]
                #self.logger.info(row)
                update_portcsv(dpid, row)
                update_resultcsv([str(sfe), str(ssip), str(rfip), str(sdfp), str(sdfb)])

            gflows[dpid] = []
            #iteration = 1
            set_iteration(dpid, 1)
```

Los valores característicos relacionados con los ataques DDoS se obtienen para la detección de ataques DDoS los cuales son:

La velocidad de la IP de origen, es el número de direcciones IP de origen por unidad de tiempo. En caso de ataque, un gran número de ataques se generan mediante falsificación aleatoria para enviar paquetes de datos, el número de la dirección IP de origen aumentará rápidamente.

La velocidad del puerto de origen, es el número de puertos de origen por unidad de tiempo. Cuando se produce una gran cantidad de solicitudes de ataque, un gran número de puertos se generan aleatoriamente.

La desviación estándar de paquetes de flujo, es la desviación estándar del número de paquetes en un periodo de tiempo. Para producir un ataque, los paquetes de datos de ataque

son relativamente pequeños y la desviación estándar de los paquetes de flujo será menor que el flujo normal.

La desviación de bytes de flujo, es la desviación estándar del número de bits en el periodo de tiempo. En el caso de un ataque, para reducir la carga de paquetes, el atacante enviará un bit más pequeño de paquetes de datos y los bits de flujo de desviación estándar serán más pequeños que el flujo normal.

La velocidad de las entradas de flujo, es el número de entradas de flujo por unidad de tiempo. En caso de un ataque, el número de entradas de flujo por unidad de tiempo aumenta drásticamente más alto que el valor normal.

Para la mitigación del ataque de DDoS se identifica la interfaz que recibe el flujo de ataque, se procede con el bloqueo de la interfaz y se conmuta el trafico hacia otra salida Internacional.

Figura 18

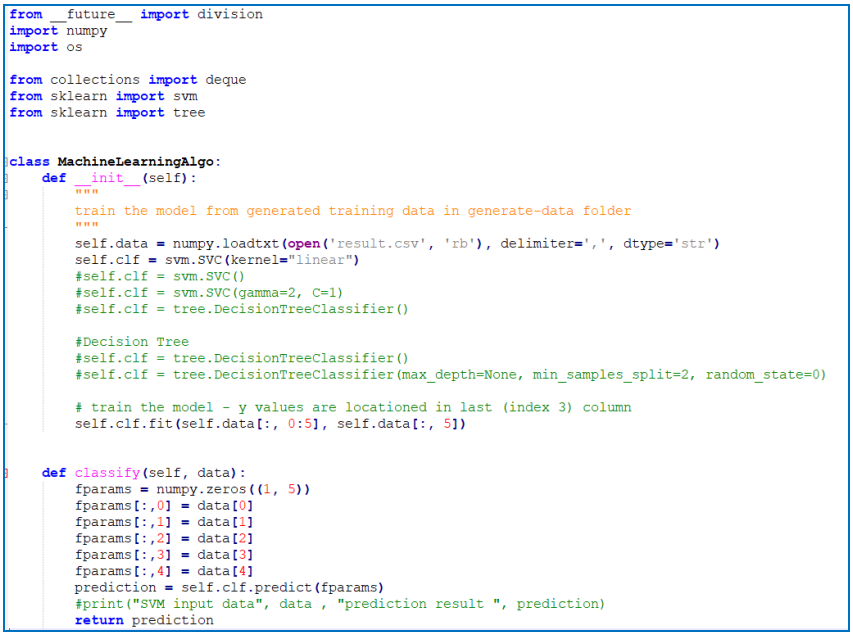
Script algoritmo mitigación ataque DDoS

```
        # install a flow to avoid packet_in next time
        if out_port != ofproto.OFPP_FLOOD:

            # check IP Protocol and create a match for IP
            if eth.ethertype == ether_types.ETH_TYPE_IP:
                ip = pkt.get_protocol(ipv4.ipv4)
                srcip = ip.src
                dstip = ip.dst
                protocol = ip.proto


                if self.mitigation and PREVENTION:
                    if not (srcip in self.arp_ip_to_port[dpid][in_port]):
                        if not in_port in BLOCKED_PORTS[dpid]:
                            self.logger.info(" %s  : attack detected in switch %d from port %d", get_time(), dpid, in_port)
                            self.block_port(datapath, in_port)
                            self.logger.info(" %s:  Switch %d Blocked the port %d",get_time(), dpid, in_port)
                            self.remove_attack_flows(datapath, in_port)
                            self.logger.info(" %s:  Switch %d Removed the attacker flows ",get_time(), dpid )
                            BLOCKED_PORTS[dpid].append(in_port)
                            self.block_port(datapath, in_port)
                        #print ip
                        return

                match = parser.OFPMatch(in_port=in_port, eth_type=ether_types.ETH_TYPE_IP, ipv4_src=srcip, ipv4_dst=dstip)

                # verify if we have a valid buffer_id, if yes avoid to send both
                # flow_mod & packet_out
                flow_serial_no = get_flow_number(datapath.id)
                if msg.buffer_id != ofproto.OFP_NO_BUFFER:
                    self.add_flow(datapath, 1, match, actions, flow_serial_no,  buffer_id=msg.buffer_id)
                    return
                else:
                    self.add_flow(datapath, 1, match, actions, flow_serial_no)
        data = None
        if msg.buffer_id == ofproto.OFP_NO_BUFFER:
            data = msg.data

        out = parser.OFPPacketOut(datapath=datapath, buffer_id=msg.buffer_id,
                                  in_port=in_port, actions=actions, data=data)
        datapath.send_msg(out)
```

Estos parámetros son evaluados en la detección de DDoS basada en Máquinas de vectores de soporte Support Vector Machine (SVM).

Figura 19

Script del algoritmo de machine learning basado en SVM

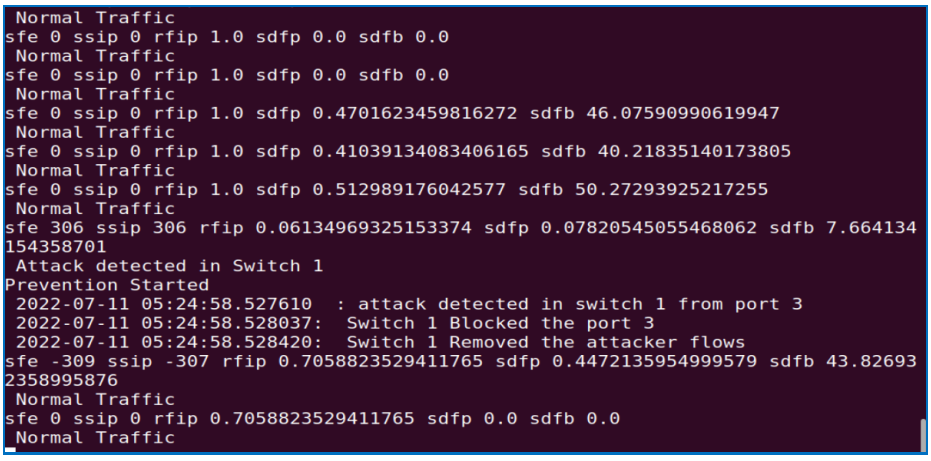


```
from __future__ import division
import numpy
import os

from collections import deque
from sklearn import svm
from sklearn import tree


class MachineLearningAlgo:
    def __init__(self):
        """
        train the model from generated training data in generate-data folder
        """
        self.data = numpy.loadtxt(open('result.csv', 'rb'), delimiter=',', dtype='str')
        self.clf = svm.SVC(kernel="linear")
        #self.clf = svm.SVC()
        #self.clf = svm.SVC(gamma=2, C=1)
        #self.clf = tree.DecisionTreeClassifier()

        #Decision Tree
        #self.clf = tree.DecisionTreeClassifier()
        #self.clf = tree.DecisionTreeClassifier(max_depth=None, min_samples_split=2, random_state=0)

        # train the model - y values are locationed in last (index 3) column
        self.clf.fit(self.data[:, 0:5], self.data[:, 5])


    def classify(self, data):
        fparams = numpy.zeros((1, 5))
        fparams[:,0] = data[0]
        fparams[:,1] = data[1]
        fparams[:,2] = data[2]
        fparams[:,3] = data[3]
        fparams[:,4] = data[4]
        prediction = self.clf.predict(fparams)
        #print("SVM input data", data , "prediction result ", prediction)
        return prediction
```

El resultado de la ejecución del script con el proceso completo de ataque muestra el tráfico normal, detección del ataque DDoS y la mitigación.

Figura 20

Resultado del controlador SDN para la detección y mitigación de ataques



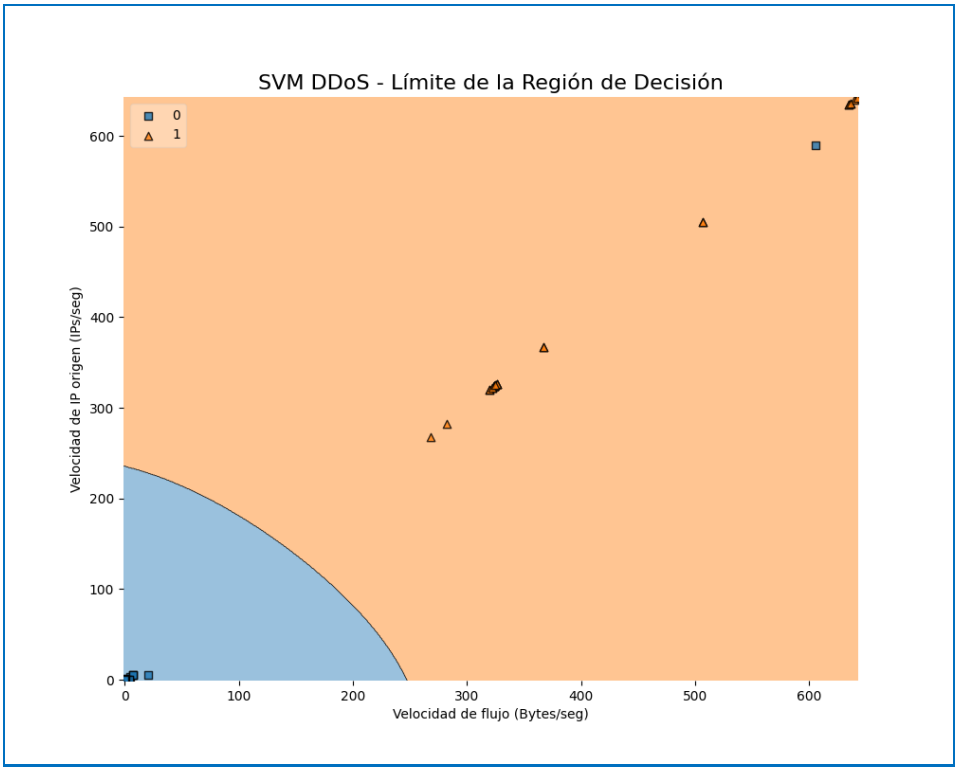
```
 Normal Traffic
sfe 0 ssip 0 rfip 1.0 sdfp 0.0 sdfb 0.0
 Normal Traffic
sfe 0 ssip 0 rfip 1.0 sdfp 0.0 sdfb 0.0
 Normal Traffic
sfe 0 ssip 0 rfip 1.0 sdfp 0.4701623459816272 sdfb 46.07590990619947
 Normal Traffic
sfe 0 ssip 0 rfip 1.0 sdfp 0.41039134083406165 sdfb 40.21835140173805
 Normal Traffic
sfe 0 ssip 0 rfip 1.0 sdfp 0.512989176042577 sdfb 50.27293925217255
 Normal Traffic
sfe 306 ssip 306 rfip 0.06134969325153374 sdfp 0.07820545055468062 sdfb 7.664134
154358701
 Attack detected in Switch 1
Prevention Started
 2022-07-11 05:24:58.527610  : attack detected in switch 1 from port 3
 2022-07-11 05:24:58.528037:  Switch 1 Blocked the port 3
 2022-07-11 05:24:58.528420:  Switch 1 Removed the attacker flows
sfe -309 ssip -307 rfip 0.7058823529411765 sdfp 0.4472135954999579 sdfb 43.82693
2358995876
 Normal Traffic
sfe 0 ssip 0 rfip 0.7058823529411765 sdfp 0.0 sdfb 0.0
 Normal Traffic
```

Después de entrenar el modelo basado en SVM, usando el conjunto de datos de entrenamiento, las muestras de prueba son trazado en un espacio de características

bidimensional de velocidad de flujo y velocidad de IP origen. Esta trama muestra que SVM clasifica las muestras de datos del tráfico normal y tráfico de ataque.

Figura 21

Clasificador de regiones de decisión basado en SVM



Pentaho Data integration

Para el desarrollo de ETL la alternativa de herramienta de código abierto es Pentaho integración de datos, la cual contiene componentes diseñados para ejecutar tareas específicas mediante trabajos y trasformaciones, la interfaz gráfica de usuario que se utiliza es Spoon, el resultado de esta fase es el diseño y ejecución del proceso ETL.

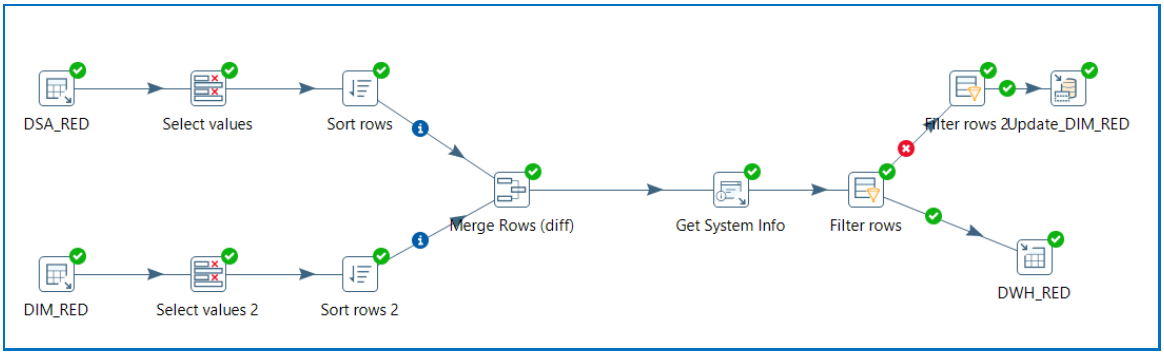
En el proceso ETL, se detalla la construcción de las tablas de dimensiones, procesos iniciales de limpieza de las tablas de dimensiones y de las tablas de hechos.

Las fuentes de datos son archivos csv generados del controlador SDN, se sube para su posterior conversión de datos, se agrega la columna fecha_carga, todos los campos serán

comparados y almacenados en la base de datos del DWH, la trasformación del proceso de ETL se realizará para todas las dimensiones como se muestra para dim_red.

Figura 22

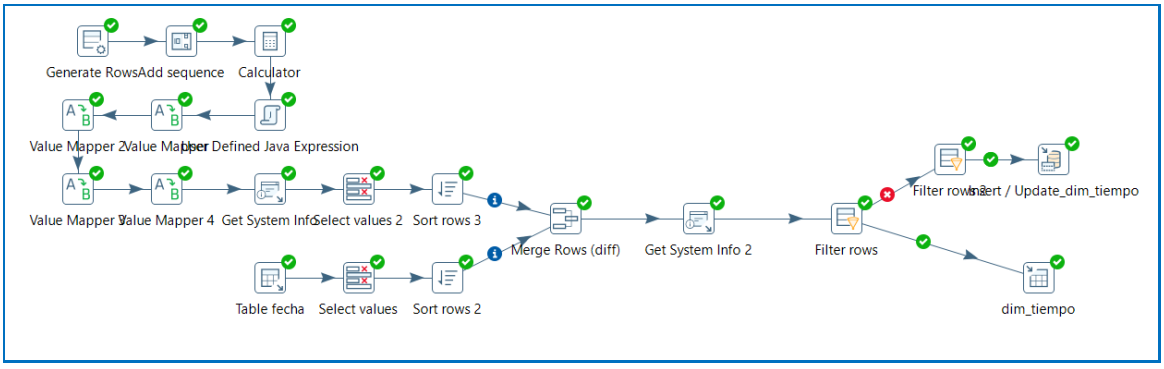
Proceso de trasformación y carga para las dimensiones



El proceso de transformación de la dim_tiempo contiene la granularidad que se necesita para evaluar los eventos de ataque.

Figura 23

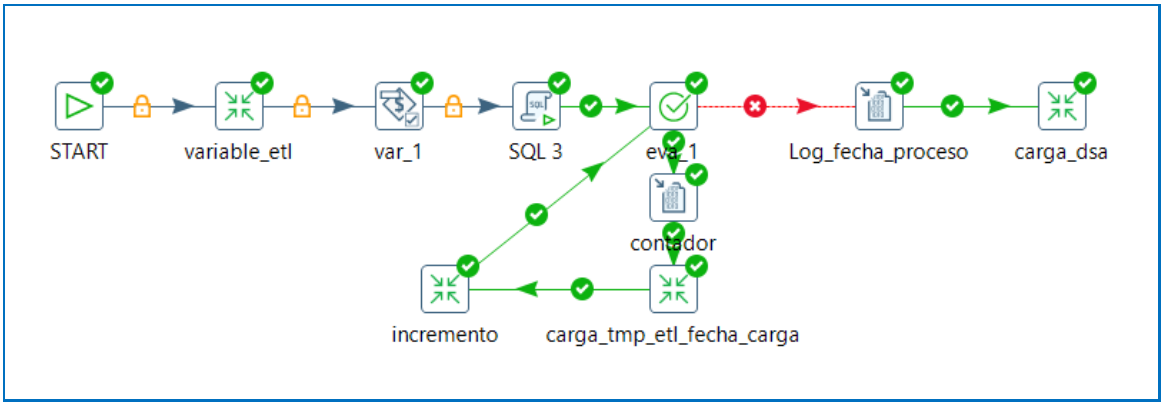
Proceso de trasformación y carga para la dimensión tiempo



Para la carga del DSA de forma secuencial y conservación de la integridad de los datos en el proceso ETL el trabajo en Pentaho se muestra a continuación.

Figura 24

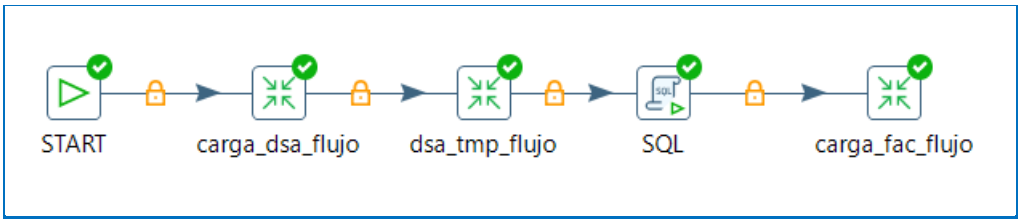
Proceso de trasformación y carga del DSA



El proceso de carga de las DSA y tmp_flujo hacia la fact_flujo se muestra en el siguiente trabajo en Pentaho.

Figura 25

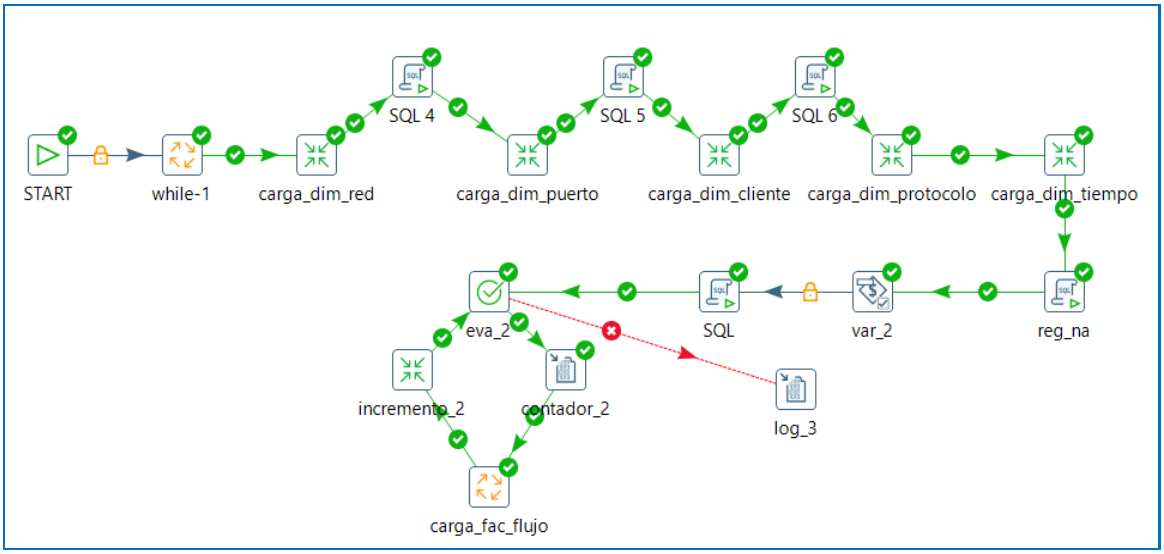
Proceso de trasformación y carga del DSA y FAC_FLUJO



La transformación completa se muestra en el trabajo de la siguiente grafica.

Figura 26

Proceso de trasformación y carga de la tabla de hechos y dimensiones



Power BI

Se llevó a cabo la integración de la herramienta Power BI con la base de datos SQL Server para desarrollar una solución de Business Intelligence. Esto permitió importar las tablas de dimensiones y las tablas de hecho de manera fácil y rápida en Power BI, lo que facilita la conexión, análisis y visualización de los datos del negocio. La presentación interactiva y la actualización en tiempo real de los datos brindan información valiosa, lo que a su vez simplifica la toma de decisiones y permite su publicación en dispositivos conectados a Internet.

La elección de esta herramienta se basó en estudios previos, donde Power BI ha demostrado ser la mejor opción para procesos de BI. Con los resultados obtenidos en el proceso ETL, se pueden establecer métricas específicas para el negocio, lo que contribuye a la toma oportuna de decisiones para mitigar eficazmente los ataques DDoS.

Revisión y retrospectiva

En esta etapa se contrastan los requisitos solicitados con los resultados entregados, se verifica la correspondencia entre los métodos empleados y el trabajo realizado en las fases anteriores, y se propone la aprobación y aceptación después de la demostración del proyecto.

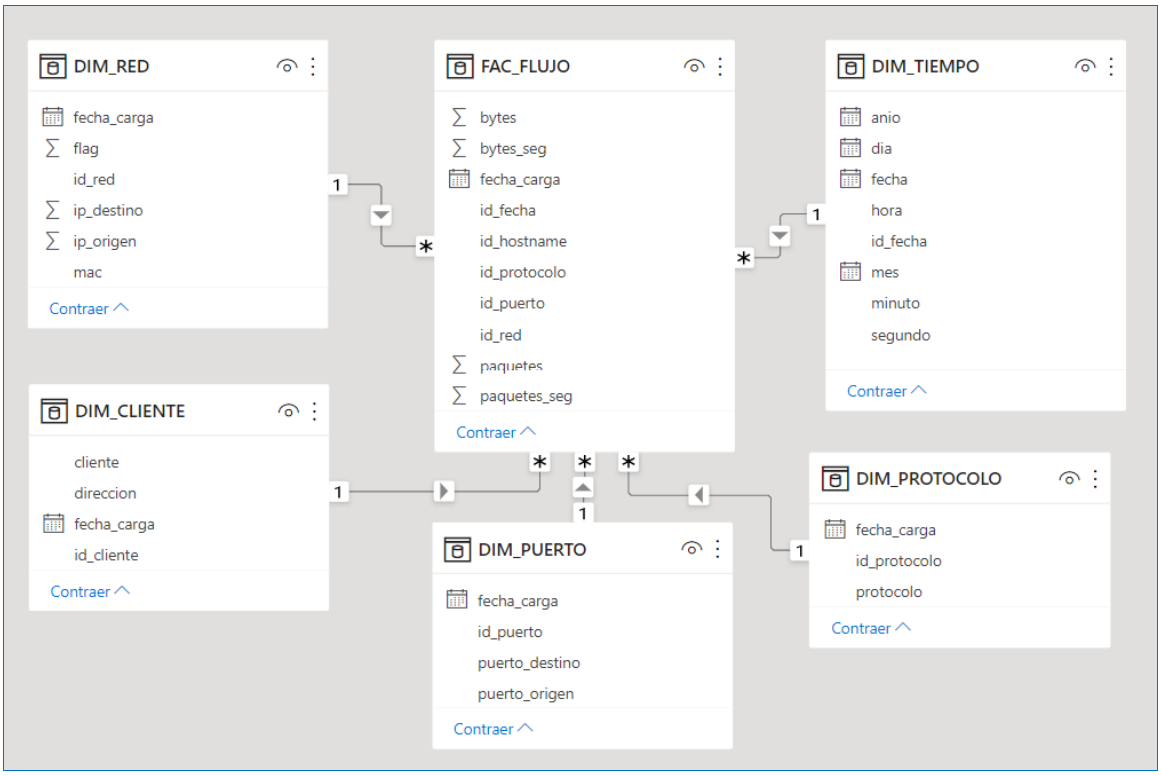
Como parte de la revisión retrospectiva, se resume el proceso de construcción del almacén de datos DWH. Se llevó a cabo un diagnóstico de la cantidad de datos en los archivos fuente, lo cual contribuyó a comprender el problema. Mediante un sprint de diseño del modelo en PowerDesigner, se ingresaron tablas, campos, registros, atributos, claves primarias y foráneas. Esto permitió la desnormalización de los datos originales de las fuentes para generar los modelos y, al mismo tiempo, generar los informes.

Utilizando SQL Server como gestor de base de datos, se crearon las estructuras de los modelos para el DSA y el modelo estrella, incluyendo las tablas de dimensiones y hechos necesarias para implementar el DWH. En la siguiente fase, se empleó Pentaho para el ETL, el proceso de extracción, transformación y carga de los datos de origen, que luego se presentarán mediante Power BI.

Una vez que se establezca la conexión entre Power BI y la base de datos de SQL Server, se facilitará automáticamente la creación del modelo con el objetivo de presentar y visualizar informes para el análisis de ataques DDoS.

Figura 27

Modelo estrella Flujo de datos en Power BI

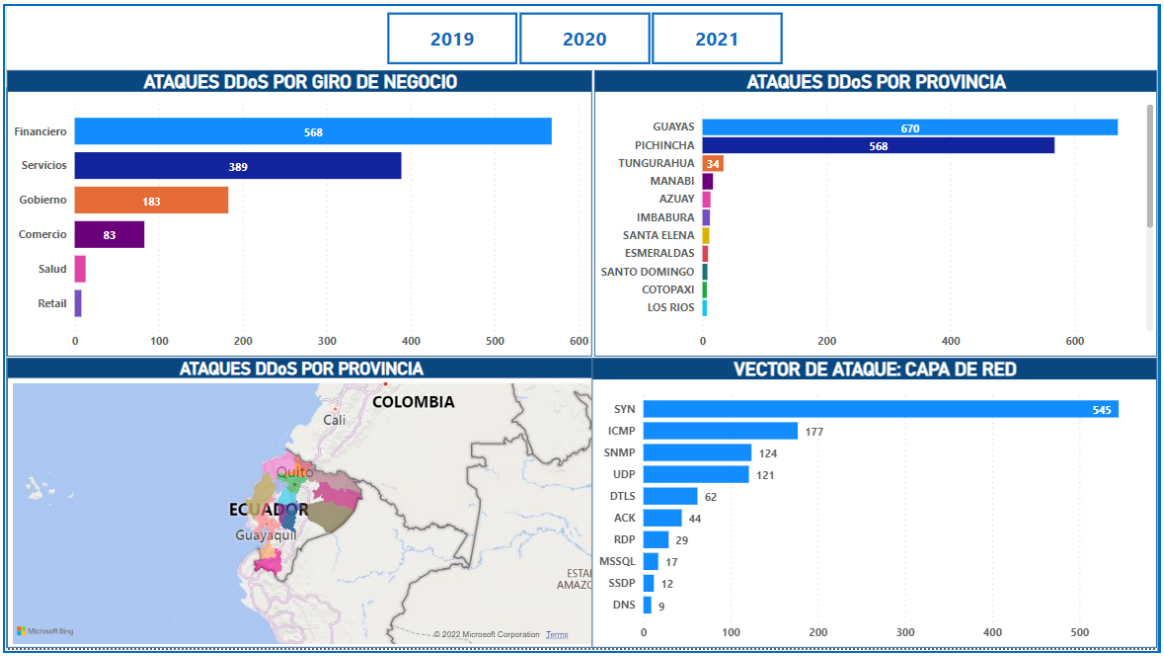


Validación de la solución

Para la elaboración de este sprint se procederá a analizar los datos históricos desde el año 2019 hasta el 2021, se presentan los gráficos que aporten valor en la toma de decisiones, por el proceso realizado se puede apreciar el proceso actual y consecuencias y las ventajas de implementación de la inteligencia de negocios en el ISP ante ataques de denegación de servicios.

Figura 28

Reporte propuesto análisis datos históricos

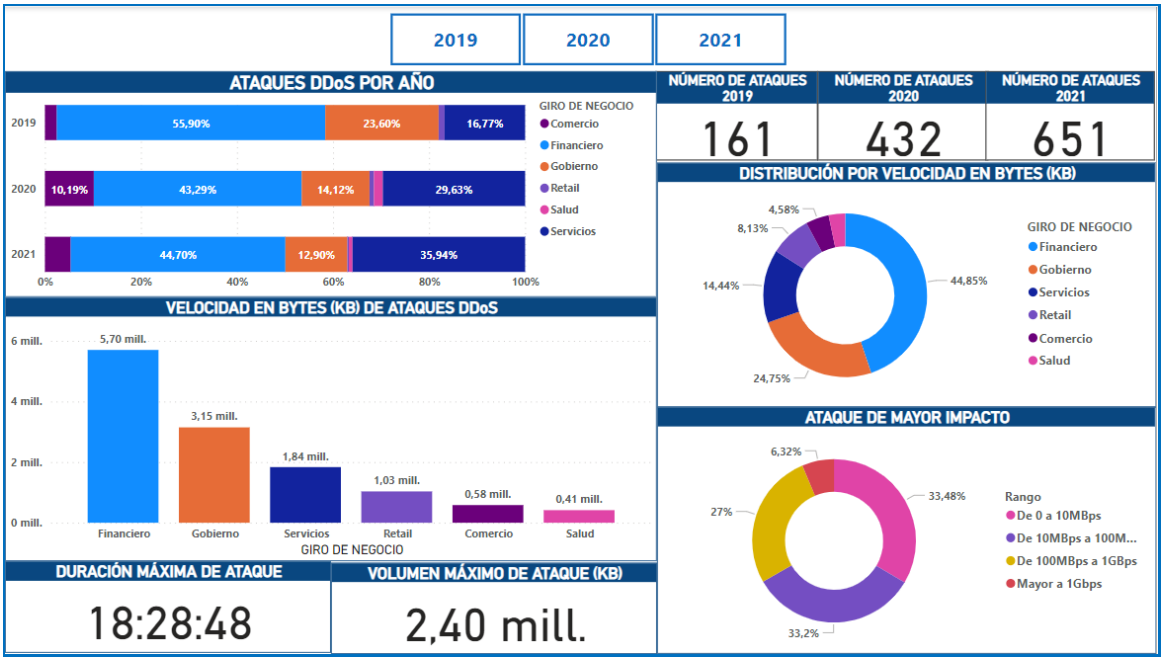


Estos paneles permiten medir, supervisar y analizar los ataques de denegación de servicio que han ocurrido desde el 2019 hasta el 2021, los paneles muestran los ataques DDoS ocurridos por giro de negocio, por provincia y cuál es el vector de ataque en los 3 años históricos.

Para el análisis por giro de negocio con mayores ataques en este periodo de tiempo son: el sector Financiero, Servicios y Gubernamentales con el mayor número de ataques, corresponden a las provincias de Guayas con mayor actividad DDoS y Pichincha en el mismo sentido. Los ataques DDoS se han analizado para la capa de red que pretenden saturar la infraestructura de la red como enrutadores y servidores en línea, en la cual se tiene como vector de ataque: SYN triplica a ataques ICMP y ataques SNMP.

Figura 29

Reporte propuesto análisis datos históricos tendencias de ataques



En este panel se analizan las tendencias de ataques DDoS del cual encontramos: los ataques al sector financiero y gubernamentales han estado disminuyendo mientras que los ataques a servicios están en aumento.

Con respecto al volumen de ataque se evidencia al sector financiero un 44.85% con 5.7GBytes/seg, seguido por entidades gubernamentales con un 24.75% con 3.15GBytes/seg.

Los ataques de mayor impacto corresponden a volúmenes de hasta 10MBps con un 33.48%, seguidos de ataques hasta 100MBps con un 33.2% y ataques mayores a 1GBps con un 6.32%.

El ataque con mayor duración en este periodo duro más de 18 horas con un volumen de 2.4GBps.

Capitulo V

Lanzamiento

Una vez analizada la situación actual, se procede a presentar la solución planteada que permite analizar y mitigar ataques de denegación de servicio, para lo cual se procede a implementar una máquina de vectores de soporte integrada con el controlador SDN el cual estará levantado en una Máquina Virtual ubicada en el Data Center de Quito dentro de la infraestructura del ISP, los datos serán analizados para el año 2022 desde enero hasta julio a fin de evidenciar si la solución planteada permite analizar y controlar los ataques de denegación de servicio, con la aceptación de la solución se procederá con él envió de los entregables y su socialización.

Como parte de la detección de ataques de denegación de servicio mediante el uso de máquina de vectores de soporte, tiene como objeto lograr una alta precisión con una sobrecarga mínima y tasa baja de falsos positivos dadas en la revisión de literatura del capítulo 2, el algoritmo de aprendizaje automático usa valores característicos de las tablas de flujos de la red que entrena el modelo, estos parámetros son capaces de detectar tráfico malicioso de tráfico normal en la red, los valores de velocidad de IP origen, velocidad de flujo y flujo de pares aumentan significativamente en tráfico de ataque, mientras que para valores de desviación estándar del flujo los valores en tráfico de ataque disminuyen.

Figura 30

Correlación de parámetros del SVM

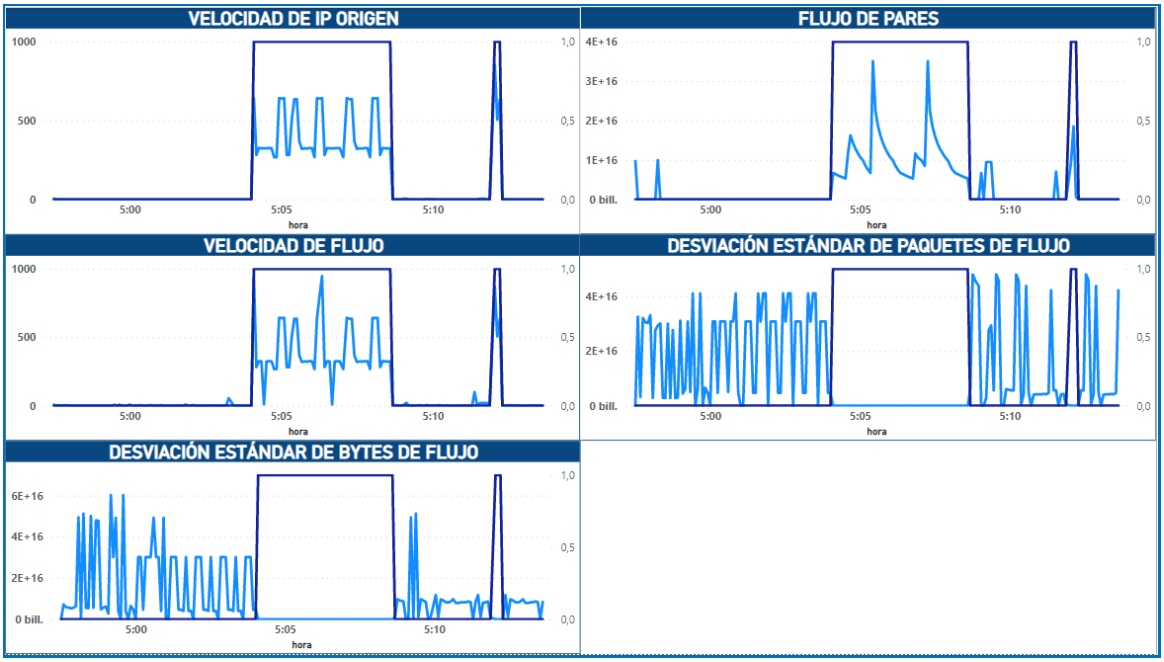
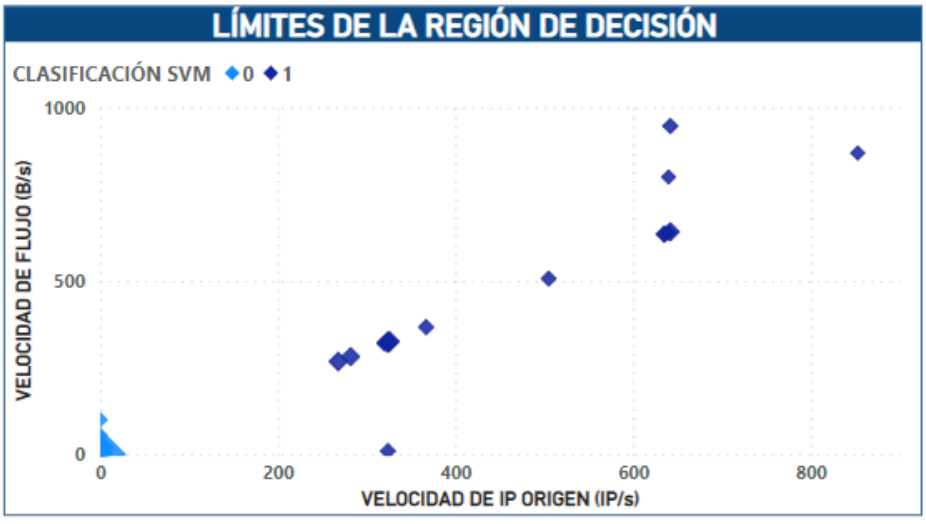


Figura 31

Clasificación de la máquina de vectores de soporte



Para el análisis del modelo se ha considerado una salida Internacional para de la infraestructura del ISP durante los primeros 7 meses del 2022, obteniendo los siguientes resultados.

Figura 32

Reporte propuesto análisis datos periodo año 2022 tendencias de ataques

Se observan 142 ataques totales en este periodo de tiempo, la tendencia en el vector de ataque son SYN e ICMP, siendo los sectores de servicios con mayor ataque, se verifica los sectores financieros y comercio con una reducción considerable.

Figura 33

Reporte mitigación de ataques en porcentaje por vector de ataque

Con respecto a los vectores de ataque que han sido mitigados se tiene un 96,25% en ataques SYN de 80 en total, ICMP con el 96,67% de 30 en total, DTLS con un 76,92% de 13 en total de ataques DDoS.

En resumen, los resultados obtenidos en este estudio se presentan las preguntas de investigación que son contestados con el desarrollo y visualización de los resultados.

OE2-RQ1: ¿Cuáles son las soluciones de Business Intelligence que permiten analizar las vulnerabilidades DDoS y que mitiguen ataques informáticos en la actualidad?

El examen de los registros históricos revela un incremento en los ataques DDoS desde el año 2019. Se ha identificado que el sector de negocio es el más afectado y se ha observado un notable crecimiento en el método de ataque. Toda esta información ha sido utilizada para implementar medidas que disminuyan la vulnerabilidad de la infraestructura frente a ataques en el presente año. En este sentido, las soluciones de Inteligencia Empresarial se adaptarían a las necesidades de la compañía, asegurando un alto nivel de disponibilidad en el servicio.

OE2-RQ2: ¿Los datos históricos de vulnerabilidades DDoS se podrán acoplar al algoritmo de inteligencia de negocios?

Se comprobó la eficacia del método para detectar ataques DDoS mediante el uso de un entorno SDN, el cual recopila paquetes de información tanto del tráfico normal como del tráfico

de ataque. La clasificación de estos paquetes se realiza mediante un algoritmo basado en SVM. En consecuencia, los datos históricos se utilizan para entrenar el modelo del algoritmo de aprendizaje automático.

OE3-RQ1: ¿Cuáles son las acciones que se pueden tomar ante la detección de las amenazas?

A partir del análisis de datos históricos, se pudieron implementar medidas correctivas para el período examinado en 2022. Nuestro objetivo es evitar la exposición de nuestras aplicaciones, puertos y protocolos al mundo, lo que implica comprender y abordar las vulnerabilidades presentes en la infraestructura tanto del cliente como del proveedor de servicios de Internet. Al reducir los posibles puntos de ataque, podemos enfocar nuestros esfuerzos en su mitigación de manera más efectiva.

OE3-RQ2: ¿Cuál es el nivel de confianza con el que se va a trabajar para el análisis de los resultados?

Después de revisar la literatura, se decidió utilizar SVM como algoritmo de aprendizaje automático en combinación con el entorno SDN, el cual recopila los datos de flujo. Estos valores característicos permiten evaluar el tráfico y detectar ataques DDoS. Nuestro enfoque se centró en analizar los cambios en los valores característicos del tráfico y verificar la efectividad de este método mediante la implementación de un entorno experimental SDN. Los resultados obtenidos cumplen con las expectativas, ya que la tasa de detección es alta y la tasa de falsas alarmas es baja.

Conclusiones y recomendaciones

Conclusiones

- Se pudo confirmar la viabilidad del proyecto a través de una revisión inicial de la literatura sobre métodos para detectar y mitigar ataques de denegación de servicio. Esta problemática en particular pudo ser aplicada al campo de la inteligencia de negocios, dado que hay escasa investigación en este ámbito.
- La combinación de un algoritmo clasificador SVM y un controlador SDN ha posibilitado la aplicación de una solución de inteligencia empresarial que ayuda a reducir los ataques DDoS, que son cada vez más comunes. Esto permite al proveedor de servicios de Internet implementar políticas de seguridad de la información adicionales para asegurar la disponibilidad del servicio y destacarse como un valor adicional en un entorno altamente competitivo.
- Del análisis histórico de los años 2019 al 2021, permitió definir las principales amenazas y vulnerabilidades respecto a ataques de denegación de servicio ocurridos, dicha retroalimentación evidencio la hipótesis planteada y permite construir un modelo de inteligencia de negocios disponible para el periodo de tiempo del año 2022, de forma preventiva y correctiva mitiga ataques de denegación de servicio, apoyando a la toma de decisiones para le gestión empresarial.
- Se utilizó Power BI como herramienta para cumplir con el diseño del data warehouse, lo cual permitió analizar métricas en forma de valores tabulados. Estas métricas fueron objeto de ataques dirigidos principalmente a empresas financieras y gubernamentales. Las empresas financieras fueron blanco debido a su valor monetario, mientras que las gubernamentales fueron atacadas principalmente por motivos geopolíticos. Durante el año 2022, se logró contrarrestar la mayoría de estos ataques mediante el análisis de las

vulnerabilidades presentes en las empresas y promoviendo una cultura de seguridad de la información.

Recomendaciones

- Con mayor frecuencia los ataques de denegación de servicio distribuidos son explotados debido a vulnerabilidades que encuentra el atacante, estas pueden evitarse si se genera una cultura de ciberseguridad, una mentalidad por parte del ISP en todos sus niveles de que el riego existe y de esta forma permitirá que se pueda operar minimizando el riesgo con menor esfuerzo.
- Establecer diferentes mecanismos de protección con el uso de diferentes herramientas de machine learning como el uso de árbol de decisiones entre otros puede mejorar la eficiencia en la detección de ataques de denegación de servicios.
- Para el caso de la mitigación de ataques de denegación de servicios, existe una amplia gama de hardware, software y métodos, dependerá del costo, disponibilidad y eficiencia, como son Redes de distribución de contenido (CDNs), Balanceadores de carga, firewalls para ataques sofisticados de aplicaciones y restringir el tráfico directo de Internet de la infraestructura del ISP.
- Para este estudio se realizó el análisis de detección y mitigación para la capa de red, se puede analizar ataques de denegación de servicios para la capa de aplicaciones.

Referencias Bibliográficas

An, W., Aziz, M., & Songqing, C. (2017). *An Adversary-Centric Behavior Modeling of DDoS Attacks.* Atlanta, GA, USA: IEEE.

ARCOTEL. (2019). *www.arcotel.gob.ec*. Obtenido de www.arcotel.gob.ec: http://www.arcotel.gob.ec/wp-content/uploads/downloads/2018/08/ARCOTEL-2018-0652-2018-07-31-TELECOMUNICACIONES-MATRIZ.pdf

Barrett, E., Ili, K., & Desmond, C. (2019). *Feature dynamic deep learning approach for DDoS mitigation within.* Germany: Springer-Verlag.

Campo, E. (2018). Introducción a las máquinas de vector soporte (SVM) en aprendizaje supervisado. Zaragoza, Madrid.

Cano, J. (2007). *Business Inteligence, Competir con Información.* España: ESADE Business School.

Chambers, D., & Barrett, E. (2018). *A lightweight DDoS attack mitigation system within the ISP domain utilising self-organizing map.* Vancouver, Canada: Conference Paper, Springer Verlag.

Chen, S., & Song, Q. (2012). Perimeter-based defense against high bandwidth ddos attacks. *IEEE*, 16:526–537.

Chonka, A., Jaipal, S., & Zhou, W. (2013). Chaos theory based detection against network mimicking ddos attacks. *Comm. Letters*, 717–719.

Cisco Systems, I. (2018). Reporte Anual de Ciberseguridad de Cisco 2018. *El panorama de los ataques*, 33-36.

Cisco Systems, I. (2019). Reporte de amenazas. *Defiéndase contra amenazas críticas de la actualidad*, 9-10.

Cisco Systems, I. (2020). Reporte Anual de Ciberseguridad de Cisco. *El panorama de los ataques*, 35-40.

Cloudflare. (21 de Enero de 2021). *https://www.cloudflare.com/es-es/learning/ddos/ddos-mitigation/*. Obtenido de https://www.cloudflare.com/es-es/learning/ddos/ddos-mitigation/: https://www.cloudflare.com/es-es/learning/ddos/ping-of-death-ddos-attack/

Cueto Altahona, A. C. (18 de 11 de 2019). *https://manglar.uninorte.edu.co/handle/10584/8792#page=1*. Obtenido de https://manglar.uninorte.edu.co/handle/10584/8792#page=1

El telegrafo. (2019). *https://www.eltelegrafo.com.ec/noticias/politica/3/ataques-ciberneticos-desconeccion-ecuador*. Obtenido de https://www.eltelegrafo.com.ec/noticias/politica/3/ataques-ciberneticos-desconeccion-ecuador: https://www.eltelegrafo.com.ec/noticias/politica/3/ataques-ciberneticos-desconeccion-ecuador

Giralte, L., & Conde, C. (2013). Mitigating distributed denial of service by using multiple discipline queues. *IEEE*, 301–307.

Graham-Cumming, J. (2014). Understanding and mitigating NTP based DDoS attacks. *Cloudflare vol. 9. San Francisco*.

Gupta, A. V. (2013). Detecting MS initiated signaling DDoS attacks in 3G/4G wireless networks.InCommunication Systems and Networks (COMSNETS. *Fifth International Conference on. IEEE*, 1-60.

Ili, K., Desmond, C., & Barrett, E. (2019). *Unsupervised learning with hierarchical feature selection for DDoS mitigation within the ISP domain.* Galway, Ireland: John Wiley and Sons Inc.

INCIBE-CERT. (03 de 2020). *INCIBE-CERT*. Obtenido de INCIBE-CERT: https://www.incibe-cert.es/blog/medidas-proteccion-frente-ataques-denegacion-servicio-dos

Isha, A. M. (2013). Attacks on TCP/IP Layers in WSN. *International Journal of Computer Networks and Communications Security*, 20-45.

K. Mallikarjunan Narasimha, M. k. (2016). A survey of Distributed Denial of Service attack. *IEEE*, 2-5.

Kiattikul Treseangrat, S. S. (2015). Analysis of UDP DDoS cyber Flood Attack andDefence Mechanism on Windows Serevr 2012 and Linux Ubuntu. *IEEE*, 30-36.

Kimball, e. a. (2008). *The Data Warehouse Lifecycle Toolkit.* New York: Wiley 2nd Edition.

MSDN, M. (8 de 10 de 2022). *https://social.msdn.microsoft.com/Forums/es-ES/65d92eb6-eee6-4b0c-ad31-9a3b7c942744/datos-duplicados-enviados-a-access?forum=ssises*. Obtenido de Developer Network: http://www.dataprix.com/arquitectura-data-warehouse-areas-datos-nuestro-almacen-corporativo

Muñoz, H., Osorio, R., & Zuñiga, L. (2016). Inteligencia de los negocios, Clave del éxito en la era de la información. *Revista Clío América*, 2.

Narasimha, M., & Mercy, S. (2016). *A survey of Distributed Denial of Service attack.* Coimbatore, India: IEEE.

Obaid, R., Mohammad, A. G., & Chung-Horng, L. (2019). *DDoS Attacks Detection and Mitigation in SDN using Machine Learning.* Ottawa, Canada: IEEE World Congress on Services .

Pachés, A. J. (2020). Estudio del controlador SDN Ryu sobre una Raspberry-Pi Model 4. *Telecom*, 12-15.

Seufert, S., & O'Brien, D. (2011). Machine learning for automatic defence against distributed denial of service attacks. *In Proceedings of IEEE International Conference on Communications*, 1217–1222, 2007.

Siaterlis, C., & Maglaris, V. (2010). Detecting incoming and outgoing ddos attacks at the edge using a single set of network characteristics. *In Proceedings of the 10th IEEE Symposium on Computers and Commu-*, 469–475.

Silva, L. (s.f.). Business Intelligence: un balance para su implementación. *INNOVAG*, 3.

Sims, J. S. (2017). Securing Cloud, SDN and Large Data Network Environments from Emerging DDoS Attacks. *International Conference on Cloud Computing, Data Science Engineering- Confluence*, 466-469.

Sims, J. S.-p. (2017). Securing Cloud, SDN and Large Data Network Environments from Emerging DDoS Attacks. *International Conference on Cloud Computing, Data Science Engineering- Confluence*, 466-469.

Tasnuva Mahjabin, Y. X. (2020). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*, 4-9.

Tovar, C. (2017). Investigación sobre la aplicación de business intelligence en la gestión de las pymes de Argentina. *Palermo Business Review*, 5.

US-CERT. (26 de enero de 2021). *https://www.us-cert.gov/ncas/alerts/TA13-088A*. Obtenido de https://us-cert.cisa.gov/ncas/alerts/TA13-088A

Wang, L. a. (2015). Big Data Driven Supply Chain Management and Business Administration. *American Journal of Economics and Business Administration*, 60–67.

Wayner, X. B. (2018). Data Warehouse: Análisis Multidimensionalde BAFICI utilizando Power Pivot. *Espacios*, 24.

Yanlan Julio, P. L. (2018). Implementación de un Datamart como una solución de Inteligencia de Negocios para el área de logística de T-Impulso. *REVISTA DE INVESTIGACIÓN DE SISTEMAS E INFORMÁTICA*, 2.