DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
MAESTRÍA EN GESTIÓN DE SISTEMAS DE INFORMACIÓN E INTELIGENCIA DE NEGOCIOS

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER

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.

AUTOR: CARRION BASANTES SANTIAGO ANDRES
DIRECTOR: PhD. GUALOTUÑA ALVAREZ, TATIANA MARISOL

2023

Agenda

1. Introducción
2. Metodología
3. Desarrollo
4. Resultados
5. Conclusiones
6. Recomendaciones

1 **Introducción:** Antecedentes

DYN DNS

New York Times
Financial Times
Playstation Network
Reddit
Twitter
Spotify

50.000 - 100.000 IoT

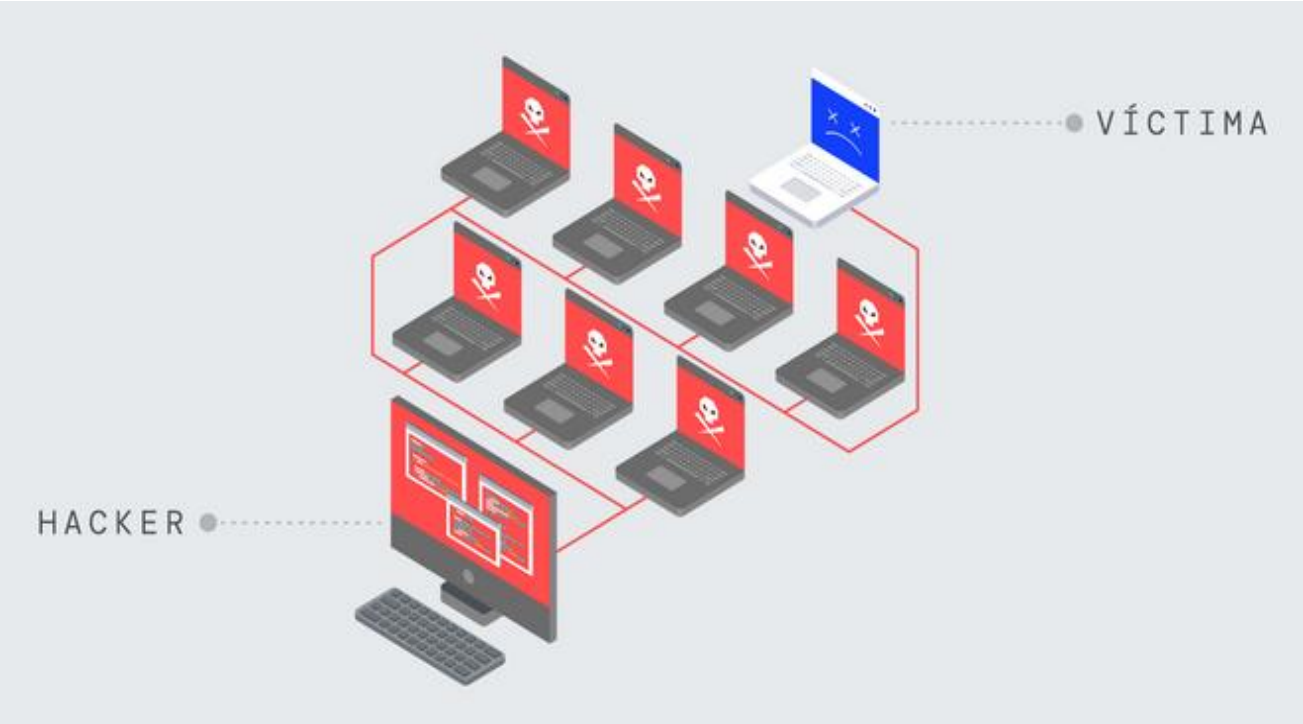
Botnets

48% Empresas
59% ISPs
2019

Aumento 20%

GRAFICO BASADO EN (OIT, 2019)

1 **Introducción:** Antecedentes



- **28 febrero 2018**
- **10 minutos**
- **1,35 Tbps**

- **abril del 2019**
- **300 entidades públicas**
- **133 ataques/seg**
- **Julian Assange**
- **31 en el ranking mundial**

1 Introducción: Problemática

Motivos

- Hacktivismo
- Cibervandalismo
- Rivalidades

Consecuencias mensurables

- Pérdida de ingresos
- Daño a la reputación y marca

- ARCOTEL

1 Introducción: Objetivos

Objetivos 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.

1 Introducción: Objetivos

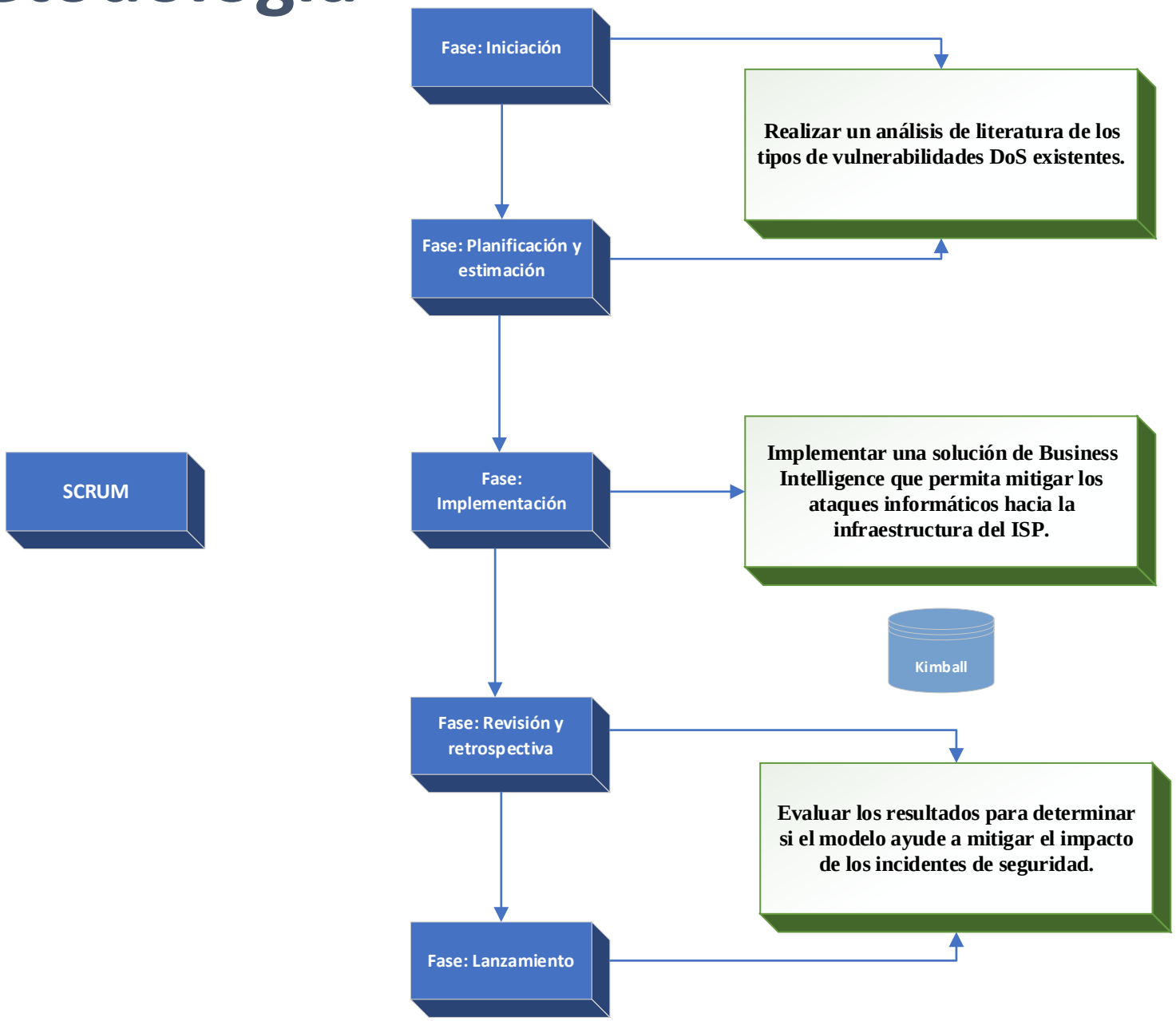
Objetivos Específicos

- Realizar un análisis de literatura de los tipos de vulnerabilidades DoS existentes.
- Implementar una solución de Business Intelligence que permita mitigar los ataques informáticos hacia la infraestructura del ISP.
- Evaluar los resultados para determinar si el modelo ayude a mitigar el impacto de los incidentes de seguridad.

1 Introducción: Alcance

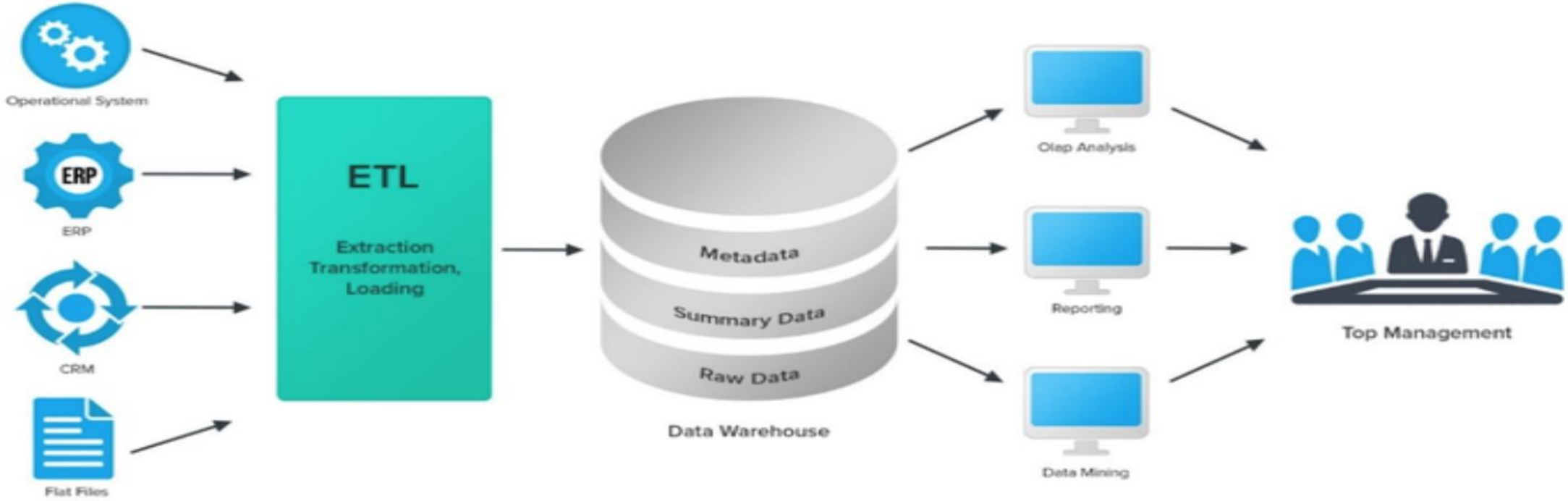
- Analizar los datos históricos
- Identificar el tipo de vulnerabilidad DDoS
- Modelo de inteligencia de Negocios
- Solución de mitigación de DDoS que combina, seguridad cibernética e inteligencia de negocios

2 Metodología



3 Desarrollo

Esquema General



BASE ORIGEN SQL SERVER

DATOS HISTORICOS

BASE DSA

PENTAHO DATA INTEGRATION

DESARROLLO DATA WAREHOUSE

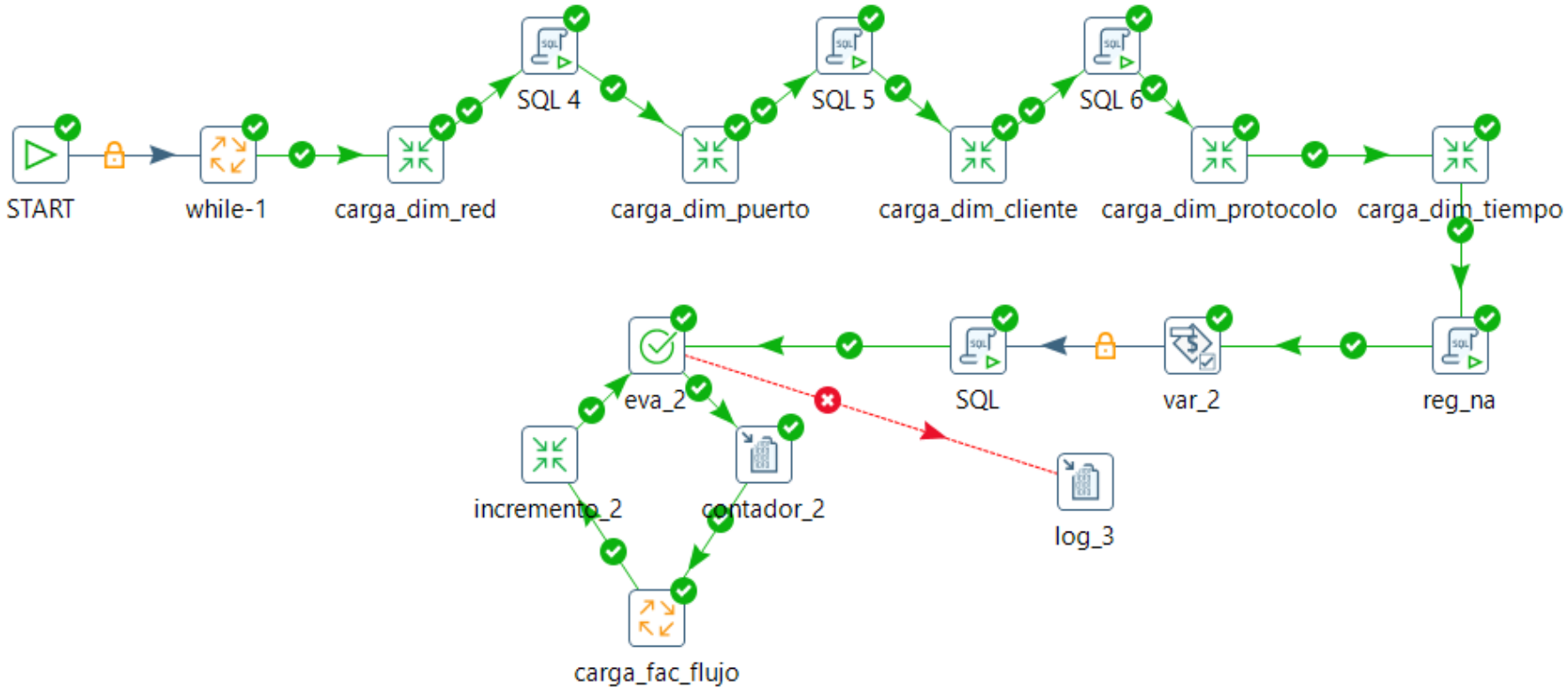
MODELO KIMBALL

VISUALIZACIÓN DE RESULTADOS

POWER BI

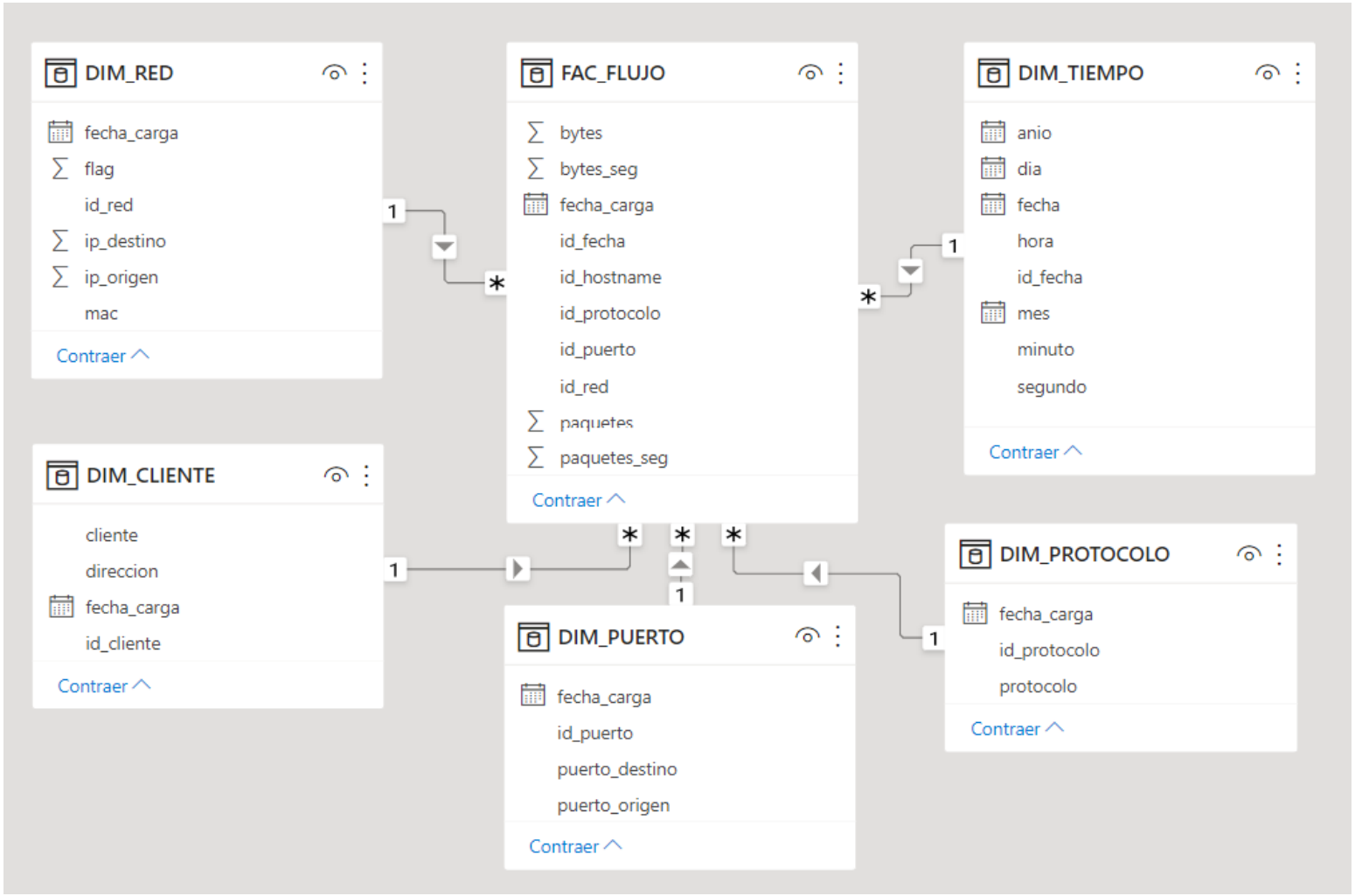
3 Desarrollo

Proceso ETL, Carga DSA y DWH dimensiones y tabla de hechos



3 Desarrollo

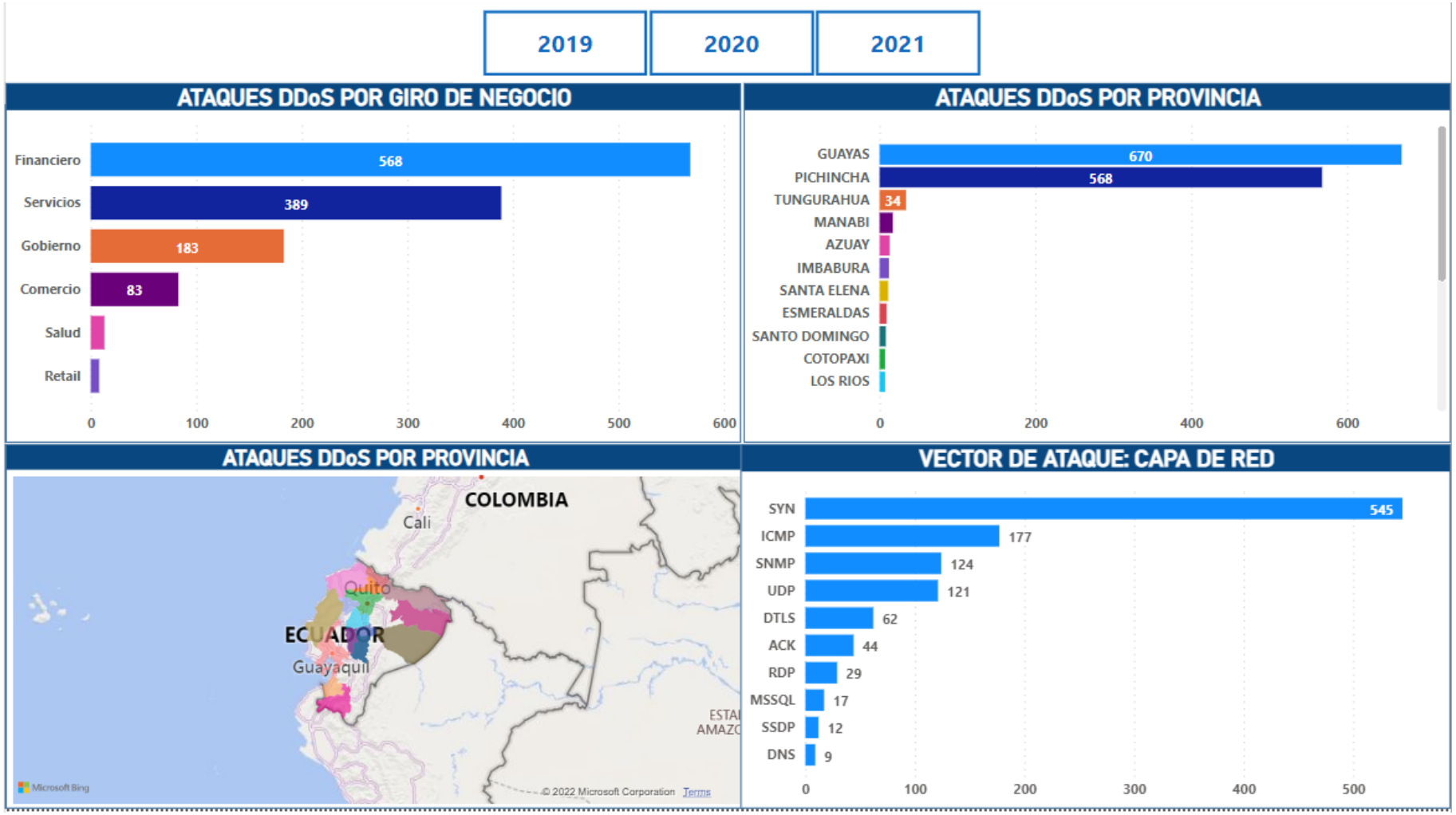
Modelo Dimensional Metodología Kimball



4 Resultados

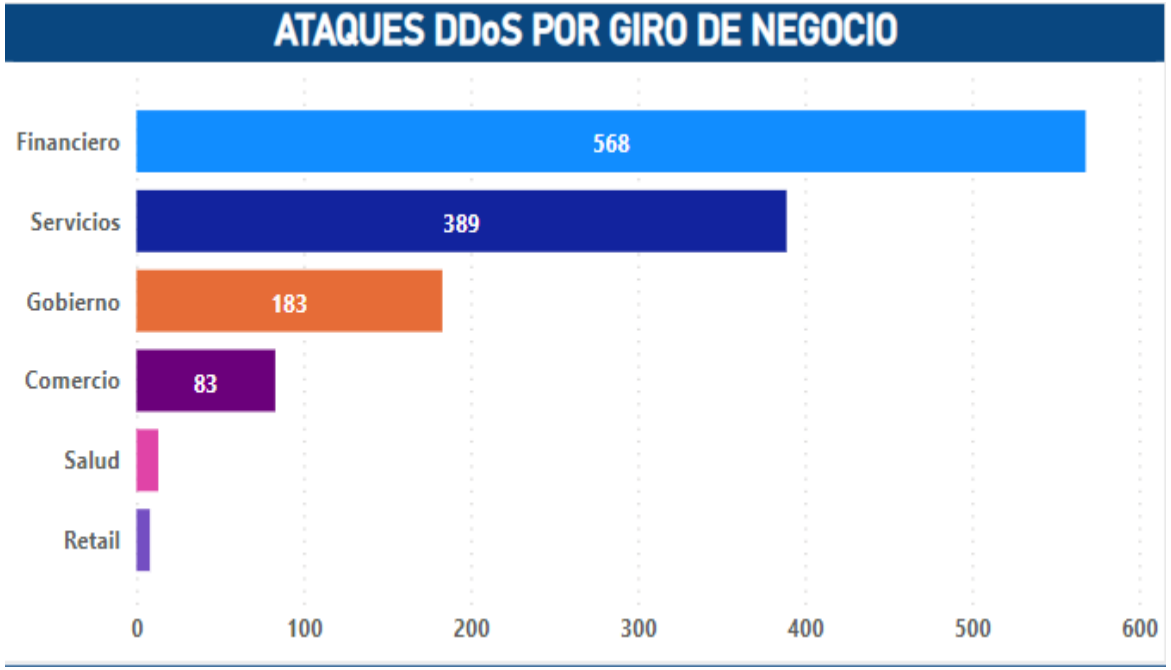
Análisis de ataques DDoS por giro de negocio y provincia

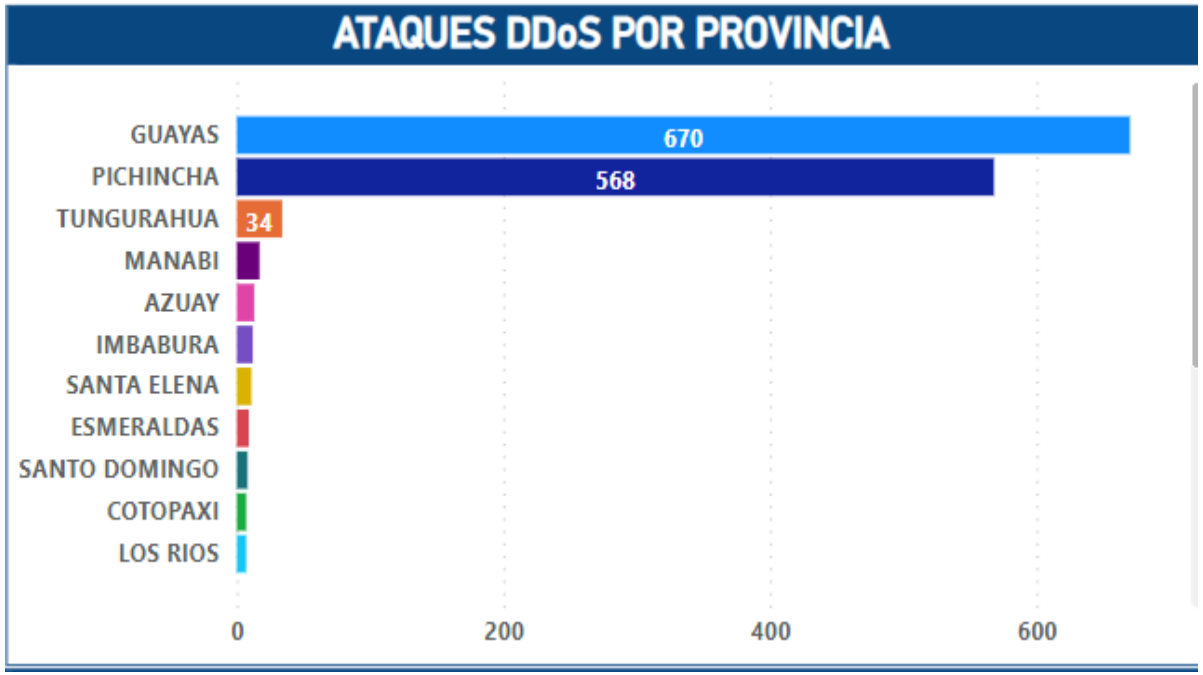
Análisis de ataques DDoS por vector de ataque



4 Resultados

Ataques DDoS

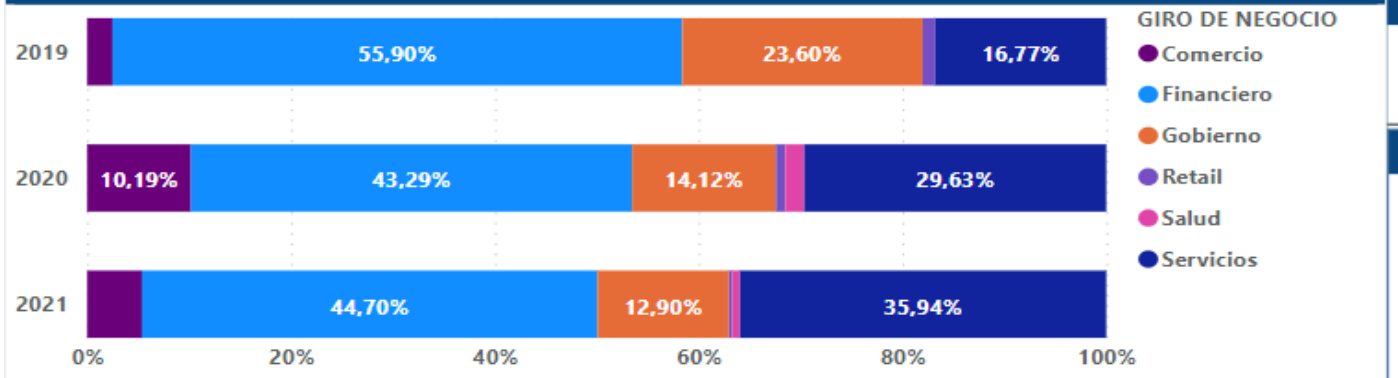




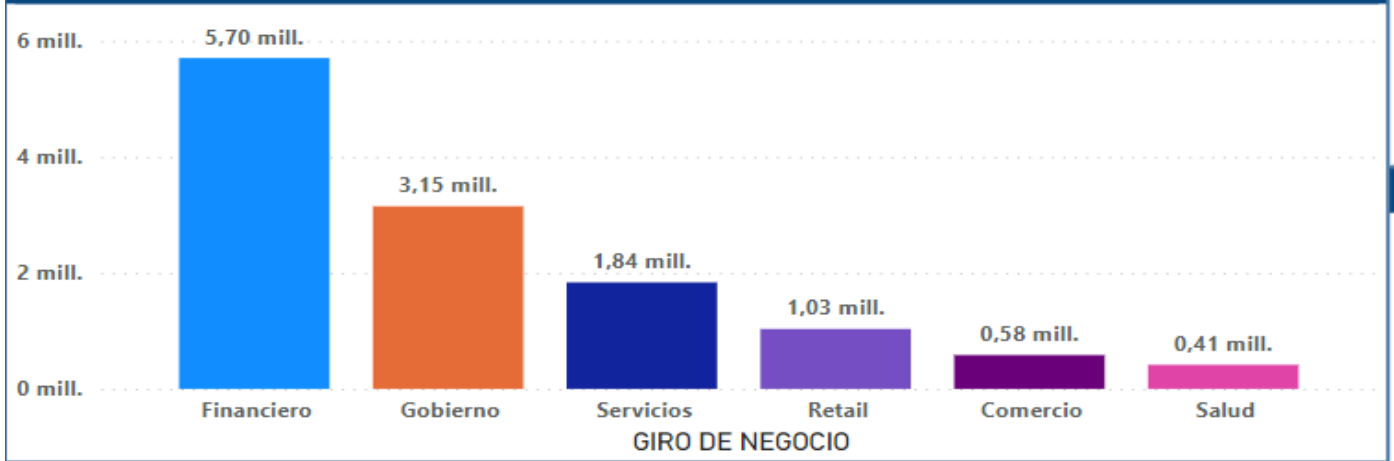
4 Resultados

Tendencias de ataques DDoS

ATAQUES DDoS POR AÑO



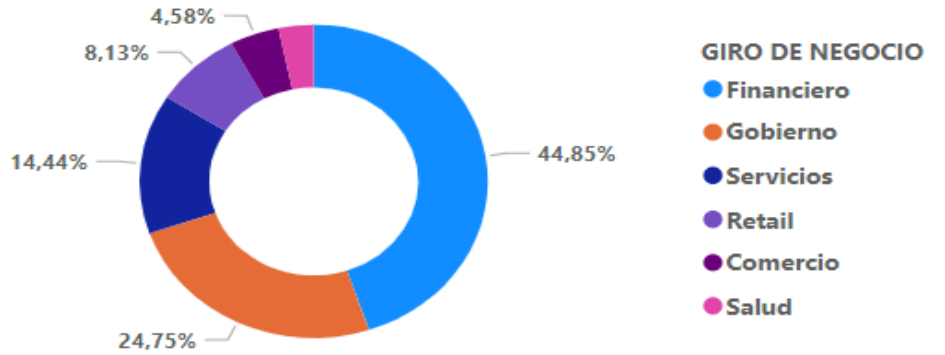
VELOCIDAD EN BYTES (KB) DE ATAQUES DDoS



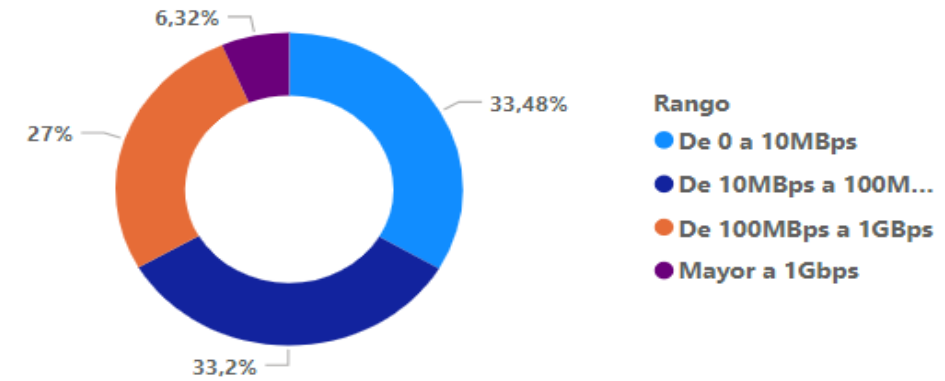
DURACIÓN MÁXIMA DE ATAQUE	VOLUMEN MÁXIMO DE ATAQUE (KB)
18:28:48	2,40 mill.

NÚMERO DE ATAQUES 2019	NÚMERO DE ATAQUES 2020	NÚMERO DE ATAQUES 2021
161	432	651

DISTRIBUCIÓN POR VELOCIDAD EN BYTES (KB)



ATAQUE DE MAYOR IMPACTO



5 Conclusiones

- Revisión de literatura - Scrum - Kimball
- Algoritmo ML - SDN - Mitigar ataques DDoS
- Análisis histórico – amenazas y vulnerabilidades – modelo BI
- Analizar métricas – vector de ataques - mitigación

6 Recomendaciones

- Aplicar políticas de ciberseguridad
- Herramientas de ML
- Mitigación de ataques
- Análisis para capas de aplicación

Gracias!