ANÁLISIS Y AUTOMATIZACIÓN DE CAPACIDAD Y TRÁFICO DE LA RED BANCO AV VILLAS

JULIAN CUERVO GIL

UNIVERSIDAD SANTO TOMAS
INGENIERÍA DE TELECOMUNICACIONES
OPCIÓN DE GRADO
2023

ANÁLISIS Y AUTOMATIZACIÓN DE CAPACIDAD Y TRÁFICO DE LA RED BANCO AV VILLAS

RAFAEL ORLANDO CUBILLOS SÁNCHEZ

UNIVERSIDAD SANTO TOMAS
INGENIERÍA DE TELECOMUNICACIONES
OPCIÓN DE GRADO
BOGOTÁ
2023

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Ciudad y Fecha (día, mes, año) (Fecha de entrega)

Contenido

LISTA DE TABLAS 4
LISTA DE FIGURAS 5
1. CAPÍTULO 1 6
1.1 MARCO GENERAL INTRODUCTORIO 6
1.2 INTRODUCCIÓN 6
1.3 PLANTEAMIENTO DEL PROBLEMA 7
Pregunta problema 7
1.4 Objetivos 8
Objetivo general 8
Objetivos Específicos 8
1.5 ALCANCE 9
1.6 MARCO TEÓRICO 9
TRAFICO DE RED 10
1.7 INDICADORES DISPUESTOS PARA LA IMPLEMENTACION Y MEDICION DE LAS MEJORAS SOBRE LA CAPACIDAD DE LA RED Y PROCESOS ADYACENTES 13
2 CAPITULO 2 15
2.2 METODOLOGIAS Y DESARROLLO DE LA SOLUCION 15
2.3 METODOLOGIAS A IMPLEMENTAR PARA EL DESARROLLO DE INDICADORES 15
METODOLOGIA DE OBTENCION Y LIMPIEZA DE DATOS 15
METODOLOGIA PARA EL DESARROLLO E IMPLEMENTACION DE LA SOLUCION: 16
2.4 PROCESO DE LA SOLUCION PREVIA A LA AUTOMATIZACIÓN 17
2.5 ANALISIS DE RESULTADOS AL TERMINO DE LA SOLUCION PREVIA 22
3. CAPITULO 3 24
3.1 INTRODUCCIÓN 24
3.2 DESARROLLO DE LA AUTOMATIZACION DE LA SOLUCION 24
3.3 Desarrollo de herramienta para el procesamiento de texto 24
3.4 Modelación de tráfico sobre el tiempo 32
3.5 ANALISIS DE RESULTADOS FINALES 32
3.6 CONCLUSIONES Y RECOMENDACIONES 36
REFERENCIAS 38

LISTA DE TABLAS

Tabla 1 Formato de información posterior al proceso (fuente propia)..... 21

LISTA DE FIGURAS

Figura 1 Nexus 7000.....11
Figura 2 Nexus 5000.....12
Figura 3 Nexus 9000.....12
Figura 4 Resultado gráfico para la información preliminar recolectada en Power BI selección de todos los equipos 19
Figura 5 Resultado gráfico para la información preliminar recolectada en Power B selección de un equipo 19
Figura 6 Resultado grafico para la información preliminar recolectada en Power B selección de todos algunos equipos 20
Figura 7 Trafico por puerto X tiempo 32

1. CAPÍTULO 1

1.1 MARCO GENERAL INTRODUCTORIO

1.2 INTRODUCCIÓN

Como practicante en el área de telecomunicaciones del Banco Av Villas desempeñando diferentes tareas dentro del área, en conjunto con el equipo se evidencio una necesidad desempeñando tareas de monitoreo de red, puesto que la actualidad del banco no permite dirigir presupuesto para aumentar el nivel de las licencias de servicios que se usan para el monitoreo de la red administrada por esta área.

Esto se evidencio al tratar de buscar formas más eficientes de realizar tareas que el equipo de telecomunicaciones realiza usualmente en el banco como análisis de tráfico, despliegue automático de configuración de equipos de red, revisión de cumplimiento de políticas de seguridad desde los recursos tecnológicos administrados por la entidad, así como atención de cara a los usuarios para los servicios internos del banco que dependen de esta área.

A raíz de una solicitud de la superintendencia en donde se debía entregar un informe de capacidad de la red, teniendo en cuenta la limitante económica y con el fin de dar cumplimiento al requerimiento de la superintendencia se planteó implementar algo sencillo que permitiera mostrar información más detallada en el informe solicitado.

1.3 PLANTEAMIENTO DEL PROBLEMA

La falta de una gestión efectiva de la capacidad de la red en la organización ha generado decisiones erróneas por parte del equipo de telecomunicaciones. Esto se evidencia en la baja frecuencia de informes de capacidad, los cuales solo se presentan en respuesta a solicitudes externas, en lugar de ser una práctica interna regular. La información requerida en estos informes, especialmente por la superintendencia financiera, es superficial y carece de detalles cruciales para una toma de decisiones precisa.

La carencia de importancia dada a la capacidad de la red se ha traducido en problemas financieros, como la sobreestimación de recursos en proyectos de actualización de equipos. La falta de información detallada ha llevado a costos adicionales y decisiones equivocadas, como la sustitución de equipos sin considerar su ocupación real.

Además, la ausencia de informes de capacidad afecta proyectos paralelos, como la recolección de líneas telefónicas sin uso. La falta de monitoreo continuo de la ocupación y tráfico de la red limita la eficacia de estos proyectos y complica la gestión general de la red.

En resumen, la ineficiencia en la gestión de la capacidad de la red ha impactado negativamente en la toma de decisiones, generando sobrecostos y afectando la ejecución de proyectos críticos para la organización.

Pregunta problema

Con base en las problemáticas identificadas, ¿Cómo podemos extraer, procesar y hallar valor de información que sea relevante para solventar la necesidad del área de telecomunicaciones?

1.4 Objetivos

Objetivo general

Implementar una solución mediante el uso de diferentes herramientas y metodologías que automatice el proceso de extracción, procesamiento y análisis de información referente del tráfico de la red del Banco Av Villas.

Objetivos Específicos

- Seleccionar un subconjunto representativo de equipos de red en varias sucursales que pertenezcan a la capa CORE y llevar a cabo un monitoreo del tráfico en un periodo corto de tiempo.

- Analizar los resultados de los procesos de la implementación con el fin de satisfacer los requerimientos impuestos por el equipo de telecomunicaciones de la entidad

- Generar un análisis final en donde se evidencien las principales características y beneficios que puede traer el realizar un monitoreo constante con la implementación.

1.5 ALCANCE

- **Implementaciones propuestas**

El alcance de esta implementación está dirigido únicamente a la capa CORE de la red del Banco, elección hecha a petición de la dirección del área de telecomunicaciones de la entidad. Adicionalmente, en la fase funcional de la implementación no se podrán documentar muestras a periodos superiores de 3 o 4 muestras en un día debido a la limitante de la duración del contrato de aprendizaje.

Teniendo en cuenta el rigor del control ejercido sobre la red del banco por parte del equipo de ciberseguridad, las pruebas que eran permitidas fueron limitadas por día debido a las conexiones ssh que implicaría poder hacer pruebas ilimitadas sobre la red en operación.

Para el análisis de los datos obtenidos durante el proceso de esta implementación, se hará uso de la herramienta de visualización y modelado de datos Power BI, elección realizada debido a las licencias con las que cuenta el banco.

1.6 MARCO TEÓRICO

GESTIÓN DE LA CAPACIDAD

“El propósito de la práctica de gestión de la capacidad y el desempeño es asegurar que los servicios logren el desempeño acordado y esperado, satisfaciendo la demanda actual y futura de una manera rentable. El desempeño son actividades realizadas en un período de tiempo requerido para cumplir con la demanda de servicio. El rendimiento del servicio depende de la capacidad del servicio, que se define como el rendimiento máximo que puede ofrecer un CI o un servicio de TI. Las métricas específicas de capacidad y rendimiento dependen de la tecnología y la naturaleza del servicio o CI. La práctica de gestión de la capacidad y el rendimiento se ocupa del rendimiento del servicio y el rendimiento de los recursos tecnológicos sobre los cuales se apoya, como la infraestructura, las aplicaciones y los servicios de terceros. La práctica de gestión de la capacidad y el desempeño también cubre la capacidad y el desempeño del personal.”

STERLING BASTIDAS, Ana María y CÓRDOBA GÓMEZ, Luis Clímaco. GUÍA DOMINIO MGGTI.G.ST - GESTIÓN DE SERVICIOS DE TI. https://www.mintic.gov.co/portal/inicio/ [página web]. (1, octubre, 2023). [Consultado el 28, diciembre, 2023]. Disponible en Internet: <https://www.mintic.gov.co/arquitecturaempresarial/630/articles-237663_recurso_1.pdf>.

Las principales actividades de la Gestión de la Capacidad se resumen en:

- Desarrollo del Plan de Capacidad

- Modelado y simulación de diferentes escenarios de capacidad
- Monitorización del uso y rendimiento de la infraestructura TI
- Análisis de rendimiento y capacidad del servicio
- Investigación y seguimiento del desempeño actual del servicio-
- Análisis de requisitos de capacidad
- Previsión de la demanda y planificación de recursos
- Planificación de la mejora del rendimiento.

TRAFICO DE RED

“El tráfico de red (también llamado tráfico o tráfico de datos) hace referencia a los datos que se desplazan por una red en un momento determinado. Los datos de la red están compuestos por paquetes, que son las unidades fundamentales más pequeñas de datos que se transmiten por una red. Los datos del tráfico de red se desglosan en estos paquetes para su transmisión y vuelven a armarse al llegar a destino. Los paquetes están formados por cargas (datos sin procesar) y encabezados (metadatos) que contienen información, como las direcciones IP de origen y destino.”

MONITOR DEL tráfico de red: ver, analizar y optimizar el tráfico | SolarWinds [Anónimo]. Observability and IT Management Platform | SolarWinds [página web]. (6, junio, 2023). [Consultado el 28, diciembre, 2023]. Disponible en Internet: <https://www.solarwinds.com/es/network-bandwidth-analyzer-pack/use-cases/network-traffic-monitor>.

AUTOMATIZACION DE REDES

“La automatización de red es el proceso de automatizar la configuración, la administración, las pruebas, la implementación y la operación de dispositivos físicos y virtuales en una red. La disponibilidad de los servicios en red mejora al automatizar las tareas y funciones de red cotidianas, y controlar y administrar automáticamente los procesos repetitivos.

Todo tipo de red puede usar la automatización de red. Las soluciones basadas en hardware y software permiten que los centros de datos, los proveedores de servicios y las empresas implementen la automatización de la red para mejorar la eficiencia, reducir el error humano y bajar los gastos operativos.”

MONITOR DEL tráfico de red: ver, analizar y optimizar el tráfico | SolarWinds [Anónimo]. Observability and IT Management Platform | SolarWinds [página web]. (6, junio, 2023). [Consultado el 28, diciembre, 2023]. Disponible en Internet: <https://www.solarwinds.com/es/network-bandwidth-analyzer-pack/use-cases/network-traffic-monitor>.

Figura 1 Nexus 7000

“El Cisco Nexus 7000 es un switch de centro de datos de alta capacidad, diseñado por Cisco Systems. Destaca por su arquitectura modular, alta densidad de puertos, conmutación de alto rendimiento y redundancia para garantizar la disponibilidad. Su sistema operativo NX-OS proporciona una gestión eficiente y una variedad de servicios de red avanzados, cuenta con una memoria de 12,6 GB”

Cisco Systems. "Cisco Nexus 7000: Switches para centros de datos". Recuperado de https://www.cisco.com/c/es_es/products/switches/data-center-switches/index.html#~customer-stories

Figura 2 Nexus 5000

“El Cisco Nexus 5000 es un switch de centro de datos compacto y eficiente, diseñado por Cisco Systems. Destaca por su diseño modular, capacidad de conmutación de alto rendimiento y opciones flexibles de conectividad. Sus características incluyen un equilibrio óptimo entre capacidad de procesamiento y memoria para satisfacer las demandas de entornos empresariales dinámicos.”

Cisco Systems. "Cisco Nexus 5000: Switch compacto para centros de datos". Recuperado de Switches de Data Center: Cisco Nexus - Cisco

Figura 3 Nexus 9000

“El Cisco Nexus 9000 es un switch avanzado diseñado por Cisco Systems para entornos de centros de datos de alto rendimiento. Con una arquitectura escalable, ofrece características destacadas como alta densidad de puertos, conmutación eficiente y flexibilidad de conectividad. Equipado con potentes capacidades de

procesamiento y memoria, el Nexus 9000 proporciona un rendimiento robusto para satisfacer las exigencias de las redes empresariales modernas.”

Cisco Systems. "Cisco Nexus 9000: Switch de alto rendimiento para centros de datos". Recuperado de Switches de Data Center: Cisco Nexus - Cisco

1.7 INDICADORES DISPUESTOS PARA LA IMPLEMENTACION Y MEDICION DE LAS MEJORAS SOBRE LA CAPACIDAD DE LA RED Y PROCESOS ADYACENTES

Tras identificar los principales problemas relacionados con la gestión de la capacidad de la red y los procesos que intervienen en la elaboración de un informe de capacidad, se han generado diversos indicadores. Estos indicadores buscan medir las ventajas obtenidas con los nuevos procesos, metodologías e implementaciones, en comparación con los métodos previamente utilizados para estos mismos procesos.

- **Información contenida en la solución**

  Mostrar como la información que se obtiene a través del uso de la metodología e implementación propuesta da más valor que la información previamente manejada.

- **Cantidad de muestras reportadas en el informe**

  Definir la frecuencia para la generación del reporte, para lograr establecer un periodo óptimo para el monitoreo.

- **Toma de decisiones**

  Al recrear posibles escenarios reales en donde el nuevo informe tenga presencia en la toma de decisiones, se pretende demostrar en este indicador la ventaja en materia económica que brinda la toma de decisiones con fundamento en información con un mayor valor y más aproximada a la realidad de la red.

- **Monitoreo preventivo**

  Al poseer información que permita tener una idea mucho más acertada acerca del estado de la red, posibilitará periódicamente realizar diferentes análisis para identificar y diagnosticar a tiempo, posibles alteraciones a la normalidad de la red.

- **Automatización y simplificación**

  Desarrollando este indicador se espera generar una metodología acompañada de implementaciones las cuales reduzcan la complejidad y

el tiempo empleado para la creación de reportes e informes de capacidad de la red sin sacrificar la calidad de estos, dejando evidencia de la mejora desarrollada para la gestión de la capacidad frente a lo existente previamente.

2 CAPITULO 2

2.1 INTRODUCCIÓN

Las metodologías utilizadas a continuación fueron construidas de manera autonoma mediante el desarrollo de la implementación y ajustadas con recomendaciones hechas por el equipo de telecomunicaciones de la entidad, adicionalmente, para la obtención de datos y su limpieza, la metodología usada adapto el planteamiento básico del análisis de datos al caso de uso en cuestión. Una vez fue avanzando el desarrollo de la implementación, las metodologías descritas más adelantes fueron construidas.

2.2 METODOLOGIAS Y DESARROLLO DE LA SOLUCION

2.3 METODOLOGIAS A IMPLEMENTAR PARA EL DESARROLLO DE INDICADORES

METODOLOGIA DE OBTENCION Y LIMPIEZA DE DATOS

1. Establecimiento de indicadores de la implementación.

2. Elección del modelo de medición para los indicadores (muestreo).

3. Elección de las herramientas necesarias para la obtención y limpieza de los datos.

4. identificación de equipos a tratar.

5. Entrega de la información para ser procesada.

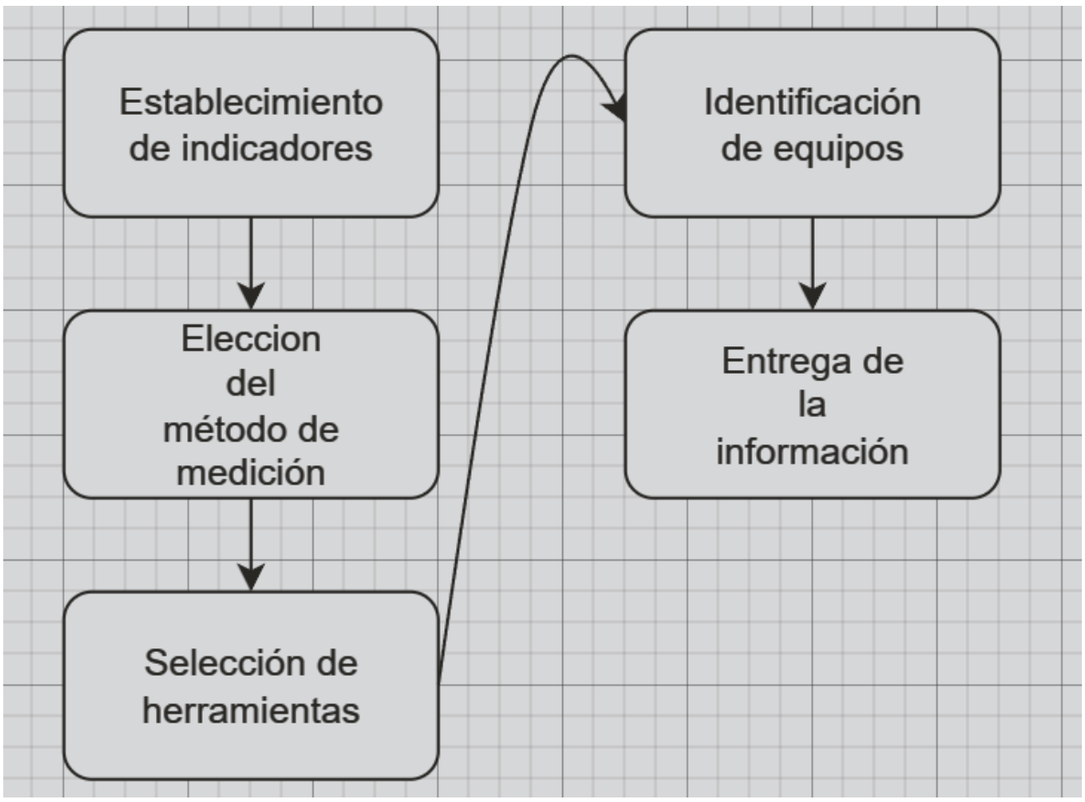


Figura 4 Diagrama metodología para la obtención de datos. (Elaboración propia)

METODOLOGIA PARA EL DESARROLLO E IMPLEMENTACION DE LA SOLUCION:

1. Análisis de los datos previo a ser procesados.

2. Establecimiento de un proceso preliminar (Proceso de extracción y procesamiento de datos no automatizado)

3. procesamiento de los datos obtenidos.

4. Elección de herramienta de modelación.

5. modelación de los datos.

6. Revisión de los resultados preliminares.

7. Establecimiento de recomendaciones y mejoras.

8. Implementación final (alcance de las mejoras recomendadas)

9. Desarrollo automatizado de la solución

10. Análisis de los resultados

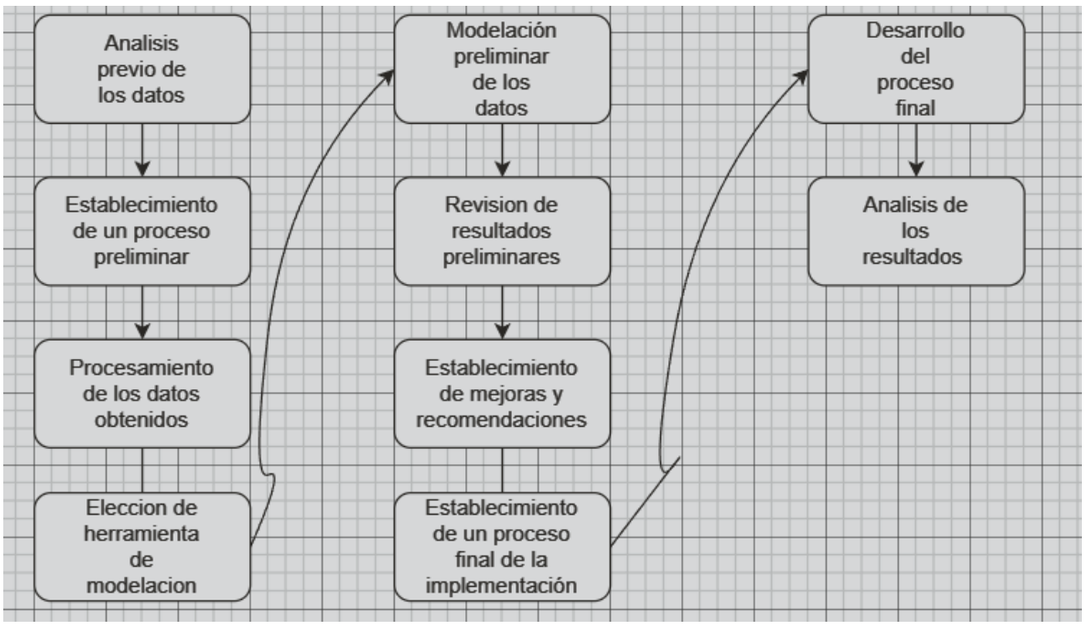


Figura 5 Diagrama del desarrollo e implementación de la solución (Elaboración propia)

2.4 PROCESO DE LA SOLUCION PREVIA A LA AUTOMATIZACIÓN

- **Identificación de los equipos pertinentes:**

Se analiza la arquitectura de red del Banco, dando así con los equipos que pertenecen a la capa CORE de esta y que se encuentren presentes en el centro de cómputo principal de la entidad, así como sus equipos de respaldo ubicados en el centro de cómputo de contingencia.

- **Obtención de la información**

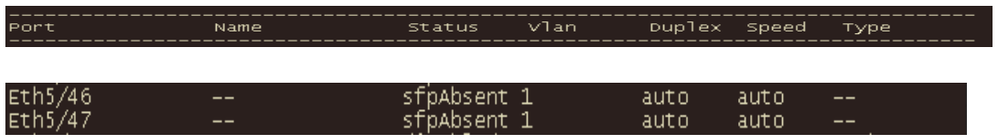
Manualmente sobre los 11 equipos objeto de estudio (a petición de la dirección de telecomunicaciones) presentes en la capa CORE del banco se ejecutaron diferentes comandos para la obtención de la información necesaria para ser procesada posteriormente, dicho proceso fue el siguiente:

- **Ocupación física de los puertos de los equipos:**

Al ser estos equipos del fabricante CISCO, se ejecutó manualmente a todos los equipos el siguiente comando:

```
# show int status
```

El cual nos dará la siguiente información en respuesta a su ejecución:



En este comando esperamos encontrar diferentes estados de los puertos como el que se encuentra presente en la ilustración anterior o como los siguientes:

Estos son los diferentes estados los cuales son los identificadores del estado del puerto de los que se obtendrá la información de la ocupación de los equipos mencionados.

Siguiendo este formato de tabla arrojado por los equipos Cisco, los cuales son objeto de estudio, se plantearon algunas preguntas las cuales se podrían responder con esta información:

- ¿Cuántos puertos hay disponibles en toda la capa CORE del banco?
- ¿Cuáles son los equipos con mayor sobre estimación de su capacidad? (Equipos con mayor cantidad de puertos sin utilizar)
- ¿Qué dispositivos concentran un flujo mayor transferencia de datos al sobre esta capa?

Para responder a estas preguntas, se utilizó una herramienta que será parte integral de la solución final. PowerBI es la herramienta seleccionada para modelar gráficamente los datos, proporcionando una comprensión más profunda de los mismos. Al analizar y contrastar los datos para responder a estas preguntas, se

obtuvieron los siguientes resultados de la modelación gráfica:

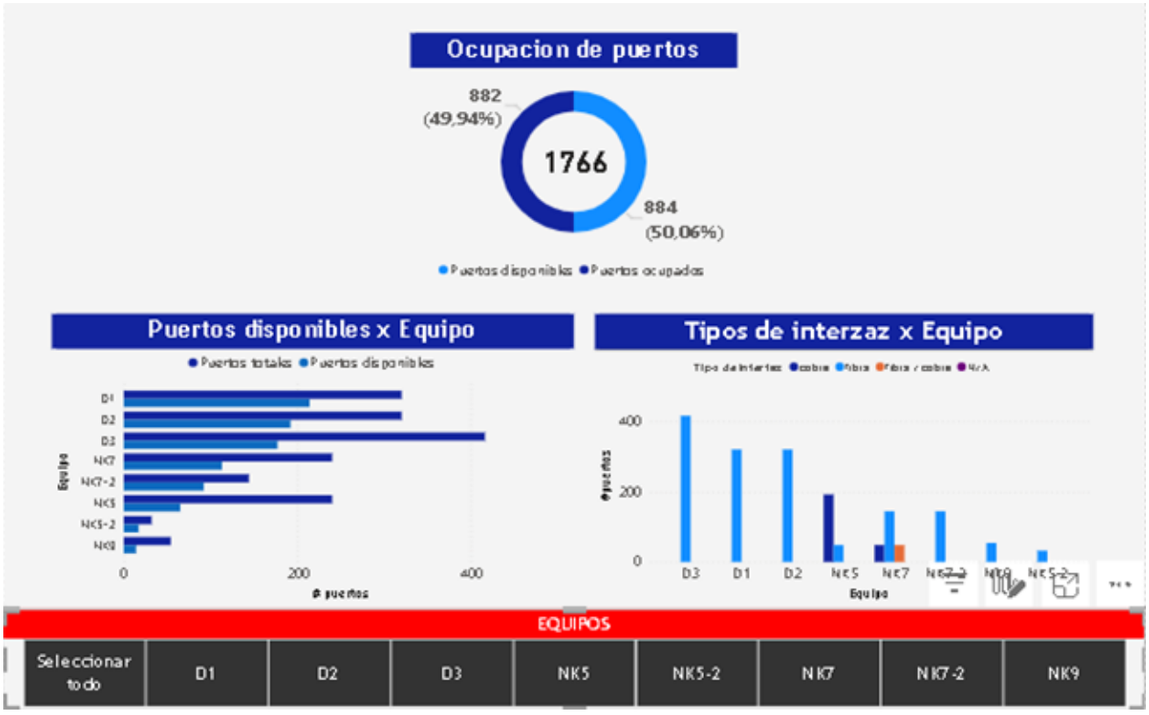


Figura 6 Resultado gráfico para la información preliminar recolectada en Power BI selección de todos los equipos (fuente propia)

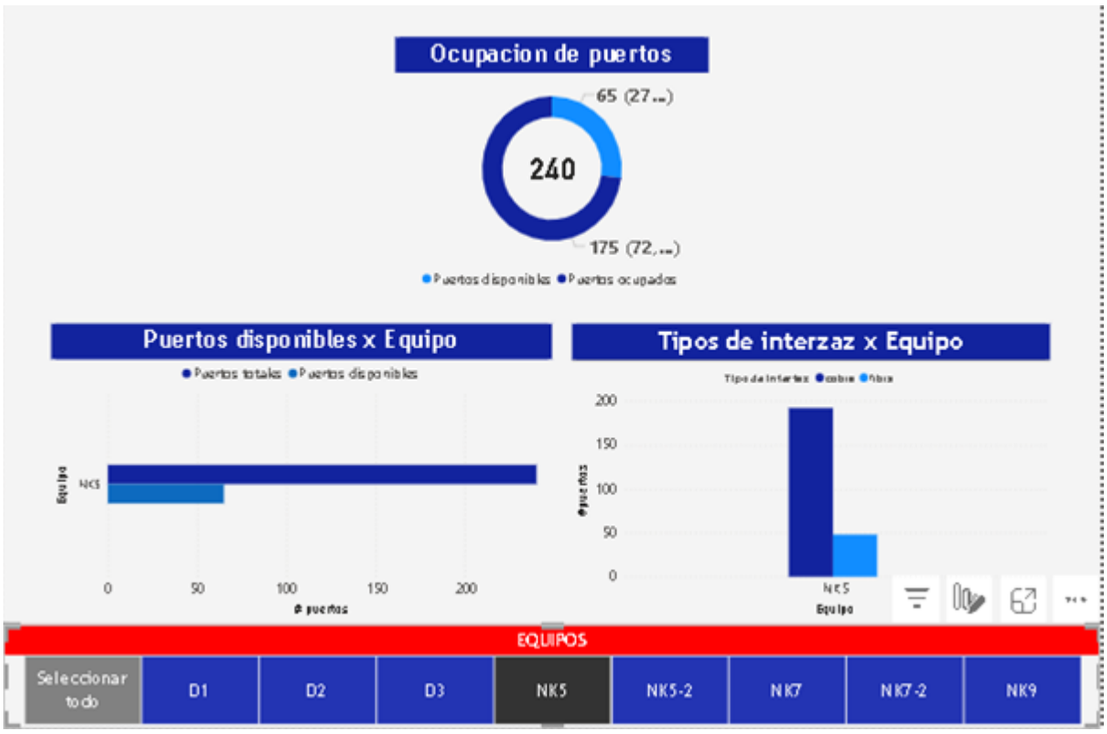


Figura 7 Resultado gráfico para la información preliminar recolectada en Power B selección de un equipo (fuente propia)

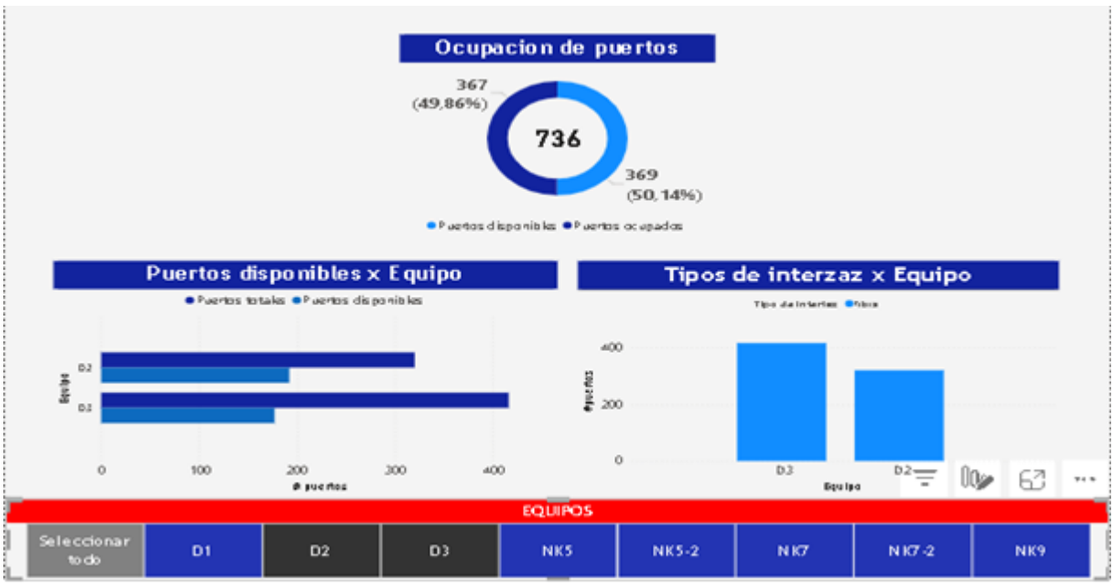


Figura 8 Resultado grafico para la información preliminar recolectada en Power B selección de todos algunos equipos (fuente propia)

En el gráfico de Power BI se presenta una interfaz que visualiza todos los equipos CORE del banco. Puedes seleccionar cada equipo para ver en pantalla los puertos disponibles y los tipos de interfaz asociados. También, tienes la capacidad de comparar estas características entre varios equipos.

Este análisis proporciona insights sobre la capacidad de los equipos, lo que puede ser útil para decisiones de renovación de la red o dar información acerca del estado de estimación de capacidad hecho por la entidad. Sin embargo, para abordar completamente las problemáticas planteadas, es esencial incorporar un análisis del tráfico, que es el objeto de mayor valor en la propuesta de implementación.

- **Limpieza y agregación de formato de base de datos**

  De igual manera que en la obtención de la información, esta limpieza y ordenamiento de los datos en una base de datos, en este caso Excel se realizó manualmente, esto aparte de que esta información solo contaba con el estado de conexión de los puertos, mas no con el tráfico que fluía a través de ellos, la información se obtuvo con el siguiente formato traído de los equipos utilizando comandos como se detalla a continuación:

  - Trafico en instante de tiempo de los puertos de los equipos capa CORE:

En búsqueda de comandos los cuales permitan obtener la información requerida sin que esta contenga información innecesaria, probando de diferentes maneras, finalmente se determinó el comando que supliera la necesidad el cual es el siguiente:

```
# show int | in ETH|300
```

El cual emite la siguiente información en respuesta a su ejecución.

```
Ethernet3/1 is up
  Hardware: 1000/10000 Ethernet, address: 0c11.67ea.3d08 (bia 0c11.67ea.3d08)
  EtherType is 0x8100
  Load-Interval #2: 5 minute (300 seconds)
    300 seconds input rate 120960160 bits/sec, 23151 packets/sec
    300 seconds output rate 188632120 bits/sec, 24185 packets/sec
```

El comando nos permite ver únicamente el puerto y su tráfico promedio correspondiente al intervalo de los últimos 5 minutos a través de este puerto en bits por segundo en un formato el cual requiere ser procesado para obtener la información como se requiere lo cual será tratado a continuación.

Como se mencionó, este proceso se realizó manualmente, por lo que está sujeto a un número mayor de errores, sin embargo, la obtención del formato deseado se completó y dicho formato se puede ver a continuación:

Puerto	Status	Input rate (Mbits/sec)	Output rate (Mbits/sec)	TRAFICO
Ethernet3/1	Up	55,542608	366,334744	421,877352
Ethernet3/2	Up	45,287512	50,405672	95,693184
Ethernet3/3	Up	682,014576	299,428088	981,442664
Ethernet3/4	Up	386,280048	404,0754	790,355448
Ethernet3/5	Down (Administratively down)	0	0	0
Ethernet3/6	Down (SFP not inserted)	0	0	0
Ethernet3/7	Down (SFP not inserted)	0	0	0
Ethernet3/8	Down (SFP not inserted)	0	0	0
Ethernet3/9	Down (Administratively down)	0	0	0

Tabla 1 Formato de información posterior al proceso (fuente propia)

En la tabla se evidencia la claridad que representan los datos al ser extraídos y organizados de esta manera para poder seguir siendo procesados.

a continuación, se podrá observar el resultado del procesamiento completo de los datos luego de ser extraída la información de la tabla anterior y ser modelada en Power Bi.

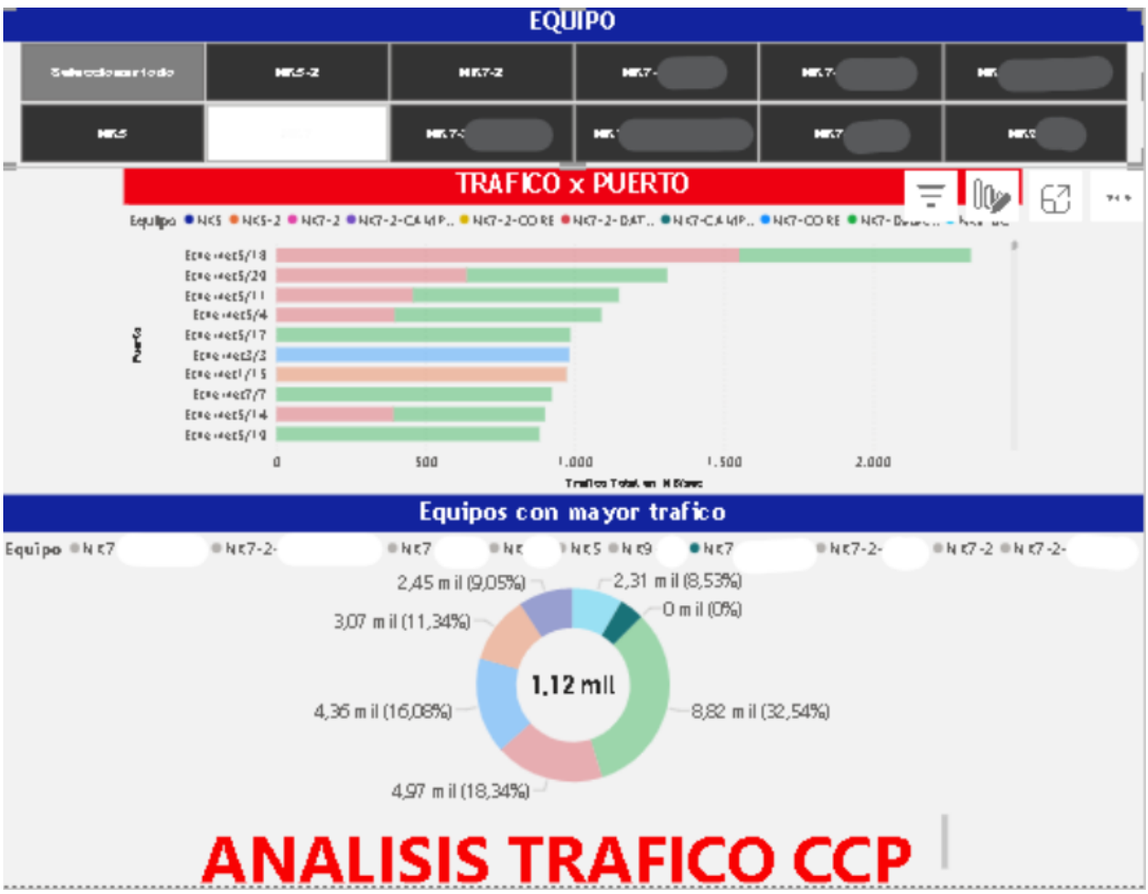


Figura 9 Análisis de tráfico capa CORE (fuente propia)

2.5 ANALISIS DE RESULTADOS AL TERMINO DE LA SOLUCION PREVIA

Al analizar minuciosamente la información recopilada mediante el procedimiento mencionado anteriormente, se concluyó que dicha información, al incorporar ajustes o características adicionales, podría tener un valor considerable por las razones que se detallan a continuación:

- Añadiendo información en periodos de tiempo determinados aumentaría la posibilidad de establecer diagnósticos basados en el tráfico o en el estado de los puertos.
- Presentar ante gerencia reportes en donde se involucren proyectos que se beneficien de la información referente a la capacidad física y el tráfico de la red.

- Establecer modelos en donde se pueda identificar las épocas del año en donde la operatividad de la red es crucial debido al tráfico fluyendo a través de la capa CORE.

- Generación de calendario en el cual las ventanas de mantenimiento o cambios en la red reduzcan su impacto a la operación de la entidad.

- Obtención adicional del porcentaje de utilización de memoria y cpu del equipo.

- Facilitar y mejorar tareas involucradas con la gestión de la red.

- Sentar las bases para el caso en que se desee ampliar el impacto de la implementación sobre la red y tomar la totalidad de esta, sumando routers de borde y switches de acceso de la red.

3. CAPÍTULO 3

3.1 INTRODUCCIÓN

Debido a la ineficiencia de realizar este proceso como se expuso anteriormente, se desarrollará la automatización de la implementación basándose en la metodología expuesta en el capítulo anterior, en este capítulo se mostrará y explicará el código utilizado para desarrollar la implementación, este código fue desarrollado utilizando el lenguaje de programación Python y la información recolectada a través de este fue modelada de igual forma como previamente se realizó en Power BI.

3.2 DESARROLLO DE LA AUTOMATIZACIÓN DE LA SOLUCIÓN

3.3 Desarrollo de herramienta para el procesamiento de texto

- Conexión e interacción con los dispositivos

Aunque existen herramientas de inteligencia artificial que podrían simplificar considerablemente el proceso, las políticas internas del banco y la naturaleza sensible de la información en cuestión impiden que dichos datos sean manejados íntegramente por agentes externos a la entidad sin la aprobación previa del departamento de seguridad de la información del banco. Este proceso de aprobación podría llevar un tiempo considerable. Por lo tanto, se optó por una alternativa que aborda específicamente la necesidad de obtener los datos mencionados anteriormente en el documento, evitando la complejidad asociada con la aprobación de la seguridad de la información.

Para su desarrollo, se utilizaron las características de la librería netmiko con las que se establece conexión a los equipos en cuestión siguiendo su formato de conexión descrito a continuación:

```
device = {
"host" : "1.1.1.1",
"Username" : User,
"password" : password,
"device_type" : "cisco_ios",
"global_delay_factor" : 0.1
}
```

Aquí se definió un objeto usado por la librería Netmiko que contiene los datos necesarios para realizar la conexión SSH a un equipo de red, en este caso CISCO, lo cual se define también en este objeto.

```
Command = "show int status"

net_connect = netmiko(**device)
show_outpur =
net_connect.send_command(command)
```

se evidencia las funciones propias de la librería usadas para realizar la conexión haciendo uso del objeto mencionado anteriormente y mostrando la sintaxis requerida para hacer la ejecución de un comando tipo show en un equipo Cisco.

- Procesamiento y extracción de información sobre formatos de texto

Para esta tarea también se hará uso del lenguaje de programación Python con otra de sus herramientas la cual para esta oportunidad será la librería ‘re’, esta librería permite la creación e identificación de expresiones regulares al interior de un documento de texto, lo cual si analizamos la problemática a tratar funciona perfectamente.

Para esta fase de la solución, se desglosará sección por sección del código implementado a continuación:

```
import pandas as pd
import re
import datetime
import pytz

# Create a regular expression to match Ethernet ports and
status
ethernet_port_regex = re.compile(r'Ethernet([\d/]+) is
(up|down|Administratively down|Link not connected)')

# Create a regular expression to match IP addresses
ip_regex = re.compile(r'(\d+\.\d+\.\d+\.\d+)')

# Create a regular expression to match input bit rates
input_bit_rate_regex = re.compile(r'(\d+) seconds input rate
(\d+) bits/sec')

# Create a regular expression to match output bit rates
```

```
output_bit_rate_regex = re.compile(r'(300|30)([\d/]+) seconds output rate (\d+) bits/sec')
```

Librerías

se pueden observar al inicio las librerías que fueron requeridas para la creación de la implementación de la automatización, las cuales fueron Pandas, re (Regular expression), datetime, pytz (Python timezone)

- Expresiones regulares

En la segunda parte, creamos expresiones regulares para identificar distintos tipos de información en el texto, como números, caracteres alfanuméricos o especiales, utilizando operadores para seguir un patrón. Por ejemplo, [/d] indica que después de cierto carácter viene un slash. También establecemos expresiones para extraer el puerto ethernet, la IP, input y output.

El formato constante asegura que la solución sea aplicable a todos los equipos en cualquier momento y sienta las bases para identificar otras características en futuras implementaciones. Estas expresiones buscan coincidencias en todo el texto.

```
# Create lists to store the extracted data
ethernet_ports = []
port_statuses = []
input_bit_rates = []
output_bit_rates = []
ip_addresses = []
```

Variables de almacenamiento y lectura del documento

En la primera parte de la imagen se establecen diferentes arreglos en los que se almacena la información extraída del resto del código que se ejecuta, luego de esto se leerá el documento de texto del cual se extrae la información y se entrega al resto del código como una variable la cual será procesado.

```
# Open the text file in read mode
def read_text_file(info):
    """Reads a text file and returns the contents as a
string."""
    with open("1.txt", "r") as f:
        text = f.read()

    return text

# Read the text file and assign the contents to the `text`
variable
text = read_text_file("eth.txt")

# Split the text into lines
lines = text.splitlines()

# Initialize variables to hold the current Ethernet port,
status, and IP address
current_ethernet_port = None
current_port_status = None
current_ip = None
```

División del texto y creación de variables de almacenamiento temporal.

Para este caso, posterior a ser leído el archivo de texto, este se divide en líneas para luego inicializar 3 variables las cuales serán necesarias para el momento en el que se relacionen bien sea la dirección ip, estado del puerto y el mismo puerto a diferentes líneas, con ayuda de estas variables más adelante se establecerá relación de la información entre diferentes líneas del texto que pertenecen al mismo puerto.

```
for line in lines:
    # Check if the line contains Ethernet port information
and status
    ethernet_port_match = ethernet_port_regex.search(line)
    if ethernet_port_match:
        current_ethernet_port = "Ethernet" +
ethernet_port_match.group(1)
        current_port_status = ethernet_port_match.group(2)

    # Check if the line contains IP address
    ip_address_match = ip_regex.search(line)
    if ip_address_match:
        current_ip = ip_address_match.group(1)


    # Check if the line contains output bit rate
    output_bit_rate_match =
output_bit_rate_regex.search(line)
    if output_bit_rate_match:

output_bit_rates.append(output_bit_rate_match.group(3))

    # Check if the line contains input bit rate
```

```
input_bit_rate_match = input_bit_rate_regex.search(line)
if input_bit_rate_match:
    input_bit_rates.append(input_bit_rate_match.group(2))
    ethernet_ports.append(current_ethernet_port)
    port_statuses.append(current_port_status)
    ip_addresses.append(current_ip)
```

La sección crítica del código se encuentra aquí anterior, donde se ejecuta un ciclo que recorre línea por la línea del texto dividido. Mediante condicionales, se buscan y almacenan las coincidencias de expresiones regulares en arreglos específicos, utilizando variables temporales para mantener la sincronización de la información del tráfico a lo largo de las diferentes líneas. Este proceso se repite para cada característica deseada, como puertos, estado, IP del dispositivo y tráfico promedio de entrada y salida en los últimos 5 minutos, concluyendo al alcanzar el número máximo de líneas en el documento.

```
# Ensure all lists have the same length
min_length = min(len(ip_addresses),
len(ethernet_ports), len(input_bit_rates),
len(output_bit_rates), len(port_statuses))
ip_addresses = ip_addresses[:min_length]
ethernet_ports = ethernet_ports[:min_length]
input_bit_rates = input_bit_rates[:min_length]
output_bit_rates = output_bit_rates[:min_length]
port_statuses = port_statuses[:min_length]
```

Se realiza una validación y corrección en el caso de que sea necesario del tamaño de los arreglos con el fin de que estos cumplan la característica de que todos tengan el mismo tamaño para poder ser almacenados como una base de datos relacional de columnas y filas lo cual es el fin final del tratamiento que se le dio a los datos al procesarlos, de lo contrario la información no iba a preservar la calidad y fidelidad de los datos.

```
# Create a DataFrame from the extracted data
df = pd.DataFrame({
    'IP Address': ip_addresses,
    'Ethernet Port': ethernet_ports,
    'Port Status': port_statuses,
    'Input Bit Rate': input_bit_rates,
    'Output Bit Rate': output_bit_rates
})
```

Se emplea la librería Pandas para transformar los datos extraídos en una tabla estructurada. Esta librería facilita la creación de columnas identificadas con cabeceras que representan la información correspondiente. Se agregan los datos de las cabeceras y se relacionan con los arreglos que proporcionan los valores para completar la tabla.

```
# Fill NaN values in the 'Output Bit Rate' column with empty
strings
df['Output Bit Rate'] = df['Output Bit Rate'].fillna('')

# Get the current date and time.
# Save the Colombia time zone to the variable
timezone_colombia.
timezone_colombia = pytz.timezone('America/Bogota')

# Get the current date and time.
now = datetime.datetime.now()

# Localize the current date and time to the Colombia time
zone.
now_colombia = now.astimezone(timezone_colombia)

# Format the date and time.
formatted_datetime = now_colombia.strftime("%Y-%m-%d|%H-%M")

# Add the current date to the DataFrame as a new column.
df['Date'] = formatted_datetime
```

Se hace uso de la librería Pytz, recientemente importada, para obtener la fecha y hora de la región específica de Bogotá. Se agrega esta información al formato adecuado para cumplir con los requisitos. La fecha y hora de la ejecución se incorporan a la base de datos existente (DataFrame utilizando Pandas) mediante la creación de una nueva columna que vincula cada fila con la marca temporal mencionada anteriormente.

```
import pretty table
```

Esta librería se utilizó con el fin de darle un manejo más cómodo a la información en el momento de realizar pruebas sobre la obtención de los datos y que de las pruebas se obtuvieran mejores resultados, la visualización de estos datos se puede ver de esta manera:

Puerto Ethernet	Estado de puerto	Input Bit Rate	Output Bit Rate	fecha
Ethernet3/1	up	52050568	384777896	2023-11-14|09-12
Ethernet3/2	up	47808848	95905032	2023-11-14|09-12
Ethernet3/3	up	756717592	514024488	2023-11-14|09-12
Ethernet3/4	up	560506584	676157136	2023-11-14|09-12
Ethernet3/5	down	56	56	2023-11-14|09-12
Ethernet3/6	down	56	56	2023-11-14|09-12
Ethernet3/7	down	56	56	2023-11-14|09-12
Ethernet3/8	down	56	56	2023-11-14|09-12
Ethernet3/9	down	56	56	2023-11-14|09-12
Ethernet3/10	down	56	56	2023-11-14|09-12
Ethernet3/11	down	56	56	2023-11-14|09-12
Ethernet3/12	down	0	56	2023-11-14|09-12
Ethernet4/1	up	43000	27912	2023-11-14|09-12

Tabla 2 Formato de tabla de la implementación

El formato presentado mediante el uso de la librería mencionada da mucha más claridad a la información como se puede ver en la tabla anterior, facilitando el uso

```
df.to_csv(f"NXinfo_{formatted_datetime}.csv",
index=false))
```

Para finalizar esta parte de la implementación, solo falta guardar la base de datos en un formato que permita a power bi darle un manejo más cómodo, en este caso el formato será .csv, lo cual permite que la aplicación de business inteligence obtenga los datos a modelar.

3.4 Modelación de tráfico sobre el tiempo

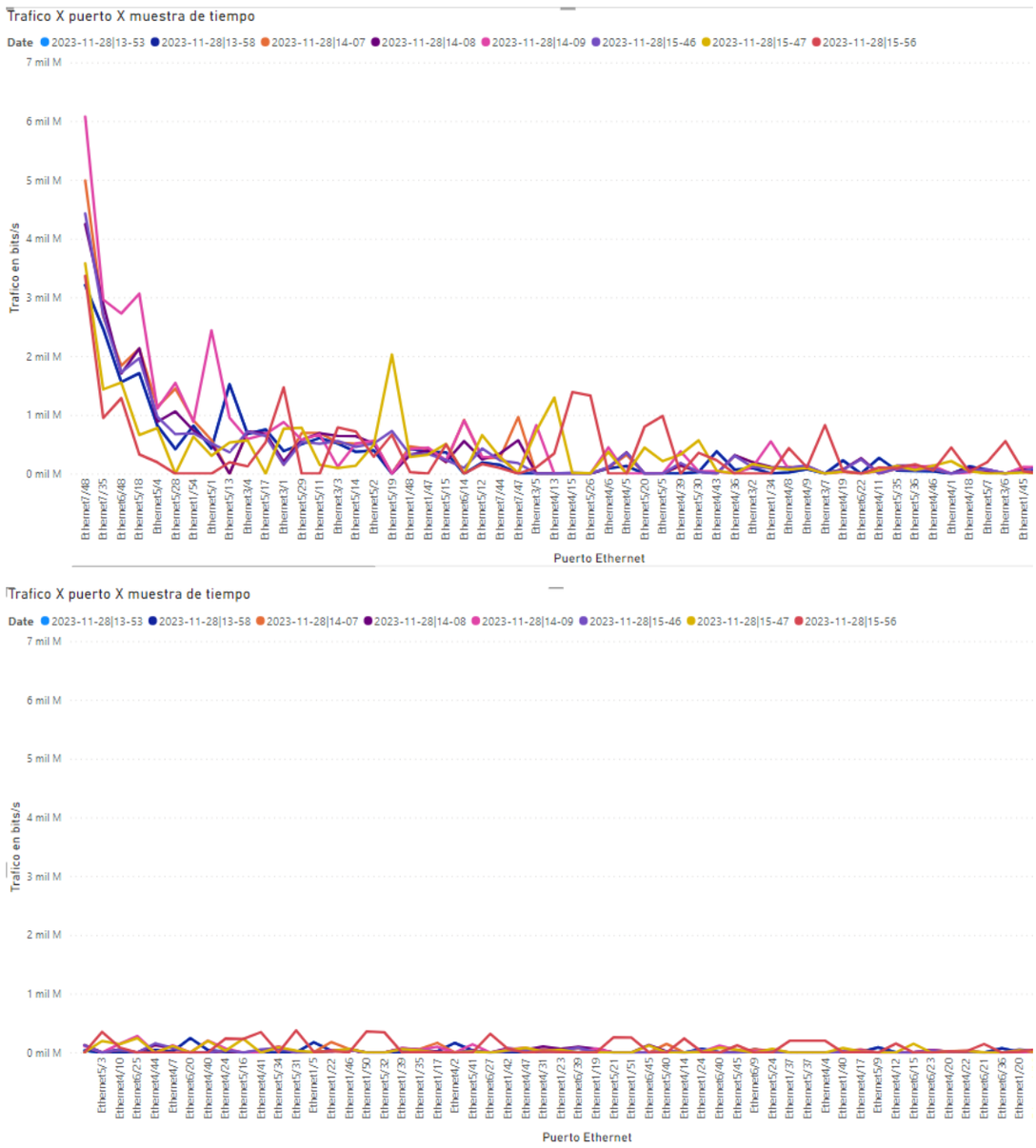


Figura 10 Trafico por puerto X tiempo

3.5 ANALISIS DE RESULTADOS FINALES

La gráfica proporciona una representación visual del valor del tráfico que fluye a través de los puertos Ethernet de la red CORE del Banco Av Villas. Este conjunto de datos es esencial para evaluar el rendimiento de la red lo cual se esperaba lograr con la implementación de esta solución para la entidad.

- Ventajas sobre la Gestión de Capacidad

Identificación de Patrones de Uso:

La gráfica permite identificar patrones de tráfico a lo largo del tiempo. Esto ayuda a comprender las tendencias de uso de la red, facilitando la planificación de la capacidad en función de la demanda real.

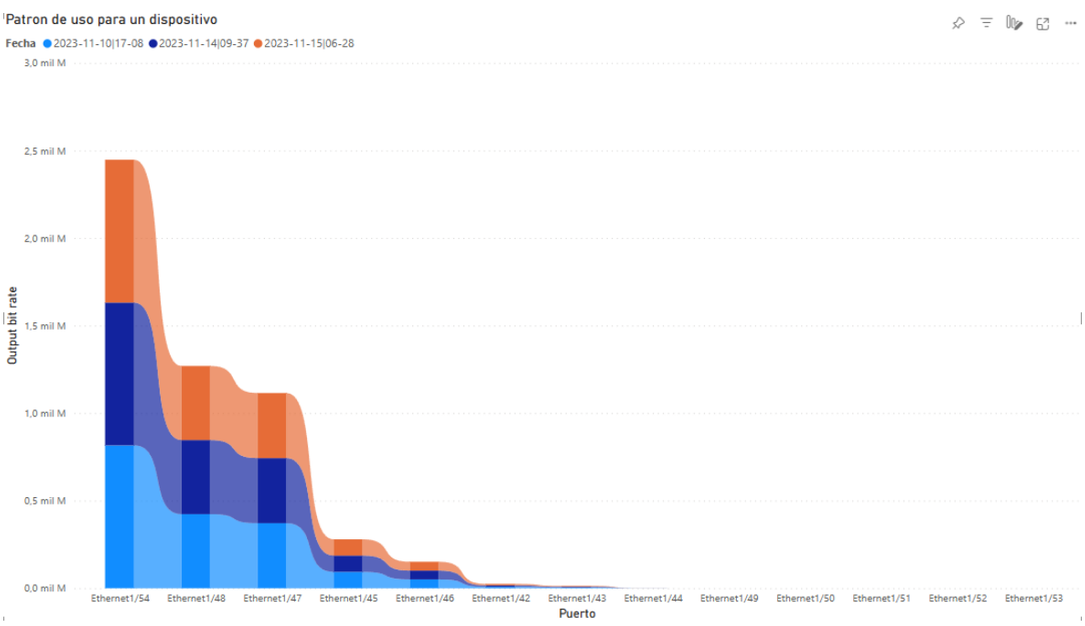


Figure 11 patrón de uso para un dispositivo

Para esta prueba la cual cuenta con 3 muestras diferentes que evidencian el banco en operación a las 9 de la mañana del martes 14 de noviembre como el valor de tráfico más alto otra a las 5 de la tarde momento en el que ya está cesando la operación para un día como ese y por ultimo y con la menor taza de tráfico, a las 6 de la mañana.

Optimización de Recursos:

Al analizar la carga de trabajo en los puertos Ethernet, la entidad bancaria puede asignar recursos de manera más eficiente. Esto evita la subutilización o el sobrecargue de ciertos segmentos y recursos de la red.

Predicción de Picos de Tráfico:

La visualización histórica del tráfico facilita la identificación de posibles picos de carga. Esta información es crucial para anticipar y gestionar eficientemente eventos de alta demanda, como promociones especiales o eventos bancarios.

Mejora de la Experiencia del Usuario:

Al entender los patrones de tráfico, la entidad bancaria puede optimizar la red para mejorar la experiencia del usuario. Esto se traduce en transacciones más rápidas y confiables, lo que contribuye a la satisfacción del cliente.

Ventajas para el Diagnóstico de Red:

Detección de Anomalías:

La gráfica permite identificar de manera rápida cualquier anomalía en el tráfico de la red. Cambios bruscos o patrones inusuales pueden indicar problemas potenciales que requieren atención inmediata.

Localización de Cuellos de Botella:

Al examinar los puertos Ethernet con mayor tráfico, se pueden identificar posibles cuellos de botella. Esta información es esencial para realizar mejoras locales y aumentar la eficiencia de la red.

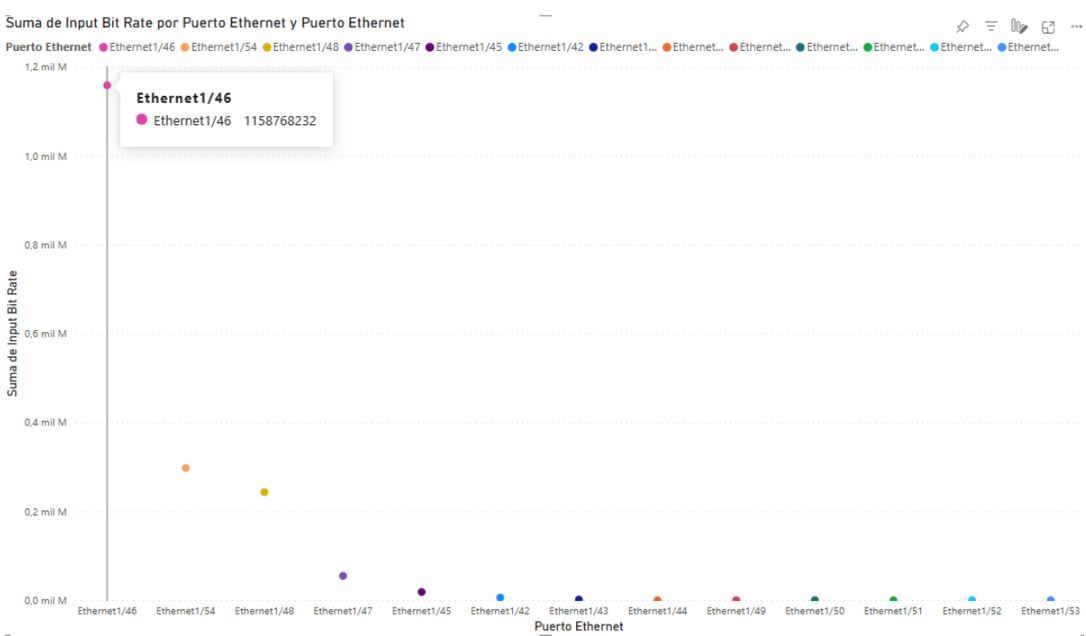


Figure 12 Puerto con tráfico superior a 1 Gbit

Para dar una demostración se creo el anterior escenario en el que se podría evidenciar como un puerto tiene un tráfico considerablemente mayor a los demás, en este caso identificando el puerto y el equipo y otros datos se puede dar lugar a los siguientes ítems presentados.

Respuesta Rápida a Incidentes:

La capacidad de monitorear el tráfico en tiempo real permite una respuesta más rápida a posibles incidentes. Esto minimiza el tiempo de inactividad y reduce el impacto en las operaciones diarias.

Planificación de Mantenimiento:

La información histórica de la gráfica puede utilizarse para planificar el mantenimiento preventivo. Identificar patrones de tráfico bajos puede indicar momentos óptimos para realizar actualizaciones o cambios en la red sin afectar significativamente las operaciones.

3.6 CONCLUSIONES Y RECOMENDACIONES

- La implementación de sistemas de monitoreo de red, independientemente del tamaño de la compañía, actúa como garantía contra errores en la implementación de proyectos y en la gestión operativa. Estas herramientas ofrecen una visión integral que contribuye a la toma de decisiones informadas y a la prevención de posibles contratiempos.

- La gestión de capacidad de una red debería ocupar un lugar central y recibir una atención sustancialmente mayor. Su importancia radica en las repercusiones potenciales, que van más allá de lo económico, abarcando aspectos operativos y normativos. La falta de información actualizada sobre la red puede tener un impacto significativo en la eficiencia global de la entidad.

- La automatización de procesos en la administración de recursos de red para el caso del Banco Av Villas, ha sido subestimada por la alta dirección. Esta falta de énfasis ha afectado negativamente la capacidad de la red y ha contribuido a la gestión reactiva de solicitudes e incidentes. La automatización se revela como un componente esencial para optimizar la eficiencia operativa y garantizar la capacidad adecuada de la red.

- La asignación de personal altamente capacitado y dedicado en el área de telecomunicaciones es imperativa. Estos profesionales deben destinar tiempo significativo a la automatización de operaciones y a la implementación continua de mejoras. La inversión en recursos humanos en este sentido generará un entorno más efectivo, liberando tiempo para la innovación y la resolución proactiva de desafíos en lugar de reaccionar ante ellos.

- La creación de diferentes ambientes de pruebas en los que el personal del área de telecomunicaciones de la entidad pueda implementar previo a la aplicación sobre los entornos de producción, es algo fundamental para garantizar una mayor eficiencia del equipo, así como evaluar el riesgo y la viabilidad de los proyectos.

- La implementación de la herramienta automatizada basada en Netmiko y Python ha demostrado su eficacia al agilizar la obtención de datos críticos sobre la red del Banco Av Villas. Esta automatización no solo optimiza la eficiencia operativa, sino que también minimiza el tiempo necesario para realizar análisis detallados.

- La modelación gráfica de datos utilizando Power BI proporciona una visualización clara y accesible del tráfico de la red a lo largo del tiempo. Esta capacidad de análisis visual agrega un valor estratégico significativo, permitiendo a los responsables de la toma de decisiones identificar patrones, anticipar necesidades y responder proactivamente a cambios en la carga de la red.

REFERENCIAS

- Cisco Community. (2023). 01 - Netmiko: la herramienta de automatización para dispositivos de red. Recuperado de https://community.cisco.com/t5/blogs-general/01-netmiko-la-herramienta-de-automatizaci%C3%B3n-para-dispositivos-de/ba-p/4954431

- Pyneng Documentation. (2023). Netmiko - Automatización de dispositivos de red con Python. Recuperado de https://pyneng.readthedocs.io/en/latest/book/18_ssh_telnet/netmiko.html