Escuela Superior Politécnica del Litoral

Facultad de Ingeniería en Electricidad y Computación

Diseño y Simulación de un Sistema de Red LAN mediante segmentación por VLANs para el despliegue del Control De Acceso y CCTV

Proyecto Integrador

Previo la obtención del Título de:

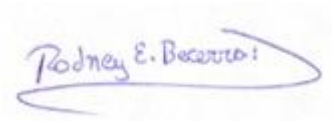
Ingeniero en Telecomunicaciones

Presentado por:
Rodney Ernesto Becerra Delgado
Diego Joel Roque Ramirez

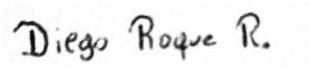
Guayaquil - Ecuador
Año: 2023

Declaración expresa

“Los derechos de titularidad y explotación, nos corresponde conforme al reglamento de propiedad intelectual de la institución; *Rodney Ernesto Becerra Delgado y Diego Joel Roque Ramirez* damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual".



Rodney Ernesto
Becerra Delgado



Diego Joel
Roque Ramirez

Evaluadores

Firmado electrónicamente por:
VERONICA ALEXANDRA SOTO VERA

Verónica Soto, Ms.C.

Profesor de la materia

Firmado electrónicamente por:
PATRICIA XIMENA CHAVEZ BURBANO

Patricia Chávez, Ph.D.

Profesor tutor

RESUMEN

La empresa privada con sede en Guayaquil, especializada en el ámbito comercial, anticipa un crecimiento continuo en los próximos cinco años. Desde su inicio en 2020, se ha centrado en ofrecer servicios tecnológicos, asistencia a usuarios, instalación de cableado estructurado, capacitación y asesoramiento. Consciente de los avances tecnológicos y los impulsores del crecimiento, la organización busca mantenerse actualizada para proporcionar servicios alineados con los productos líderes.

El proyecto se concentra en mejorar la infraestructura de red para satisfacer la creciente demanda de conectividad, seguridad y eficiencia en la gestión de datos, especialmente debido al aumento de dispositivos y colaboradores conectados. El objetivo principal es diseñar y simular un sistema de videovigilancia con CCTV en una red LAN escalable.

La ejecución del proyecto involucra la implementación de una topología de red en estrella con seguridad perimetral y distribución central desde el conmutador núcleo. Se instalan grabadores NVR y Access Points en varias áreas para lograr redundancia a través de dos ISP y la implementación de segmentación de VLANs.

Los resultados obtenidos reflejan el éxito de la ejecución, respaldado por pruebas virtuales y físicas que validan la solución propuesta. Se verifica la coherencia de las políticas de red y el diseño se ajusta a las necesidades del cliente, asegurando la seguridad sin afectar el uso diario.

En resumen, la segmentación VLAN mejora la seguridad al limitar el acceso no autorizado, y la implementación de LACP optimiza la red. La adición de la compresión de video H.265+ aumenta la eficiencia en el almacenamiento y el uso del ancho de banda.

Palabras clave: Infraestructura de Red, Seguridad, CCTV, Segmentación VLAN.

ABSTRACT

The private company, located in Guayaquil, specializing in the commercial sector, anticipates continuous growth in the next five years. Since its inception in 2020, it has focused on providing technological services, user support, structured cabling installation, training, and consultancy. Aware of technological advancements and growth drivers, the organization aims to stay updated to deliver services aligned with leading products.

The project focuses on enhancing the network infrastructure to meet the increasing demands for connectivity, security, and data management efficiency, especially due to the rising number of connected devices and collaborators. The primary goal is to design and simulate a scalable LAN-based CCTV surveillance system.

The project's execution involves implementing a star network topology with perimeter security and central distribution from the switch core. NVR recorders and Access Points are installed in various areas to achieve redundancy through two ISPs, along with VLAN segmentation implementation.

The obtained results reflect the successful execution, supported by virtual and physical tests that validate the proposed solution. Network policy consistency is verified, and the design is tailored to the client's needs, ensuring security without disrupting daily operations.

In summary, VLAN segmentation enhances security by limiting unauthorized access, and the implementation of LACP optimizes the network. The addition of H.265+ video compression increases storage efficiency and bandwidth utilization.

Keywords: Network Infrastructure, Security, CCTV, VLAN Segmentation.

Índice General

ABREVIATURAS

ESPOL Escuela Superior Politécnica del Litoral

CCTV Circuito Cerrado de Televisión

LAN Local área network/red de área local

VLAN Virtual local area network/Red de área local virtual

NVR Network video recorder/Grabador de video de red

LACP Link Aggregation Control Protocol/Protocolo de Control de adición de enlace

SIMBOLOGÍA

Gbps Gigabit por segundo

Mbps Megabit por segundo

mm Milímetro

Fps Tramas por segundo

MP Mega Pixeles

Mbits Megabit

ms milisegundo

TB Terabyte

MB Megabyte

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

1.1 Introducción

La empresa comercial ubicada en Guayaquil, con su inicio en 2020 con un aproximado de 25 empleados, se ha centrado en servicios tecnológicos, asistencia a usuarios, instalación de cableado estructurado (tanto cobre como fibra), capacitación y asesoramiento. Sin embargo, la pandemia de COVID-19 generó una transición forzada de operaciones presenciales a virtuales, lo que resultó en un aumento significativo de su cuota de mercado. En 2023, está experimentando una transformación de pequeña a mediana empresa, con un aumento del 48% en su fuerza laboral en solo tres años.

La importancia de esta empresa radica en la necesidad de mantenerse al día con los avances tecnológicos para ofrecer servicios y asesoramiento competitivos. Esto implica la mejora y optimización de su infraestructura de red para satisfacer las crecientes demandas de conectividad, seguridad y eficiencia en la gestión de datos.

Además, se plantea el desafío de implementar una segmentación de red mediante VLANs (Redes Locales Virtuales) para optimizar el ancho de banda y evitar congestiones a medida que aumenta el número de dispositivos y usuarios conectados.

En cuanto a la seguridad, se busca implementar un sistema de videovigilancia (CCTV) dentro de la infraestructura de red para monitorear y salvaguardar activos e información sensible de la empresa.

En el horizonte de los próximos cinco años, la empresa proyecta un crecimiento continuo, lo que hace indispensable una infraestructura de red escalable que pueda manejar un mayor personal y usuarios. Mantenerse al día con las tecnologías y estándares actuales es esencial para garantizar una conectividad ininterrumpida, especialmente al trabajar con aplicaciones en la nube y una conectividad de alta calidad.

En resumen, la empresa enfrenta una fase de crecimiento y evolución rápidos. Para mantenerse competitiva y satisfacer las demandas cambiantes del mercado, necesita optimizar su infraestructura de red, implementar medidas de seguridad y estar preparada para un crecimiento continuo. La inversión en una infraestructura de red escalable, segmentada por VLANs y con CCTV, es fundamental para su éxito futuro.

1.2 Descripción del problema

El cliente es una empresa privada enfocada en el sector comercial de Guayaquil, que está en constate crecimiento, y necesita una infraestructura de red capaz de crecer en los próximos cinco años, y por lo que requiere un diseño capaz de cumplir con las características óptimas para operar bajo esta premisa. Para conseguir este objetivo, se va a segmentar la red mediante VLAN, optimizando los siguientes parámetros: ancho de banda, tráfico de red considerando sus necesidades específicas como las medidas de seguridad con equipos robustos como un firewall y servicios a utilizar como el control de acceso y CCTV.

1.3 Justificación del problema

La necesidad de adquirir una infraestructura de red para una empresa privada en Guayaquil se debe a un problema motivado por diversos factores clave. Estos factores justifican la importancia de esta inversión, ya que permitirá a la empresa mejorar su posición en el sector tecnológico y facilitar su expansión en los próximos cinco años como se explican a continuación:

Desde el año 2020, la empresa inició sus operaciones con una plantilla de 25 empleados. Sin embargo, debido a los cambios impuestos por la pandemia de COVID-19, que obligaron a un cambio de presencialidad a virtualidad en el trabajo, se ha experimentado un aumento considerable en la demanda de servicios. Este aumento en la demanda ha llevado a un incremento en el número de dispositivos y empleados que requieren conectividad a la red de la empresa.

Hasta el año 2023, la empresa no ha establecido una infraestructura de red propia, y en su lugar, ha estado utilizando el enrutador proporcionado por su ISP. Sin embargo, conforme planifican la implementación de una nueva sede o matriz, reconocen la importancia de desarrollar una infraestructura de red sólida que respalde sus operaciones en crecimiento.

Esta infraestructura de red está intrínsecamente relacionada con la seguridad de los datos que manejan. Para abordar esta preocupación y garantizar la integridad de los datos empresariales, se ha propuesto la solución de implementar la segmentación por VLAN. Además, se considera fundamental establecer un sistema de circuito cerrado de televisión (CCTV) que contribuya a la seguridad de los activos de la empresa y al control

de acceso de los empleados en la futura sede o matriz. Estas medidas se han tomado en cuenta como parte de la planificación de su expansión.

1.4 Objetivos

En el contexto de este proyecto, se han definido cinco objetivos específicos que desempeñarán un papel fundamental en la consecución del objetivo general.

1.4.1 Objetivo general

Diseñar y simular un sistema CCTV de cámaras de seguridad con control y monitoreo remoto en una red LAN escalable que cumpla con los requisitos de calidad de servicio y seguridad de las aplicaciones de la empresa, y desarrollar un análisis técnico de los dispositivos de red.

1.4.2 Objetivos específicos

1. Investigar el funcionamiento y la estructura de los activos de la empresa con el propósito de analizar la comunicación interna entre los departamentos. Además de evaluar la jerarquía del tráfico en la red mediante la elaboración de un organigrama.

2. Diseñar y simular una estructura de red LAN que permita adaptarse a los próximos cinco años en su crecimiento, considerando el número de cámaras y dispositivos de monitoreo remoto.

3. Analizar las políticas autenticación para el control de acceso a las cámaras y los sistemas de monitoreo remoto, asegurando el cifrado y VPN para la transmisión de video y proteger los datos importantes.

4. Aplicar las configuraciones de calidad de servicio, garantizando un ancho de banda optimo y generando una correcta priorización del tráfico de video junto con las otras aplicaciones de la empresa de manera jerárquica.

5. Desarrollar un análisis técnico comparando diferentes opciones de dispositivos de red en términos de rendimiento, escalabilidad y costos, para tomar decisiones informadas y optimizar la inversión.

1.5 Marco teórico

En el cantón Rumiñahui se ha llevado a cabo un proyecto destinado a mejorar la seguridad en la urbanización "Eloy Alfaro". Este proyecto implica el diseño e implementación de un sistema de circuito cerrado de televisión (CCTV) basado en tecnología IP y almacenamiento en la nube. Para garantizar una cobertura adecuada, se realizaron análisis geográficos que permitieron la ubicación estratégica de las cámaras IP, abarcando aproximadamente diez lotes por cámara. Además, se aplicó el modelo de calidad de servicio DiffServ con el objetivo de priorizar el tráfico y mejorar la velocidad de transmisión de datos. Los archivos de las cámaras IP se almacenan en un servidor en la nube con acceso a través de una dirección IP pública. Se llevaron a cabo pruebas de conectividad que arrojaron resultados positivos, y los indicadores financieros respaldan los beneficios económicos indirectos del proyecto. En resumen, este sistema de CCTV IP contribuirá a aumentar la seguridad y el bienestar de los residentes de la urbanización. (Daniel Chávez ,2022)

En otro proyecto relacionado con la seguridad, se ha implementado un sistema integral en el Aeropuerto Internacional Mariscal Sucre. Este sistema abarca aspectos como la infraestructura de red, la protección contra incendios, los botones de pánico, los intercomunicadores, el control de acceso y el sistema de videovigilancia CCTV. Se destaca la importancia de mantener actualizado el sistema Genetec, que se caracteriza por su modularidad y capacidad de integración con otros sistemas de seguridad. Este sistema proporciona una interfaz eficiente y de fácil uso para el monitoreo de las operaciones de seguridad del aeropuerto. Se enfatiza la necesidad de mantener el sistema actualizado y realizar un monitoreo constante, aprovechando las ventajas de la tecnología IP en la videovigilancia. (Juan Pavón, 2016)

En un tercer proyecto llevado a cabo en la Ciudad de México, se instaló un sistema de videovigilancia integrada utilizando el software libre ZoneMinder, funcionando en el sistema operativo UBUNTU. Durante las horas no laborables, las cámaras están configuradas para detectar movimientos y enviar alarmas por correo electrónico. Además, las cámaras fijas cuentan con visión nocturna para una mayor seguridad. La ventaja principal de ZoneMinder es su capacidad para trabajar con cámaras de diferentes fabricantes, lo que ahorra costos y permite la escalabilidad al agregar más cámaras en el futuro. (Rivas y Velazquez,2011)

En conclusión, estos proyectos de videovigilancia demuestran diversas estrategias para mejorar la seguridad utilizando tecnología IP y software especializado. Mientras que ZoneMinder es una opción económica y versátil, Genetec ofrece un enfoque más avanzado y profesional. Sin embargo, todos estos proyectos han enfrentado desafíos relacionados con el ancho de banda, lo que destaca la importancia de una conexión LAN para optimizar el rendimiento en proyectos de esta naturaleza.

CAPÍTULO 2

2.1 Metodología

En el presente capitulo tiene como objetivo investigar la metodología para la segmentación de VLANs en sistemas de CCTV. La segmentación de VLANs implica dividir una red en subredes lógicas más pequeñas, lo que mejora la seguridad y el rendimiento de la transmisión de datos. Se espera que este estudio contribuya a mejorar la seguridad y eficiencia de los sistemas de vigilancia para la empresa ubicada en la ciudad de Guayaquil. Además de enriquecer el conocimiento en el campo de las redes de seguridad.

2.2 Descripción del escenario

Para la sección de este capítulo se presenta las instalaciones físicas, y su ubicación de cada dispositivo empleado, su distribución de personal acorde a los departamentos asignados a su servicio y aplicaciones de red a emplear.

2.2.1 Instalaciones físicas

Para el diseño de CCTV se consideraron las entradas exteriores, parqueadero, oficinas, pasillos internos y externos de la empresa, para la ubicación de las cámaras exteriores, se deben clasificar según los requerimientos del cliente y la puerta de acceso biométrico obteniendo el acceso del personal al Rack de la empresa.

2.2.2 Departamentos, usuarios y distribución

En la empresa se tiene un personal total de 58 usuarios en toda la planta:

- Dos usuarios generales, un usuario como director general de toda la empresa, un usuario de gerencia general de todos los departamentos.
- Cinco usuarios encargados del departamento asignado a su despacho y 51 usuarios distribuidos por áreas asignadas.

En base a la distribución de usuarios en la planta baja se tiene:

- El departamento de administración y finanzas conformados por un personal de 17 usuarios, un usuario encargado de gerencia de departamento, ocho usuarios en el área de facturación y cobranza, y ocho usuarios en el área de contabilidad y personal.

- El departamento de gerente técnico y estudio conformados por 15 usuarios, un usuario encargado de la Gerencia de departamento de técnico y 14 usuarios en el área de técnicos.
- El departamento de marketing conformados por ocho usuarios, un usuario encargado de la Gerencia del departamento de Marketing, tres usuarios en el área de publicidad y cuatro usuarios en el área de diseño gráfico.

De igual manera, en el primer piso se tiene:

- El departamento de recursos humanos conformado por siete usuarios, un usuario en la administración de recursos humanos, dos usuarios en el área de prevención de riesgo, dos usuarios en el área de asistencia social y dos usuarios en el área de psicólogo.
- El departamento de Producción conformado por nueve usuarios, un usuario encargado de la Gerencia de producción, un usuario encargado del área de Packing como jefe teniendo dos usuarios a su cargo, un usuario encargado del área de bodega como jefe, teniendo dos usuarios a su administración, un usuario encargado del área de portería, teniendo un usuario a su cargo.

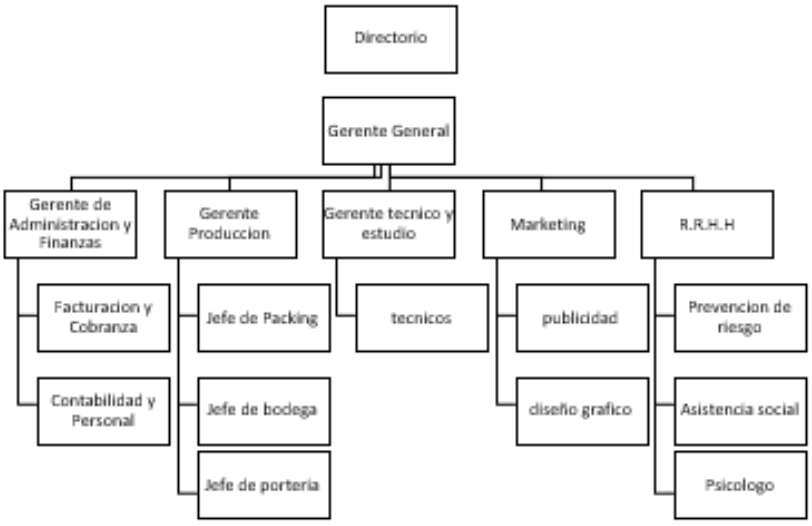


Ilustración 1. Organigrama de la empresa con sus departamentos.

Por último, en la ilustración 1 se puede observar el organigrama de la empresa, en cual se puede tener una noción de cómo es la jerarquía presente en la empresa y con esto tener un control para la creación de las VLANs.

2.2.3 Servicios de red y aplicaciones requeridas

El correo electrónico desempeña un papel fundamental en la comunicación tanto interna como externa de la empresa. La gestión de correos electrónicos personales y comerciales se realiza a través de servicios como Gmail y Outlook.

En lo que respecta a la colaboración en proyectos, Trello se utiliza para llevar un seguimiento de las tareas e hitos en las actividades de consultoría y asesoramiento.

Las reuniones y conferencias virtuales se llevan a cabo principalmente a través de Microsoft Teams, una aplicación que se implementó durante la pandemia de COVID-19 para facilitar las reuniones de equipo y las conferencias con clientes de forma remota.

En cuanto a la facturación electrónica, la empresa ha adoptado aplicaciones proporcionadas por el Servicio de Rentas Internas (SRI) para agilizar este proceso.

Para el almacenamiento y la compartición de documentos críticos, Microsoft OneDrive se utiliza como una solución de nube. Esto permite a los empleados almacenar documentos en línea y acceder a ellos desde cualquier lugar de manera conveniente.

2.3 Diseño de la arquitectura de la red

Para el diseño de la arquitectura de red se determinó cómo se interconectarán los equipos y así, analizar el desempeño y decidir el uso de que cumplan con las características deseadas.

2.3.1 Topología lógica y topología física

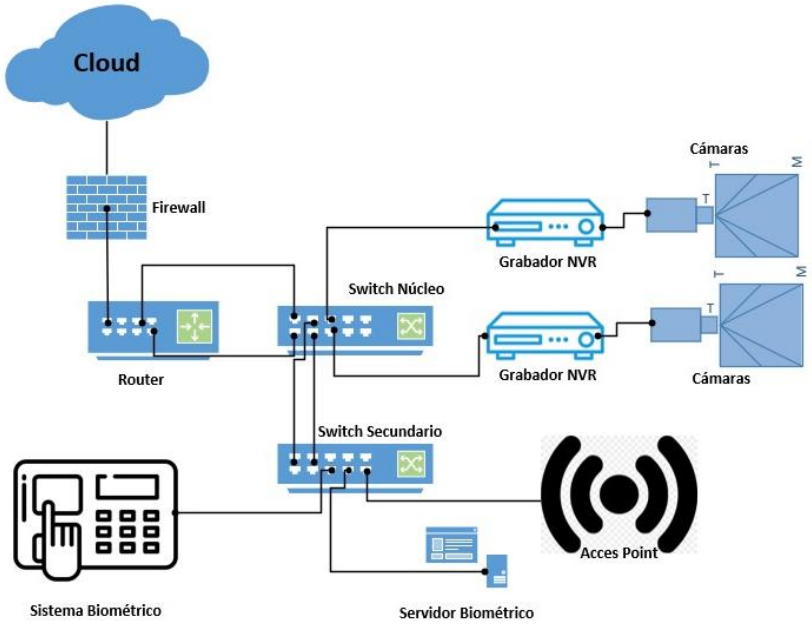


Ilustración 2. Topología de red lógica y física de la solución propuesta.

La topología lógica que se muestra en la ilustración 2 se empleó una topología tipo estrella con el conmutador núcleo en el centro, el firewall y del enrutador, genera una seguridad perimetral y distribución principal a la red del conmutador núcleo. Además, se distribuye la red en dos grabadores NVR conectados directamente a las cámaras sectorizando tanto para exterior e interior en planta baja, y el primer piso de manera interior.

Para el conmutador secundario conectado directamente del conmutador núcleo se tiene la distribución de los puntos de acceso ubicados en la planta baja interior y primer piso interior. Adicionalmente, este conmutador secundario se conecta a un servidor biométrico para almacenar la base de datos de ingreso del personal autorizado, tanto para planta baja como para el primer piso de manera interior.

2.3.2 Integración del sistema de seguridad biométrica

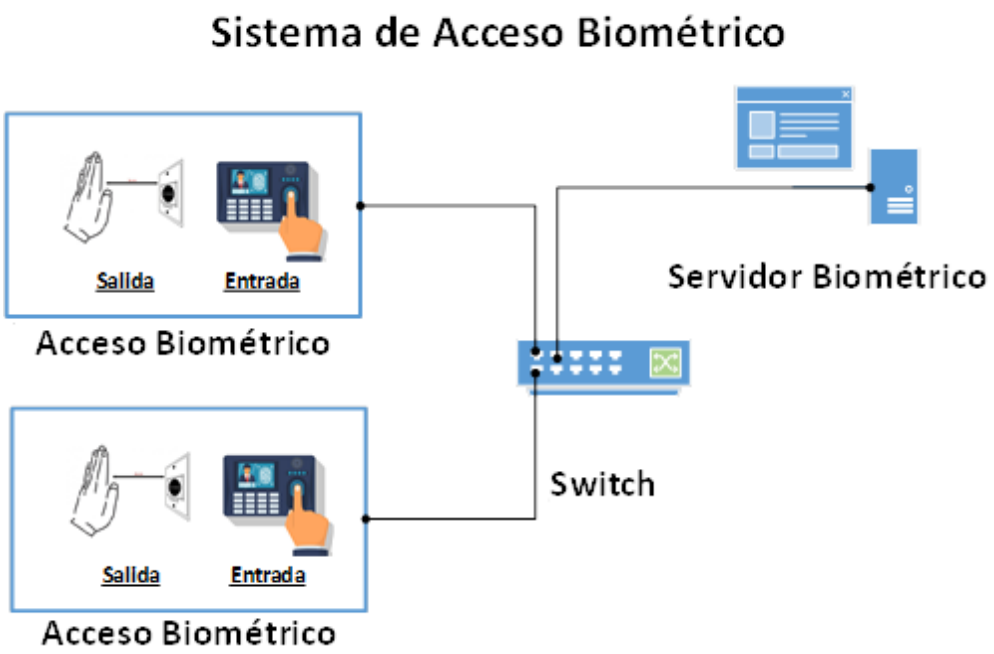


Ilustración 3. Sistema de seguridad de acceso biométrico para la solución propuesta.

En la ilustración 3 se muestra cómo se integrará el sistema biométrico. Cuenta con un servidor biométrico conectado al conmutador secundario que genera una base de datos encargara el acceso a exclusivamente el personal de la empresa.

2.4 Dispositivos de red de solución propuesta

Para esta sección se tiene los diferentes dispositivos propuestos para generar una óptima administración de la red conformada por firewall/enrutador, conmutador, punto de acceso, NVR, y cámaras.

2.4.1 Firewall

Para la selección del firewall se han comparado el equipo de Fortinet 40F y el Palo Alto Networks PA-220. Ambos firewalls son dispositivos de nivel de entrada para pequeñas y medianas empresas y comparten algunas características comunes. Tales como seguridad de red de alto rendimiento, protección contra amenazas avanzadas y capacidades de gestión centralizada, A continuación, se presenta en la tabla 1 la comparativa técnica entre ambos en términos de ancho de banda y tráfico de red:

Tabla 1. Comparativa entre firewall para la red de la solución propuesta.

Características	**Fortinet 40F (Fortinet)**	**PA-220 (Palo Alto Networks)**
Ancho de banda de firewall:	Hasta 20 Gbps	Hasta 1.5 Gbps
Ancho de banda de inspección SSL/TLS:	Hasta 5 Gbps	Hasta 250 Mbps
Rendimiento de IPS:	Hasta 5 Gbps	Hasta 500 Mbps
Conexiones concurrentes:	Hasta 2 millones	Hasta 64,000
Sesiones nuevas por segundo:	Hasta 42,000	Hasta 1,500

En lo que respecta al rendimiento de ancho de banda, el firewall Fortinet 40F presenta una clara ventaja con un impresionante ancho de banda de firewall que alcanza los 20 Gbps, en comparación con los 1.5 Gbps ofrecidos por el Palo Alto Networks PA-220. Además, el Fortinet 40F supera al Palo Alto en términos de capacidad de inspección SSL/TLS y rendimiento de IPS. También, al analizar su relación calidad-precio, se ha determinado que el firewall Fortinet 40F es la opción preferida.

2.4.2 Conmutador

Para la selección del conmutador se han comparado los conmutadores Aruba INSTANT ON 1930-48G-PoE y el Cisco Catalyst 2960-L en términos técnicos como se muestra en la tabla 2:

Tabla 2. Comparativa entre conmutadores para la red de la solución propuesta.

Características	**INSTANT ON 1930-48G-PoE (Aruba)**	**Catalyst 2960-L (Cisco)**
Ancho de banda:	Hasta 104 Gbps.	Hasta 108 Gbps.
Puertos:	48 puertos Gigabit Ethernet.	Ofrece puertos Gigabit Ethernet y puertos Fast Ethernet.
PoE:	Si lo admite	Si lo admite.
Características de tráfico de red:	Proporciona funcionalidades de calidad de servicio (QoS).	Proporciona capacidades de calidad de servicio (QoS).
Gestión y seguridad:	Permite una administración sencilla y segura, con opciones de configuración y monitorización a través de interfaces gráficas intuitivas.	Ofrece opciones de administración y seguridad avanzadas, incluyendo configuración basada en roles, autenticación de dispositivos y funciones de seguridad adicionales.

En lo que respecta al ancho de banda y al tráfico de red, se observa que ambos conmutadores tienen capacidades similares, aunque el Cisco Catalyst 2960-L ofrece un ligero aumento en el ancho de banda total. No obstante, es fundamental destacar que el conmutador Aruba INSTANT ON 1930-48G-PoE garantiza un rendimiento óptimo y una respuesta sin retrasos, lo cual es de vital importancia, especialmente en la gestión de un sistema de CCTV. Considerando estos aspectos, se ha optado por la selección del conmutador Aruba INSTANT ON 1930-48G-PoE.

2.4.3 NVR

Se ha realizado un análisis técnico y comparativo de los beneficios en ahorro de tráfico de red y ancho de banda entre el Hikvision DS-7732NI-I4/24P NVR y el Dahua NVR5232-16P-4KS2, como se muestra en la tabla 3 para la grabación de las cámaras de videovigilancia:

Tabla 3. Comparativa entre NVR para la red de la solución propuesta.

Características	**DS-7732NI-I4/24P NVR (Hikvision)**	**NVR5232-16P-4KS2 (Dahua)**
Ahorro de tráfico de red:	El Hikvision DS-7732NI-I4/24P NVR ofrece 24 puertos PoE integrados, lo que permite la conexión directa de cámaras IP y la alimentación a través de un solo cable Ethernet. Esto reduce la necesidad de utilizar dispositivos de alimentación adicionales y minimiza el tráfico de red generado por múltiples cables de alimentación.	Al igual que el Hikvision NVR, el Dahua NVR5232-16P-4KS2 también cuenta con puertos PoE integrados, en este caso, 16 puertos. Esto permite la conexión y alimentación directa de cámaras IP a través de un único cable Ethernet, lo que reduce la cantidad de cables necesarios y, por lo tanto, el tráfico de red generado.
Ancho de banda:	El NVR de Hikvision admite hasta 32 canales de cámaras IP, lo que implica un mayor potencial de ancho de banda requerido para la transmisión y grabación de video. Sin embargo, el ancho de banda real utilizado dependerá de la resolución y las configuraciones de compresión de las cámaras IP utilizadas en el sistema.	El NVR de Dahua admite hasta 32 canales de cámaras IP, al igual que el Hikvision NVR. El consumo de ancho de banda dependerá de la resolución de las cámaras IP y la configuración de compresión utilizada.

Se ha tenido en cuenta tanto el Hikvision DS-7732NI-I4/24P NVR como la otra opción de NVR debido a sus ventajas en términos de ahorro de tráfico de red y ancho de banda. Ambos NVR ofrecen beneficios similares al incorporar puertos PoE que permiten la conexión y alimentación de cámaras IP mediante un solo cable Ethernet. Esto contribuye a reducir la carga de tráfico en la red al minimizar la necesidad de utilizar múltiples cables de alimentación y simplificar la infraestructura. Sin embargo, la elección final se ha inclinado hacia el Hikvision DS-7732NI-I4/24P NVR debido a su compatibilidad con las cámaras específicas que el cliente planea utilizar en la implementación del sistema de videovigilancia.

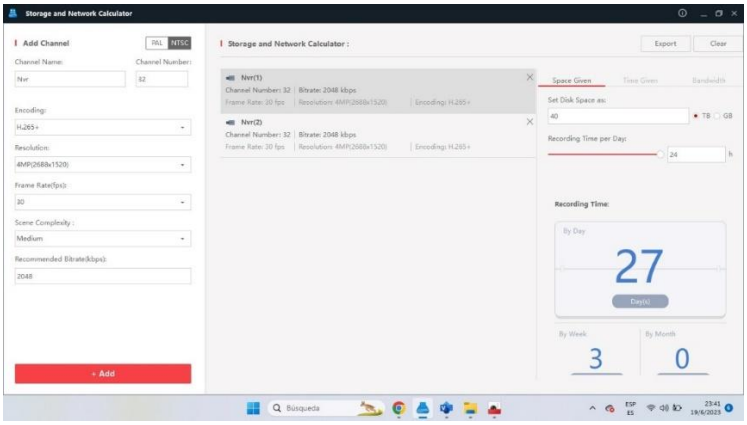


Ilustración 4. Capacidad y número de NVR para almacenamiento de grabaciones.

Se ha determinado el número necesario de NVR, como se observa en la ilustracion 4 utilizando la herramienta "Storage and Network Calculator" para este tipo de empresa, lo que ha llevado a la conclusión de que se requerirán 2 NVR. Asimismo, para mantener un registro continuo de 27 días, se identifica la necesidad de contar con un sistema de almacenamiento de 40 TB. Esto se basa en varios parámetros, como el Frame Rate, la codificación y el número de canales. En el caso específico del NVR Hikvision DS-7732NI-I4/24P, se dispone de 32 canales para la grabación.

2.4.4 Puntos de acceso

Para garantizar el crecimiento sostenido de la empresa en los años venideros, es esencial contar con puntos de acceso que brinden conectividad Wi-Fi 6 confiable. Los puntos de acceso considerados son dispositivos de nivel de entrada diseñados específicamente para pequeñas y medianas empresas. Los dispositivos Aruba AP-22 y Cisco Catalyst 9117AX están equipados con tecnología de vanguardia que les permite

adaptarse a las futuras innovaciones tecnológicas. A continuación, se presenta una comparación detallada entre los dispositivos en la tabla 4:

Tabla 4. Comparativa entre puntos de acceso para la red de la solución propuesta.

Características	**ARUBA AP-22 (Aruba)**	**Cisco Catalyst 9117AX Access Point (Cisco)**
Conectividad Wi-Fi 6:	Compatible Wi-Fi 6 (802.11ax).	Compatible con Wi-Fi 6 (802.11ax).
Velocidades de transmisión de datos:	Hasta 1.775 Gbps.	Hasta 5.4 Gbps.
Capacidad de clientes simultáneos:	Diseñado para soportar gran cantidad de clientes simultáneos.	Diseñado para manejar clientes simultáneos.
Arquitectura de acceso unificada:	Permite una gestión centralizada y simplificada de la red inalámbrica.	Proporciona funciones de seguridad inalámbrica avanzadas, como encriptación WPA3, autenticación de clientes y detección de amenazas.
Tecnología de antena adaptable:	Utiliza tecnología de antena adaptable para optimizar la cobertura y el rendimiento inalámbrico.	Compatible con características y protocolos de red estándar, como PoE, VLAN y QoS.

En lo que respecta a la elección adecuada, es importante destacar que ambos puntos de acceso son productos de alta calidad que ofrecen funciones avanzadas de Wi-Fi 6 y seguridad mejorada. No obstante, al tomar una decisión, se debe considerar la compatibilidad con otros dispositivos en el entorno. En este contexto, se ha optado por el Aruba AP-22 debido a su mayor nivel de compatibilidad con el equipo Aruba INSTANT ON 1930-48G-PoE, por pertenecer al mismo ecosistema de Aruba. Un aspecto clave en esta elección es que el Aruba AP-22 se alimenta a través de los puertos PoE proporcionados por el mismo conmutador, lo que conlleva a una optimización en la gestión de cables, lo que resulta en una solución más eficiente y ordenada.

2.4.5 Cámaras de videovigilancia

Al realizar diferentes análisis de tipos y marcas de cámaras tanto como de alta, media y baja gama, se optó por dar una solución óptima al cliente en base a la relación calidad precio y especificaciones acorde a la empresa, por tal razón se optó la marca Hikvision de 2 tipos de cámaras, domo y bullet.

Cámara tipo bullets:

Tabla 5. Comparativa entre cámaras tipo bullet para la red de la solución propuesta.

Características	**DS-2CD2T87G2-L (Hikvision)**	**HAC-HFW1239TLM-A-LED (Dahua)**
Calidad de imagen:	Ofrece un servicio de alta Calidad de imagen de 8MP y una resolución máxima de 3840 x2160.	Ofrece 1/2.8 inch 2.16 Mega Pixels CMOS y una máxima resolución 1920 (H)×1080, 2MP.
Resistencia al Agua	Posee IP67, 12V±30% DC, el cual los materiales son de un material hermético que permite que ningún ente externo genere problemas.	Posee visión nocturna IP67, 12V±30% DC, el cual permite que el material de la cámara sea hermético y se protegido contra cualquier contacto.
Visión nocturna	Posee la función colorvu Permite a las cámaras producir vídeos con vivos colores incluso en entornos con poca luz.	Permite obtener imágenes nítidas y a color todo el día, capturan colores vívidos tanto de día como de noche, sin necesidad de incorporar una fuente de luz.
Resolución de video	Transmisión principal: 50 Hz: 25 fps (3840 × 2160, 3200 × 1800 , 2688 × 1520, 1920 × 1080, 1280 × 720) × 1080, 1280 × 720)	Posee una resolución máxima de: 1080p (1920 × 1080); 960H (960 × 576/960 × 480)

Cuando se evalúa en la tabla 5, la elección entre estas dos cámaras es importante considerar las prioridades y necesidades específicas. Se baso en la necesidad de tener video en alta resolución y la función ColorVu que son funciones de las cámaras Hikvision. Por otro lado, si se busca la capacidad de capturar imágenes nítidas y en color tanto de día como de noche sin requerir iluminación adicional, la cámara Dahua podría resultar más apropiada. Sin embargo, debido a la necesidad de compatibilidad con otros equipos del proyecto, se inclina la preferencia hacia el uso de la cámara Hikvision.

Cámara tipo domo:

Tabla 6. Comparativa entre cámaras tipo domo para la red de la solución propuesta.

Características	**IPC-D12H DOMO (Hikvision)**	**HAC-D1A21N-0280B (Dahua)**
Calidad de imagen:	Ofrece un servicio de alta Calidad de imagen de 2MP y una resolución máxima de 31920x1080.	Max. 30 fps@1080p, 2MP CMOS
Nivel de compresión	Alimentación:12VCD/5Watts/PoE (802.3af)., Compresión: H.265+ / H.265 / H.264.	Alimentación 12VDC: Compresión: H.264.
Capacidad	Posee la función antivandálica ik10 resistente a extremos impactos.	Lente fijo de 3.6mm.(2.8 mm. opcional). Salida HD y SD conmutable
Resolución de video	Transmisión principal: 30 fps (1920 × 1080, 1280 × 960, 1280 × 720). Transmisión secundaria: 30 fps (640 × 640 x 360, 320 × 240).	Posee una resolución máxima de: 1080p (1920 × 1080); 720p (1280 × 720); 960H (960 × 576/960 × 480)

Ambas cámaras de la tabla 6 proporcionan una calidad de imagen de 2MP y alcanzan una resolución máxima de 1080p. Ambas cámaras también incorporan capacidades de compresión para mejorar la eficiencia del almacenamiento de datos. La

cámara Hikvision se distingue por su robustez antivandálica y versatilidad en cuanto a las opciones de alimentación. Por otro lado, la cámara Dahua ofrece una resolución de video similar y utiliza una lente fija, con la ventaja de contar con opciones de salida HD y SD que son conmutables según las necesidades del usuario.

CAPÍTULO 3

3.1 Resultados y análisis

Este capítulo se enfoca en los resultados obtenidos y el análisis del despliegue de un sistema de circuito cerrado de televisión (CCTV) mediante la segmentación por VLANs. Los resultados obtenidos han sido fundamentales para la optimización de la gestión de la red, garantizando el aislamiento del tráfico y mejorando la calidad de la vigilancia. Se proporcionará una descripción detallada del diseño de la red LAN y la implementación de la segmentación por VLANs, que ha dado lugar a la creación de dominios de difusión lógica para agrupar dispositivos y cámaras de seguridad relacionados. Además, se llevaron a cabo pruebas tanto en un entorno simulado como en una implementación física.

3.2 Topología física

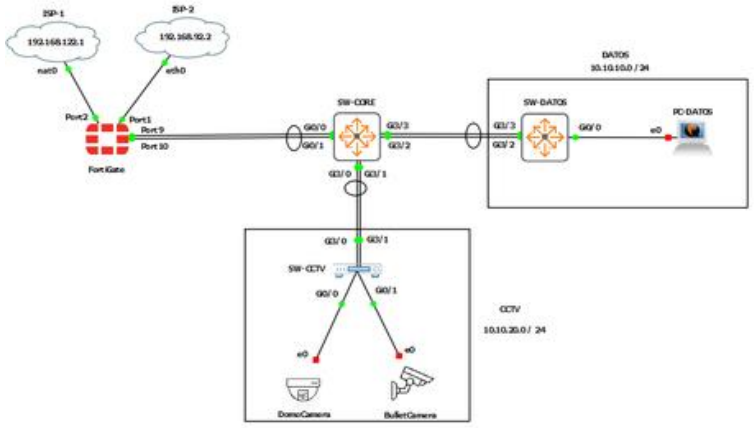


Ilustración 5. Topología física en simulación.

En la topología de red en GNS3 representada en la ilustración 5, se pueden identificar dos proveedores de servicios de Internet al principio (ISP1 e ISP2). Esta configuración brinda la posibilidad de implementar la redundancia utilizando los siguientes dispositivos mencionados a continuación:

1) Equipo FortiGate cumple la función de firewall y enrutador principal. Este dispositivo garantiza protección perimetral y un control del tráfico. Además,

2) Un conmutador Cisco para la conexión y conmutación de dispositivos. Este conmutador opera como un dispositivo de capa 2, que permite la implementación de la configuración de VLANs. En la simulación, se utiliza un equipo Cisco en lugar de uno Aruba para reducir los recursos de memoria RAM requerido.

Adicionalmente, se han agregado dos conmutadores de acceso administrables para conectar dispositivos de usuario final. Aquí, la segmentación de la red también se logra mediante la configuración de VLANs. El equipo FortiGate ejerce el control centralizado del tráfico que entra y sale de la red. Los conmutadores Cisco y Aruba permiten una gestión detallada, y los conmutadores de acceso contribuyen a segmentar la red para lograr una administración eficiente y escalable.

3.3 Segmentación por VLANs

Tabla 7. Segmentación por VLANs

Tipo de datos	VLAN	IP/Mascara de red
Administración de equipos	50	10.10.50.0/24
Datos	10	10.10.10.0/24
VoIP	30	10.10.30.0 /24
CCTV y Control de acceso	20	10.10.20.0 /24

En la tabla 7, se pueden apreciar las direcciones destinadas a la segmentación por VLANs. Se han creado VLANs específicas para datos, VoIP, CCTV y control de acceso, con el objetivo de gestionar de manera efectiva y optimizar los recursos de la red para cada servicio.

Una VLAN de administración de equipos se ha establecido para la gestión y administración de dispositivos de red. Se ha asignado una dirección IP de 192.168.37.130 al equipo FortiGate en esta VLAN, que se encuentra dentro del rango de IP 192.168.37.129. Esta configuración asegura un acceso exclusivo a los dispositivos de administración, manteniéndolos separados del tráfico de datos común en la red principal.

La VLAN de datos, ubicada en el puerto dos de la interfaz física, se destina al tráfico de usuarios y dispositivos que acceden a los recursos y aplicaciones de la red local. Esta segmentación permite una gestión más eficaz del tráfico, previene congestiones y mejora la calidad del servicio. Además, mediante el firewall Fortinet, se aplican políticas de red para denegar servicios de transmisión en vivo, evitando así el uso no deseado de ancho de banda en la red corporativa.

En la VLAN de datos, con la IP 10.10.10.0/24, se utilizan los Hit Counts, que registran la cantidad de veces que un puerto o dispositivo ha sido alcanzado por el tráfico de red. Estos contadores proporcionan información para monitorizar la actividad y planificar la capacidad de la red. Como se observa en el Anexo C ‘’Visualización de Hit Counts en la VLAN de datos’’, se registran 15 hit counts en siete días, lo que equivale a un total de 1.68 kB. Actualmente, el uso de VPCS (Virtual PCs) contribuye a que la capacidad sea baja en esta simulación, ideal para emular el comportamiento de las PC físicas.

La VLAN de VoIP, localizada en el puerto tres de la interfaz física, se encarga del tráfico de telefonía IP. Al separar este tráfico, se prioriza la transmisión de paquetes de voz y se evitan retrasos que puedan afectar la calidad de las llamadas. Esta VLAN está preparada para una posible futura implementación de servicios de telefonía IP en la empresa.

La VLAN de CCTV y control de acceso, situada en el puerto cuatro de la interfaz física, maneja el tráfico de cámaras de seguridad y facilita la administración y supervisión de imágenes y videos capturados. Al aislar el tráfico de CCTV, se minimiza el impacto en el rendimiento de otras aplicaciones y se garantiza una mayor seguridad para la información sensible. Además, se implementa el control de acceso para la gestión de dispositivos de seguridad, como lectores de tarjetas y sistemas biométricos, lo que permite una administración segura y eficiente de los accesos a áreas restringidas, reduciendo las posibles vulnerabilidades en la red.

En la VLAN CCTV, con la IP 10.10.20.0/24, se utilizan los Hit Counts para monitorizar la actividad y planificar la capacidad de la red. Como se muestra en el Anexo D ‘’Visualización de Hit Counts en la VLAN de CCTV’’, se registran 10 hit counts en siete días, lo que suma un total de 1.26 kB. La capacidad actual es baja debido al uso de VPCS; sin embargo, en la implementación física, será diferente.

Las políticas de priorización del tráfico se detallan en la tabla 8:

Tabla 8. Priorización del tráfico

Tipo de trafico	Prioridad
CCTV	1
VoIP	2
Datos	3

Los datos necesarios para garantizar la disponibilidad continua del tráfico de videovigilancia se han incorporado en el equipo FortiGate, un aspecto crucial para la visualización constante de las cámaras de seguridad. Paralelamente, se ha evaluado la posibilidad de implementar VoIP para mejorar la comunicación interna de manera eficaz y rápida. Dado que ambos tipos de tráfico mencionados presentan una carga reducida en la red, se ha otorgado prioridad al tráfico de Datos en última instancia.

Esta priorización se aplica exclusivamente a los datos administrativos de la empresa. Es relevante destacar que esta configuración se ha llevado a cabo meticulosamente, considerando la interacción entre estas prioridades y las políticas de red para evitar conflictos con las políticas adicionales aplicadas por los cortafuegos de los proveedores de servicios de Internet (ISP).

3.4 Conectividad y políticas entre equipos

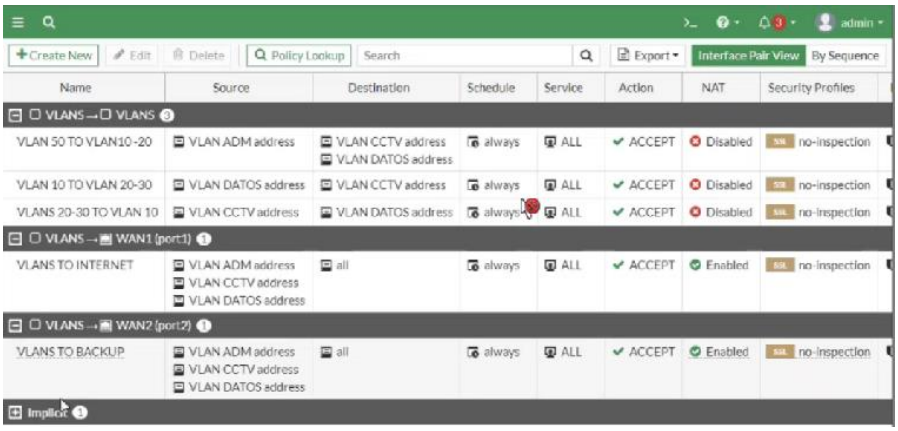


Ilustración 6. Políticas y conectividad en el equipo FortiGate.

En la ilustración 6 se pueden examinar las políticas configuradas en el equipo FortiGate, las cuales han sido establecidas para bloquear el tráfico procedente de cada

una de las VLANs. Para verificar la efectividad de estas políticas, se llevaron a cabo pruebas utilizando la interfaz de línea de comandos (CLI). Se realizaron pruebas de conectividad con el comando "ping" para evaluar la conectividad entre los dispositivos de la red. Se envió un ping desde el Fortinet hacia las PC1 de la VLAN de Datos y PC3 de la VLAN de CCTV, y los resultados mostraron respuestas exitosas, lo que indica una conectividad sólida entre el Fortinet y las PC de cada VLAN.

Además, pruebas de conectividad desde PC1, que se encuentra en la VLAN 10 (Datos), hacia PC3, ubicada en la VLAN 20 (CCTV), no se detectó comunicación. Esto demuestra que la segmentación de la red ha logrado aislar efectivamente los paquetes enviados desde las cámaras de CCTV, evitando cualquier interferencia con los paquetes de datos utilizados por el personal de la empresa.

3.5 Seguridad para el diseño de la Red

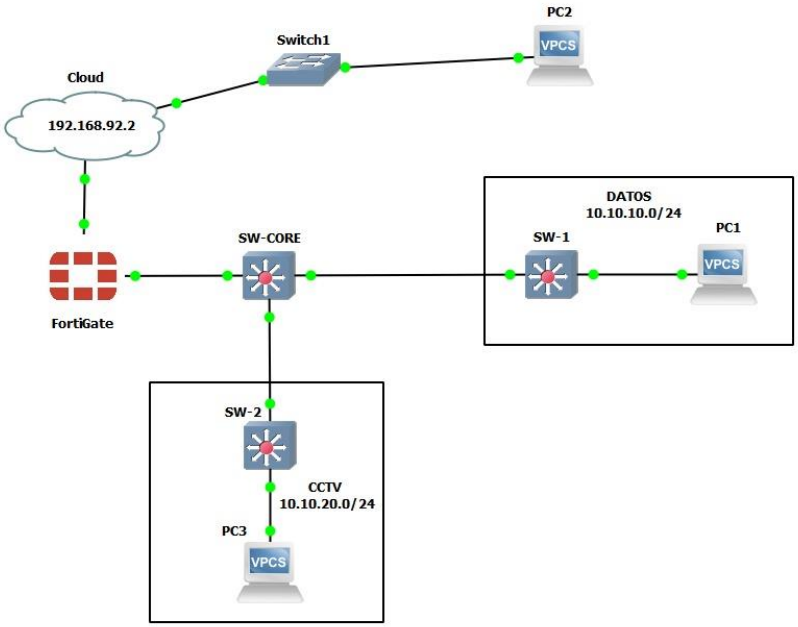


Ilustración 7. Simulación conmutador externo que se conecta a la red.

En la ilustración 7, se presenta la topología que incluye una configuración de conexión entre un conmutador básico y la nube, lo que permite la interacción entre los dispositivos conectados. Esto incluye la PC2, que intenta establecer comunicación a través del Firewall Fortinet en la red. La nube está configurada para utilizar DHCP, lo que significa que asigna automáticamente una dirección IP dentro del mismo rango de direcciones utilizado por el Firewall.

Esta configuración impone restricciones de acceso mediante medidas de seguridad detalladas que se describen en la ilustración 6. Como resultado de estas precauciones de seguridad, no es factible establecer comunicación a través del comando ping desde la PC2 hacia el Firewall Fortinet.

3.6 Cobertura de los AP

Para determinar la extensión de la cobertura de los puntos de acceso, se ha empleado la aplicación VisualRF de Aruba Central, la cual posibilita la creación de un mapa de calor que representa de manera visual la potencia de la señal en diferentes áreas. Para llevar a cabo este proceso, se ha realizado un mapeo Wi-Fi utilizando un dispositivo móvil mientras se recorría el área de interés. En cada ubicación, se registraba la intensidad de la señal, para lo cual se ha usado de base un área similar a la de cada uno de los pisos .

Los datos obtenidos se han plasmado en el mapa de calor, el cual destaca las áreas con señales fuertes y aquellas con señales más débiles. Tras un análisis detenido de estos datos, se ha llegado a la conclusión de que se requieren tres (3) puntos de acceso por piso para garantizar la cobertura de las zonas que presenten problemas de señal o áreas con poca intensidad. La ubicación óptima para estos puntos de acceso consiste en colocarlos en una posición central elevada, evitando áreas con muchas interferencias para asegurar un rendimiento óptimo de la señal Wi-Fi.

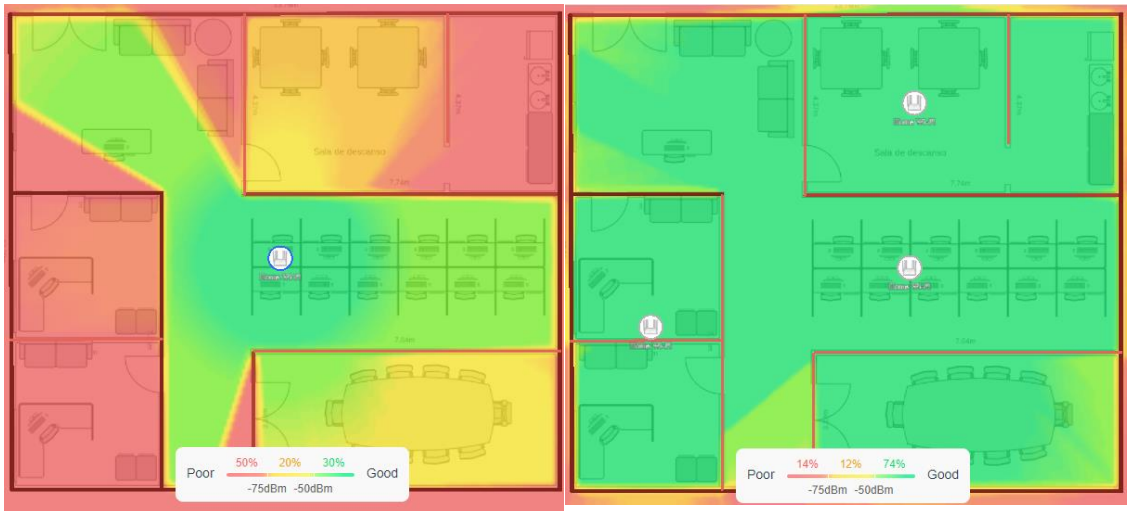


Ilustración 8. **Bosquejo de simulación de mapa de calor con mala cobertura y buena cobertura.**

Se ha desarrollado un esquema para ilustrar cómo se determinó la cantidad de puntos de acceso (AP) necesarios en cada piso de la empresa. En el lado izquierdo de la

ilustración 8, se representa un único AP en el piso, y se pueden identificar áreas en color rojo que indican una falta de cobertura de señal en esos puntos.

Este problema se debe a la elección de materiales de construcción, específicamente las paredes de ladrillo, que tienen una alta atenuación de la señal, tal como lo mencionó el cliente. Para resolver este inconveniente, se decidió agregar más AP en el piso. Como se muestra en el lado derecho de la ilustración 8, la mayoría de las áreas ahora están representadas en verde, lo que significa que todas las oficinas contarán con una mejor recepción de señal de los AP, asegurando una cobertura óptima si es necesario.

3.7 Saturación en la red

Con el objetivo de prevenir la congestión en la red y proporcionar calidad del servicio, se ha incorporado LACP en la configuración del equipo FortiGate. Esta medida produce efectos positivos en múltiples aspectos cruciales. La configuración de LACP aumenta significativamente el ancho de banda al combinar varios enlaces físicos en un solo enlace lógico. Esto resulta en una distribución equitativa del tráfico y reduce las posibilidades de congestión en enlaces individuales.

Además de los beneficios en términos de ancho de banda, la implementación de LACP ofrece ventajas en escalabilidad y administración. Al crear una interfaz lógica única a través de LACP, se simplifica la gestión de la red, lo que resulta especialmente valioso cuando se considera la expansión futura de la red. Esto facilita la adición de nuevos enlaces para satisfacer las crecientes demandas de capacidad.

Para medir el rendimiento de la red, se empleó la herramienta de línea de comandos IPerf. Se realizaron pruebas de envío y recepción de datos, incluyendo la generación de paquetes con el protocolo UDP en modo Verbose para obtener datos precisos. Los resultados obtenidos se detallan a continuación.

Tabla 9. Tráfico en UDP

Tipo de paquete	Ancho de Banda	Tasa de transferencia	Jitter	Uso de CPU	Perdidas de datagramas
UDP	1.85 Mbits/s	1 Mbit/s	2.586 ms	0.1%	0%
UDP	9.98 Mbits/s	10 Mbits/s	1.265 ms	0.3%	0%
UDP	94.8 Mbits/s	100 Mbit/s	0.676 ms	1.9%	6%

En la tabla 9 se presentan los resultados obtenidos a través de la ejecución del comando IPerf, revelando una relación entre el aumento en la tasa de transferencia de datos y la disminución del "jitter" en la red. A una tasa de transferencia de 10 Mbit/s, se observa que no se han registrado pérdidas de datagramas y el uso de la CPU se mantiene en niveles bajos, lo que sugiere un rendimiento óptimo de los equipos.

Sin embargo, al aumentar la tasa de transferencia a 100 Mbit/s, se nota un ligero aumento en el uso de la CPU, llegando a un 1.9%. Aunque este valor sigue siendo relativamente bajo, proporciona información sobre la capacidad de la infraestructura de red para manejar tasas de transferencia más elevadas.

3.8 Prototipo físico del sistema CCTV

Para la implementación del prototipo físico se han empleado los siguientes dispositivos: un conmutador Aruba, un NVR de cuatro canales, un disco duro de un TB, así como una cámara tipo Bullet y otra de tipo Domo. A partir de estos elementos, se han generado datos sobre la compresión de la información que se almacena en el NVR.

Tabla 10. Compresión de video

Cámara	Tiempo	Compresión	FPS	Resolución	Peso(MB)
Exterior	1 hora	H.264+	30	720p	78.3
Interior	1 hora	H.264+	30	720p	62.7
Exterior	1 hora	H.265+	30	720p	39.3
Interior	1 hora	H.265+	30	720p	31.1
Exterior	24 horas	H.264+	30	720p	1985.6
Interior	24 horas	H.264+	30	720p	1776.4
Exterior	24 horas	H.265+	30	720p	953.8
Interior	24 horas	H.265+	30	720p	893.7

Al analizar los resultados de la tabla 10, la compresión H265+ reduce el espacio en el disco duro a la mitad. Esto implica una ventaja significativa, ya que permite un mayor tiempo de almacenamiento de los respaldos de video en el disco y, al mismo tiempo, reduce los costos relacionados con la adquisición de discos duros. Cabe destacar que el equipo NVR Hikvision DS-77732NI-I4 es compatible con esta forma de compresión. El contraste que se nota en el tamaño de las cámaras, ya sean interiores o exteriores, se debe al menor movimiento en el interior, lo que permite que la cámara mantenga una imagen más estática, ahorrando espacio en el disco duro.

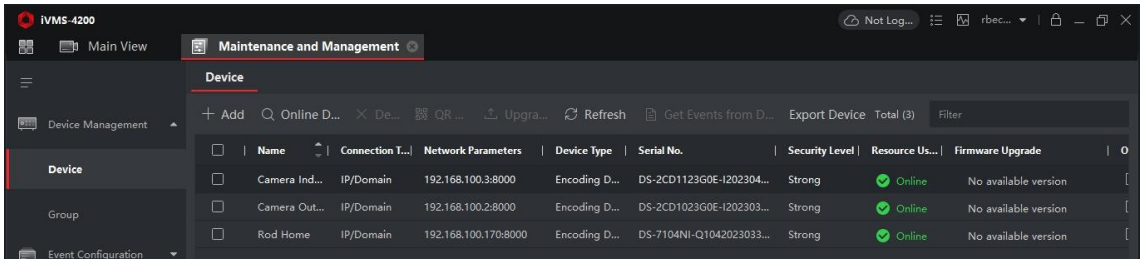


Ilustración 9. Servidor donde se alojan las cámaras.

Para visualizar tanto la transmisión en tiempo real como las grabaciones de video, se emplea la aplicación Hik-Connect. Esto facilita la capacidad de un administrador para compartir el contenido con múltiples usuarios que requieran visualizarlo en varios dispositivos simultáneamente. Además, dentro de las instalaciones de la empresa, se utiliza el servidor IVMS-4200 como se ve en la ilustración 9, en conjunto con los NVR para almacenar y reproducir todas las grabaciones de video. Para verificar el estado operativo de las cámaras, se recurre al programa Sadptool, que permite la visualización de las cámaras y sus direcciones IP correspondientes.

3.9 Estimación económica

Tabla 11. Cotización equipos y elementos de la solución propuesta.

Cantidad	Equipo	Marca	Modelo	Costo Total
1	Firewall	Fortinet	40F	$444.32
2	Conmutador	Aruba	INSTANT ON 1930-48G-PoE	$1008.00
2	NVR	Hikvision	DS-7732NI-I4/24P	$1117.12
9	Punto de acceso	Aruba	AP-22	$2968.56
24	Cámara interior	Hikvision	IPC-D12H DOMO	$1103.76
6	Cámara exterior	Hikvision	DS-2CD2T87G2-L	$426.44
6	Sistema biométrico	Hikvision	DS-K1T341AMF-S	$894.26
2	Bobina cable UTP	NEXXT	Nexxt AB356NXT21 CAT 6	$132.16
1	Rack	NEXXT	T32U66B – RAL 9005	$759.36
2	Conector RJ45	QCOM	QP-Cat5E 100 unidades	$30.92
4	Patch Panel	QPCOM	QP-16	$67.2
		Total		8952.10

Es importante recalcar que los sistemas de circuito cerrado de televisión (CCTV) se lleva a cabo a través de distribuidores, lo que asegura la autenticidad y garantía de los productos. En este proceso, se realizaron cotizaciones directamente con proveedores locales, así como en el portal web de Amazon, donde se incluyó el costo de envío a Ecuador. Esto se debió a que se encontraron opciones más económicas en Amazon en comparación con las ofrecidas por las distribuidoras locales.

CAPÍTULO 4

4.1 Conclusiones y recomendaciones

4.1.1 Conclusiones

- Con el propósito de lograr una separación lógica de los dispositivos de CCTV y, como resultado, mejorar la seguridad al reducir la exposición y prevenir intrusiones no autorizadas, se ha implementado el uso de VLANs. La inclusión del equipo FortiGate refuerza aún más esta seguridad al restringir la administración de la red a través de sus puertos.

- La combinación de la segmentación de VLANs y la implementación de LACP mejora la eficiencia y disponibilidad de la red, priorizando el tráfico de CCTV y brindando redundancia y mayor ancho de banda. Estas mejoras se fundamentan en los datos obtenidos en las secciones 3.3 y 3.7.

- La adopción del método de compresión de video H.265+ en el NVR resulta en un aumento significativo en la eficiencia del almacenamiento, la calidad de la imagen y la optimización del uso del ancho de banda en el sistema de vigilancia propuesto, como se detalla en la tabla 10 de la sección 3.8.

4.1.2 Recomendaciones

- Garantizar que tanto los dispositivos de CCTV como los equipos de red estén siempre actualizados con las últimas actualizaciones de seguridad y parches disponibles. Los fabricantes suelen implementar parches de seguridad para abordar vulnerabilidades conocidas, y es esencial aplicar estas actualizaciones de forma periódica.

- Realizar un seguimiento constante de la red de CCTV y de las VLANs. Utilizar herramientas de monitoreo para detectar cualquier actividad sospechosa y responder rápidamente a posibles amenazas como la aplicación de Saptool.

- Desarrollar un plan de respuesta ante incidentes que incluya los pasos a seguir en caso de un posible compromiso de seguridad en la red de CCTV. Esto ayudará a mitigar rápidamente las amenazas y minimizar los posibles daños.

- Establecer la topología para la VLAN de VoIP es esencial, ya que sus configuraciones cuentan con la priorización adecuada. La única pieza que resta es la implementación de la central telefónica IP para que esta VLAN pueda operar completamente.

- Verificar los datos de características técnicas de los equipos, se evalúa si son compatibles con las tecnologías y estándares de la infraestructura actual y futura. Al hacerlo, se minimiza el riesgo de invertir en equipos que podrían volverse obsoletos o incompatibles con futuros avances tecnológicos, y se asegura una inversión a largo plazo que respalde el crecimiento y la evolución de la empresa sin interrupciones.

Referencias

Referencias

Chávez, D. (2022). *Diseño de un sistema CCTV basado en tecnología IP y almacenamiento en la nube para la urbanización Eloy Alfaro* [Tesis de grado Universidad Politécnica Salesiana Sede Quito]. Dspace. http://dspace.ups.edu.ec/handle/123456789/22205

Pavón, J. (2016). *Análisis técnico de la implementación de un sistema de seguridad de video vigilancia, caso de estudio Aeropuerto Internacional Mariscal Sucre del Ecuador* [Tesis de posgrado Pontificia Universidad Católica del Ecuador]. PUCE. http://repositorio.puce.edu.ec/handle/22000/12578

Rivas y Velázquez. (2011). *Implementación de sistema de seguridad con videovigilancia y software libre* [Tesis de grado Instituto Politécnico Nacional de México]. IPN. https://tesis.ipn.mx/jspui/bitstream/123456789/11622/1/3.pdf

Palo Alto Network. (2022). *Palo Alto Networks PA-220 Datasheet. Palo Alto Network.* https://www.paloaltonetworks.com/resources/datasheets/pa-220-specsheet

Fortinet. (2022). *FortiGate FortiWiFi 40F Series Datasheet. Fortinet.* https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-40f-series.pdf

Cisco. (2020). *Cisco Catalyst 2960-L Series Switches Data Sheet. Cisco.* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-l-series-switches/nb-06-cat2960-l-ser-data-sheet-cte-en.html

Hewlett Packard Enterprise Development LP. (2020). *Serie Switches Aruba Instant On. Aruba.* https://www.arubainstanton.com/files/DS_AIO_1930SwitchSeries_latam.pdf

Hikvision Digital Technology Co.,Ltd. (2020). *DS-7732NI-I4/24P NVR Datasheet. Hikvision.* https://www.hikvision.com/content/dam/hikvision/products/S000000001/S000000002/S000000007/S000000026/OFR000040/M000000601/Data_Sheet/Datasheet-of-DS-7732NI-I4_24P_NVR_V4.61.000-20220430.pdf

Dahua Technology Co., Ltd. (2021). *Dahua NVR5216/5232-16P-4KS2E Datasheet. Dahua.* https://www.dahuasecurity.com/products/All-Products/Network-Recorders/Pro-Series/NVR5-Series/2HDD/NVR5216/5232-16P-4KS2E

Hewlett Packard Enterprise Development LP. (2022). *Hoja técnica Access Point interior Aruba Instant on AP22. Aruba.* https://www.arubainstanton.com/files/DS_AIO_AP22_latam.pdf

Cisco. (2022). *Cisco Catalyst 9117 Series Access Points Data Sheet. Cisco.* https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/datasheet-c78-741989.html

Hikvision Digital Technology Co.,Ltd. (2020). *DS-2CD2T87G2-L 8 ColorVu Fixed Bullet Network Camera Datasheet. Hikvision.* https://www.hikvision.com/content/dam/hikvision/products/S000000001/S000000002/S000000003/S000000025/OFR007893/M000041483/SM000058363/Data_Sheet/DS-2CD2T87G2-L-C_Datasheet_V5.5.115_20230418.pdf

Dahua Technology Co., Ltd. (2020). *Dahua HAC-HFW1239TLM(-A)-LED Full-color Starlight HDCVI Bullet Camera Datasheet. Dahua.* https://www.dahuasecurity.com/products/All-Products/Discontinued-Products/HDCVI-Cameras/HAC-HFW1239TLM(-A)-LED

Hikvision Digital Technology Co.,Ltd. (2020). *IPC-D121H(-M) IR Fixed Dome Network Camera Datasheet. Hikvision.* https://www.hikvision.com/content/dam/hikvision/products/S000000036/S000000037/S000000038/S000000039/OFR000047/M000000474/Data_Sheet/IPC-D121H-M_Datasheet_V5.5.83_20190626.pdf

Dahua Technology Co., Ltd. (2020). *Dahua HAC-D1A21 HDCVI IR Dome Camera Datasheet. Dahua.* https://www.dahuasecurity.com/la/products/All-Products/HDCVI-Cameras/Cooper-Series/1080P/HAC-D1A21

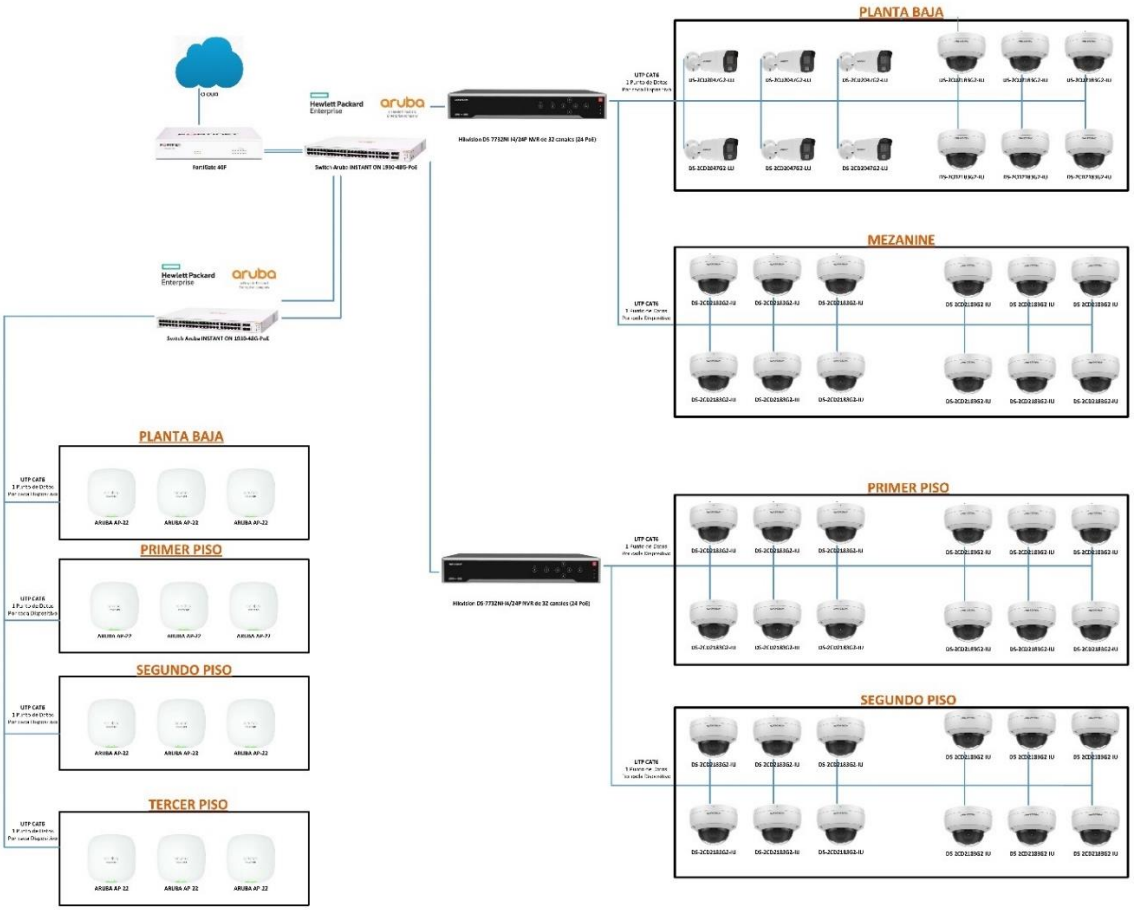
Huertas, V. (2018). *Análisis Comparativo De Protocolos De Comunicación De Redes Para Un Sistema De Videovigilancia* [Tesis de grado Universidad Señor de Sipán]. USS. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/6223/Huertas%20Honores%20Victor%20Manuel.pdf?sequence=1&isAllowed=y

Abril y Cuzco. (2019). *Implementación De Un Sistema De Video Vigilancia Remoto Para Hogares, Utilizando Herramientas de Software Libre* [Proyecto Técnico Universidad Politécnica Salesiana Sede Cuenca]. Dspace. https://dspace.ups.edu.ec/bitstream/123456789/17311/1/UPS-CT008253.pdf

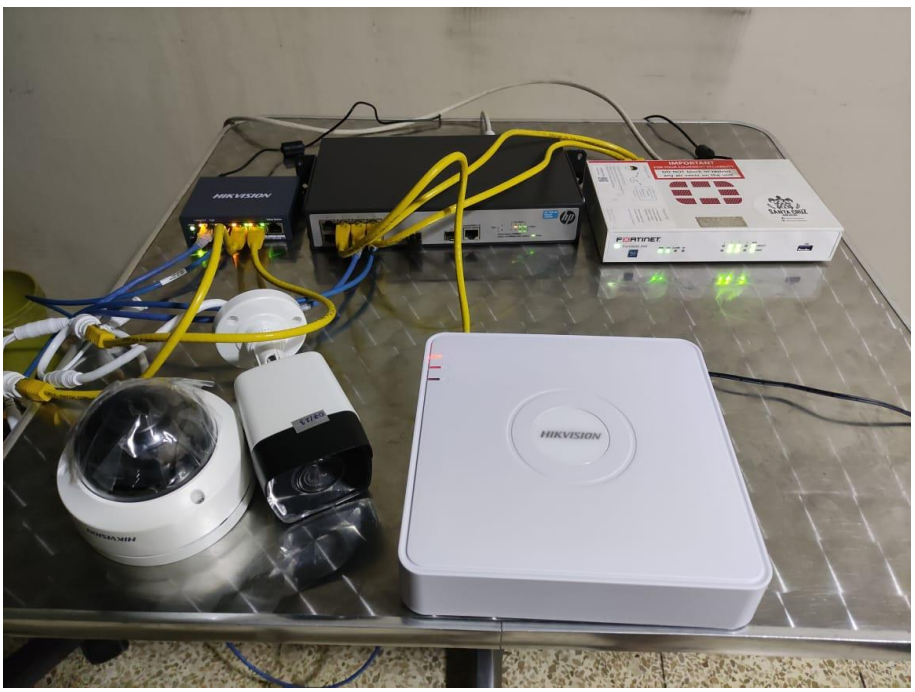
Anexos

Anexos

Topología Física y Experimental

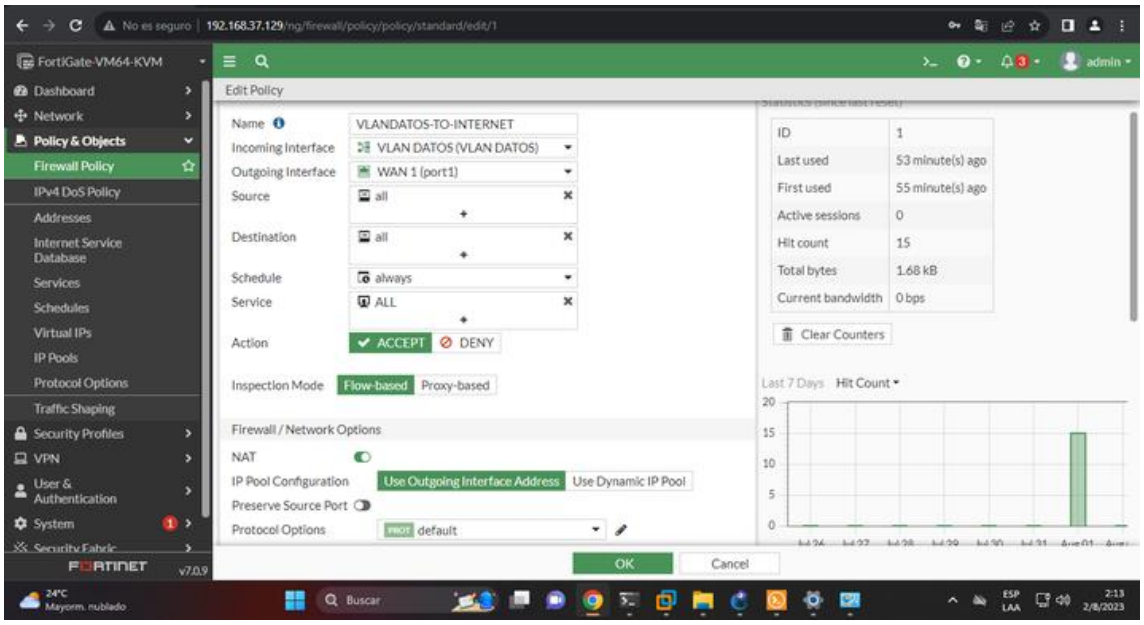


Anexo A. Primera solución de topología física.

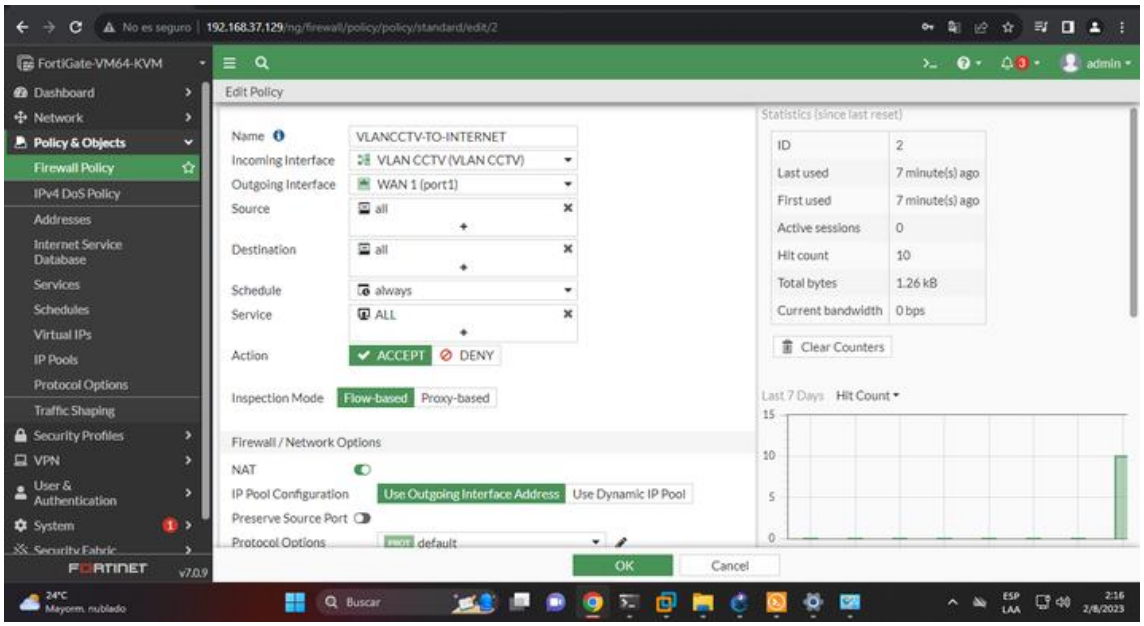


Anexo B. Topología física con uso de equipos reales.

Segmentación por VLANs

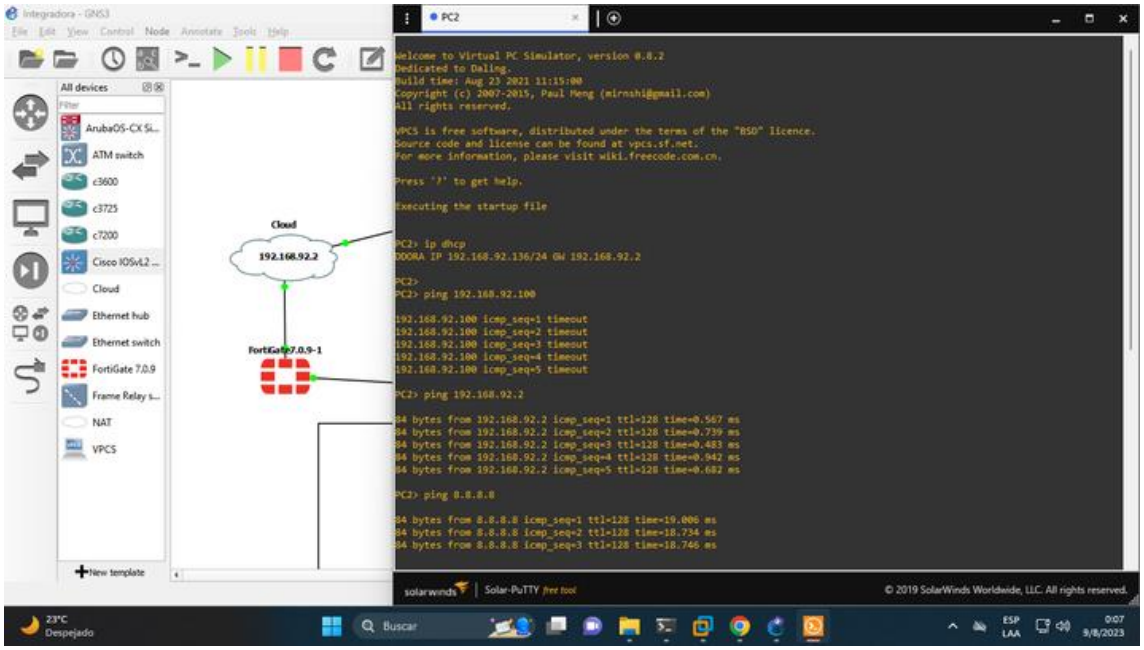


Anexo C. Visualización de Hit Counts en la VLAN de datos.



Anexo D. Visualización de Hit Counts en la VLAN de CCTV.

Seguridad en la Topología de Red

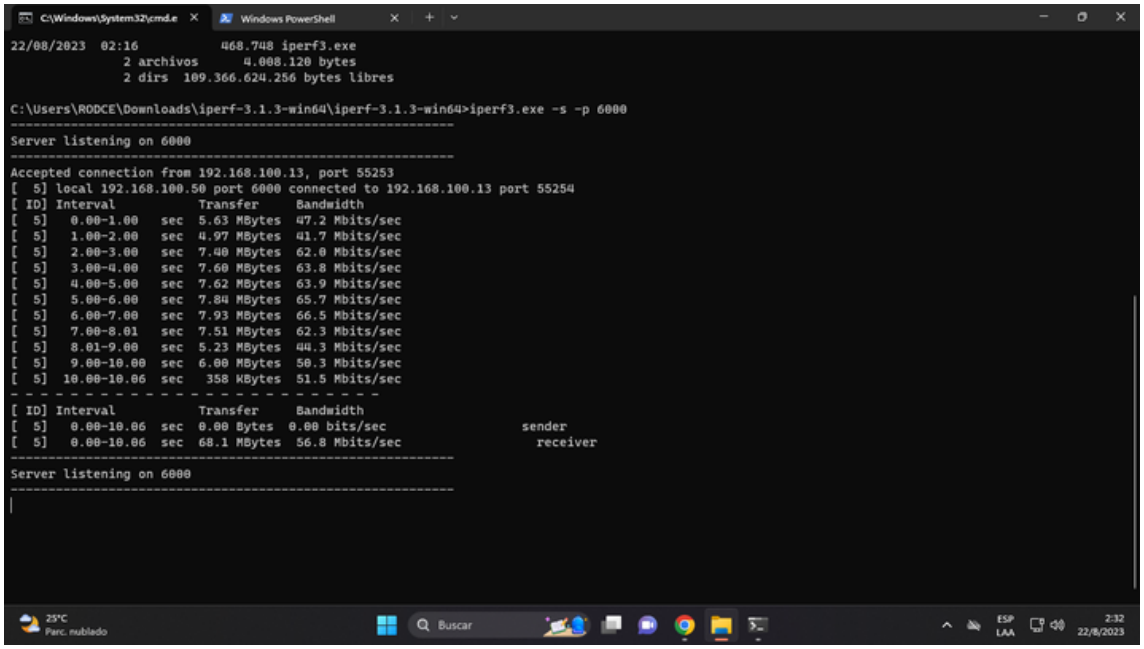


Anexo E. Prueba de ping de la prueba presente en el capítulo 3.5.

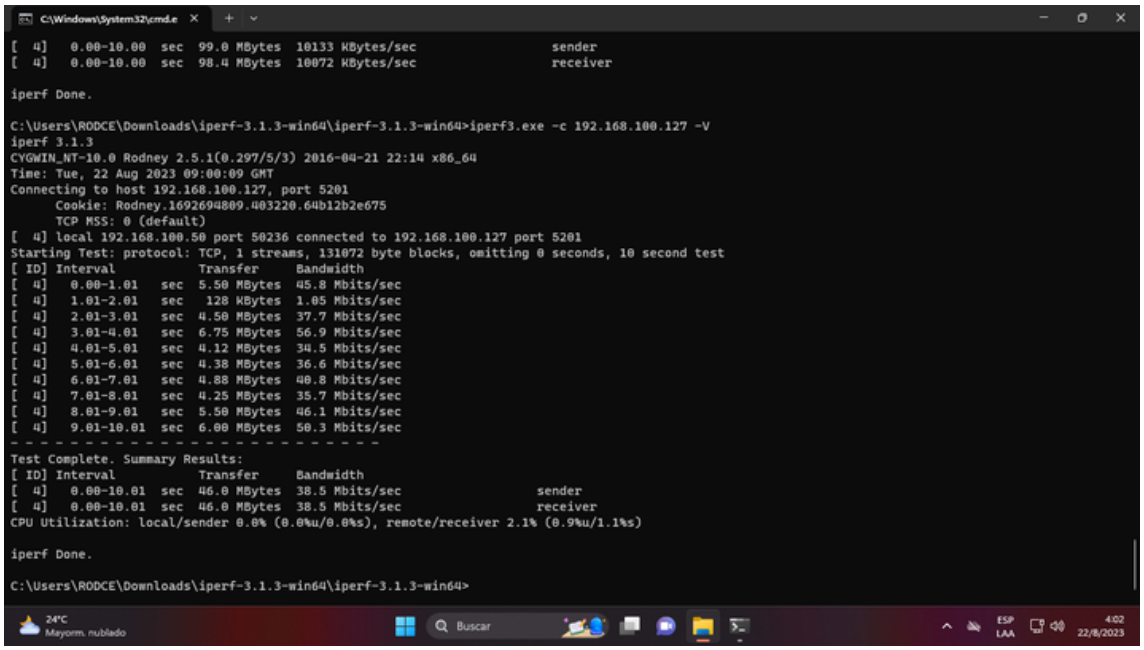
Aplicación para visualización de las cámaras remotamente.

Anexo F. Visualización acceso a las cámaras para la aplicación Hik-Connect.

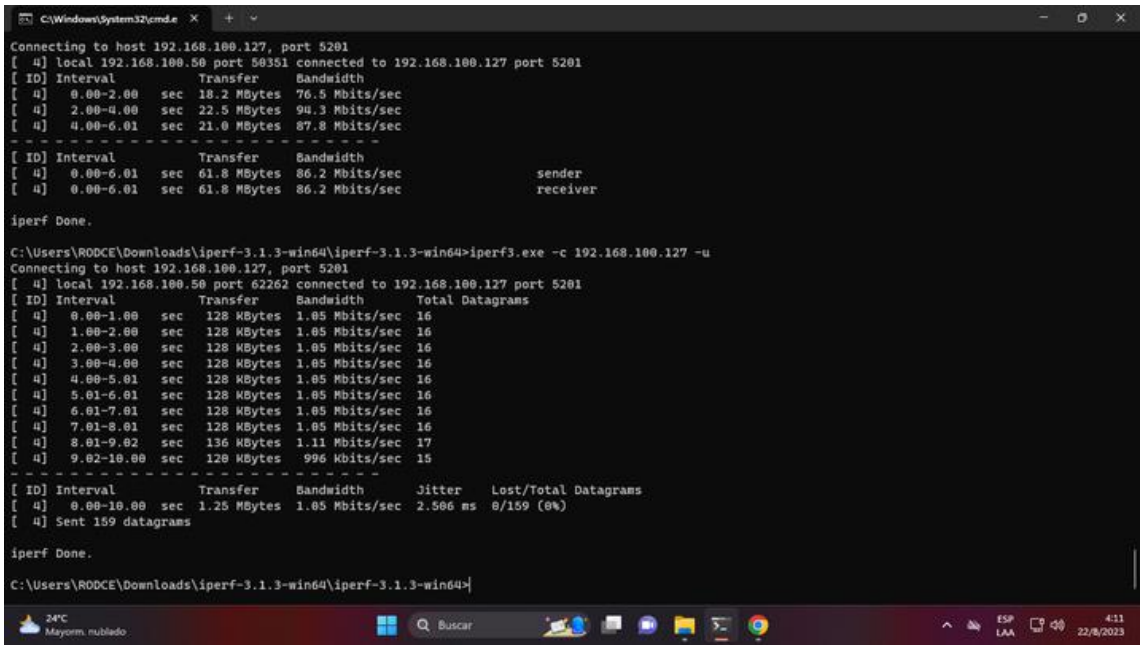
Pruebas de la saturación de red con el comando IPerf



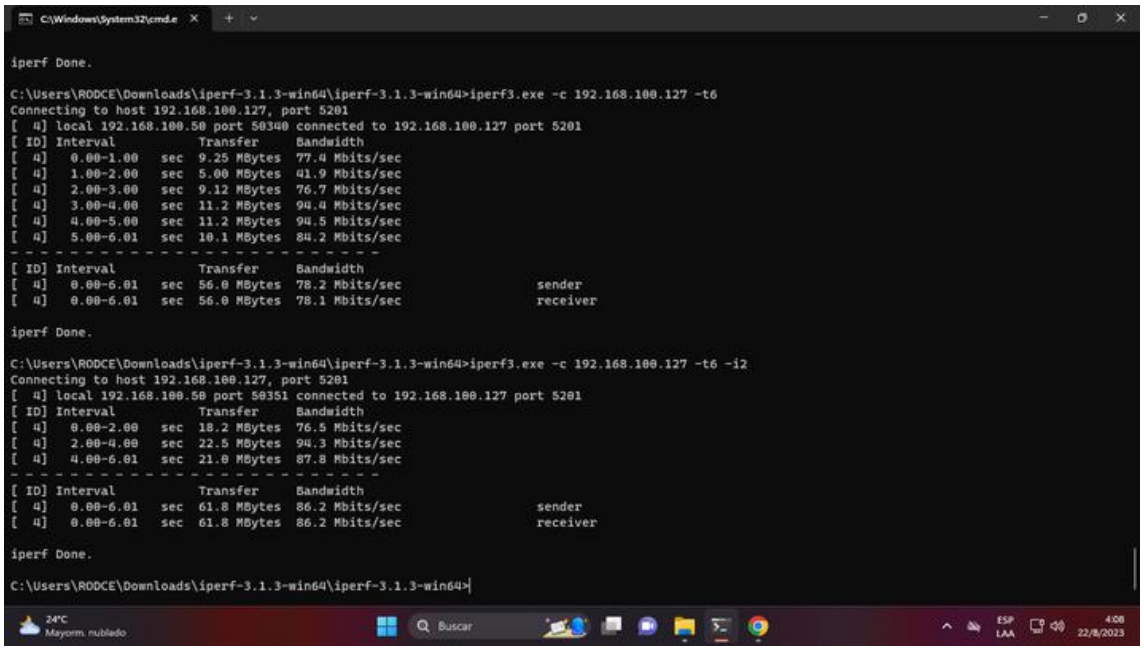
Anexo G. Ancho de banda obtenido con el comando IPerf.



Anexo H. Uso del comando IPerf en modo Verbose para ancho de banda.



Anexo I. Uso del comando IPerf para envio de datos UDP y sus resultados.



Anexo J. Uso del comando IPerf para envio de datos TCP y sus resultados.