UPN
UNIVERSIDAD PRIVADA DEL NORTE

FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

"REDISEÑO DE IP DE LA RED DE DATOS EN LA CENTRAL DE CONTROL Y VIDEO VIGILANCIA DE LA MUNICIPALIDAD DE SANTA ANITA, LIMA EN 2024"

Trabajo de suficiencia profesional para optar al título profesional de:

Ingeniero de Sistemas Computacionales

Autor:

Cesar Wilder Abanto Barrios

Asesor:

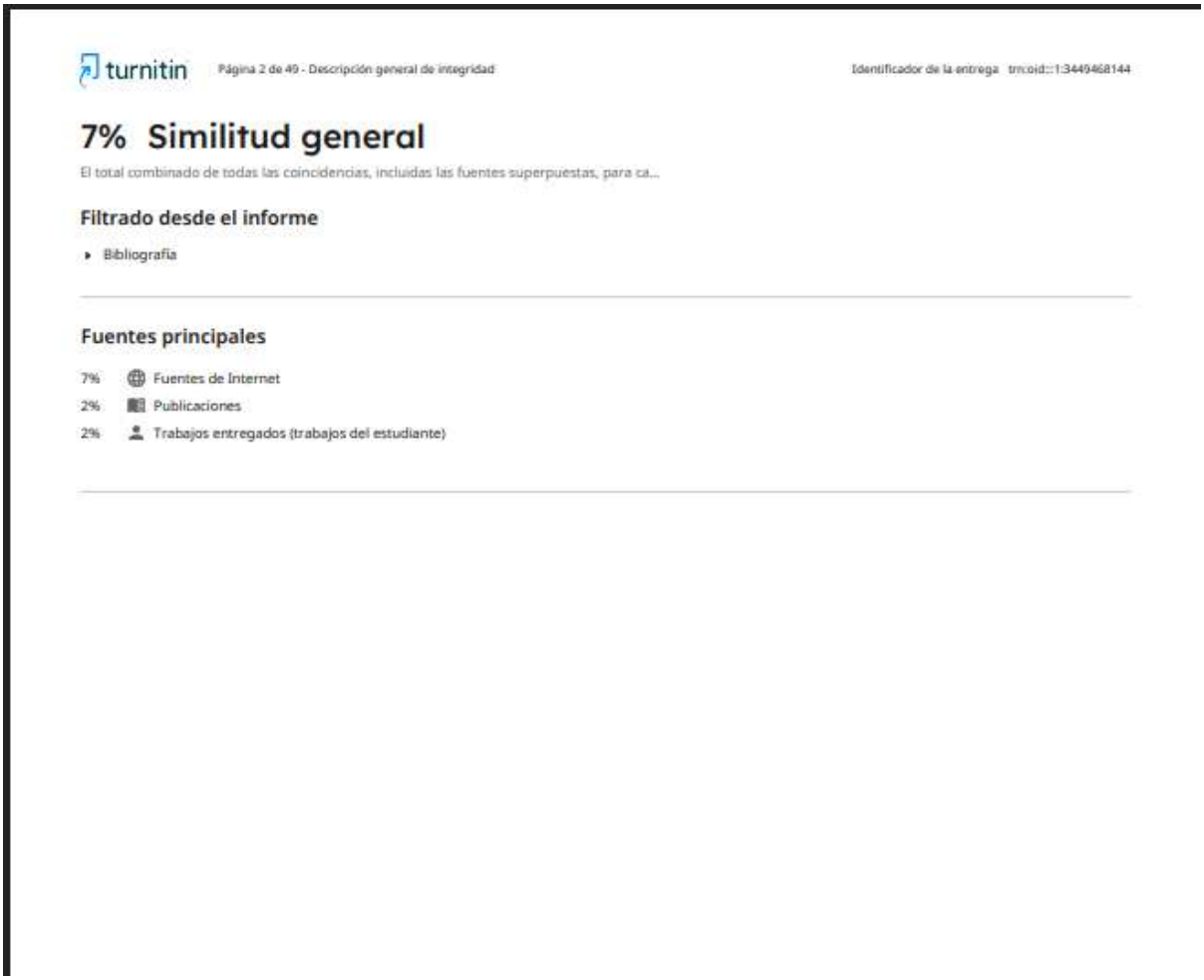
Dr. Hugo José Luis Romero Ruiz

https://orcid.org/0000-0002-6179-8736

Lima - **Perú**

2025

Informe de Similitud



turnitin Página 2 de 49 - Descripción general de integridad Identificador de la entrega trn:oid:::1:3449468144

7% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía

Fuentes principales

7% Fuentes de Internet
2% Publicaciones
2% Trabajos entregados (trabajos del estudiante)

Dedicatoria

- A mi mamá Angela, mi papá Beto, mi abuela Nelly, que siempre creyó en mi desde el inicio de mi carrera y con su amor incondicional y esfuerzo me apoyaron en este largo camino de experiencias, aprendizajes, altas y bajas, así como a las personas que me apoyaron para realizar este trabajo de suficiencia profesional.

- A mi hermano menor Caloggero, le dedico este trabajo de suficiencia profesional como prueba de que con esfuerzo y dedicación puede lograr grandes cosas, esta para mí en una de esas y sé que el estará destinada a muchas más.

- A mi abuelo Rafael, mi tío Cesar que me quisieron en vida y están orgullosos y felices desde el cielo viendo la persona que soy hoy en día, siguiendo todos sus consejos y enseñanzas, siempre los voy a tener presentes hoy y siempre.

- A mis tías Rosa Barrios y Rosa Velásquez por su apoyo incondicional en todo momento desde que estaba estudiando hasta la actualidad y por haberme dado la oportunidad de empezar a ejercer como profesional.

- Al Gerente de Seguridad Ciudadana, General (R) José Humberto Velásquez Borjas, de la Municipalidad de Santa Anita por la confianza depositada en mi para desempeñar una buena labor en mi área de trabajo.

Agradecimiento

- Al Dr. Hugo José Luis Romero Ruiz por su apoyo y asesoría a lo largo de todo este trabajo de suficiencia profesional.
- A mis profesores de la universidad, profesor Danny Herrera, profesor Cesar Reyes, profesor Juan Tapia, profesor Enrique Morales, ya que a lo largo de mi carrera universitaria que me enseñaron los conocimientos que hoy por hoy aplico en mi ámbito laboral.
- Además, a la Universidad Privada del Norte por permitirme brindarme un buen ambiente y profesores con las capacidades y enseñanzas para llegar a ser el profesional que soy hoy en día.

Tabla de contenido

Índice de Tablas 6

Índice de Figuras 6

RESUMEN EJECUTIVO 7

CAPÍTULO I. INTRODUCCIÓN 8

CAPÍTULO II. MARCO TEÓRICO 14

CAPÍTULO III. DESCRIPCIÓN DE LA EXPERIENCIA 20

CAPÍTULO IV. RESULTADOS 26

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES 29

REFERENCIAS 33

Índice de Tablas

Tabla 1 26

Índice de Figuras

Figura 1 11

Figura 2 12

Figura 3 20

Figura 4 21

Figura 5 23

Figura 6 25

Figura 7 25

RESUMEN EJECUTIVO

El trabajo de suficiencia profesional abordó el problema de inestabilidad y conflictos de direccionamiento IP en la red de datos de la Central de Control y Videovigilancia de la Municipalidad de Santa Anita, lo que afectaba la conectividad de las estaciones de monitoreo. La causa principal identificada fue un esquema de direccionamiento IP desordenado, sin segmentación lógica, que generaba tráfico excesivo de broadcast y dificultades en el diagnóstico de fallas. Para la solución, se aplicaron herramientas y modelos de gestión de redes, como el rediseño del direccionamiento IP, uso de máscaras de subred /24, separación lógica entre la red de cámaras y la red de comunicaciones, pruebas de conectividad mediante el comando ping, y la instalación de un router adicional para el área administrativa, además de una red Wi-Fi de contingencia. Los resultados evidenciaron una mejora significativa en la estabilidad de la red, eliminación de conflictos de IP y un buen desempeño con respecto a la conectividad. Se concluye que un adecuado ordenamiento del direccionamiento IP es clave para garantizar la seguridad ciudadana. Las competencias aplicadas incluyen gestión de redes, diagnóstico técnico, trabajo en equipo, toma de decisiones y responsabilidad profesional.

CAPÍTULO I. INTRODUCCIÓN

El autor del presente Trabajo de Suficiencia Profesional (TSP), se graduó de bachiller en Ingeniería de Sistemas por la Universidad Privada del Norte (UPN) en julio del 2022 y sus primeros desempeños como tal, los desempeñó en posiciones temporales en dos municipalidades limeñas, gracias a un contacto profesional y la experiencia adquirida en las entidades ediles, fue notificado de un requerimiento de personal en la Municipalidad de Santa Anita, donde encontró una convocatoria para una posición de profesionales para gestión de cámaras, actividad que fue cubierta con la entrega de su hoja de vida, a finales de abril del mismo año; fue citado a una entrevista de trabajo, para explicarle, las características del puesto (Locador de Servicios), sueldo mensual y horario en la municipalidad, hacia el 02 de mayo del 2023, el autor asumió el cargo de supervisor técnico en la Central de Control y Video Vigilancia, una instalación crítica, operativa desde 2014, que pertenece a la municipalidad de Santa Anita. Antes de ingresar a la Central de Control y Video Vigilancia.

A partir de julio del 2024, aún en el puesto de supervisor y durante uno de los turnos, se hizo evidente un conflicto crítico de infraestructura con la red de datos, motivado por la inestabilidad recurrente en las conexiones a la red de datos. El diagnóstico inicial, realizado en colaboración con el encargado del área tecnológica, con el cual se identificó la causa raíz: un esquema de direccionamiento IP obsoleto y desorganizado. La red operaba bajo un único dominio de broadcast extendido (presumiblemente una única subred grande, Ej.: 172.20.10.88/24), sin implementar segmentación lógica (VLANs), por lo que se tuvieron cambiar los 13 puntos de IP’s que pertenecían a las estaciones de la Central de Control. Esta deficiencia generaba: Conflictos de direcciones IP (duplicidad esporádica); Tráfico excesivo de broadcast, lo que degradaba el rendimiento general; Dificultad en la localización y

diagnóstico de fallas (troubleshooting); Inestabilidad en los teléfonos IP y en los sistemas de videovigilancia de las estaciones de supervisión y operadores.

El objetivo general de esta TSP fue rediseñar las IP's de la red de datos en la Central de Control y Video Vigilancia de la Municipalidad de Santa Anita, Lima en 2024. Se tuvo que diseñar un nuevo esquema de direccionamiento lógico y se inició un proceso de mapeo detallado para identificar los hosts con mayores conflictos y los cuellos de botella.

Los objetivos específicos fueron: Diagnosticar el estado actual del direccionamiento IP y la infraestructura de red de la Central de Control y Videovigilancia; Ordenar de manera lógica las direcciones IP en subredes dedicadas (VLANs), y Medir el impacto del rediseño de la red en la capacidad de operatividad de la central de control y video vigilancia.

En base a los objetivos a lograr se elaboró una propuesta de rediseño, en el cual se planteaba buscar una IP que aún mantuviera conexión y de esa forma continuar la sucesión para asignar las demás estaciones. Esta propuesta, fue consultada al encargado del área tecnológica para que diera su aprobación y aplicarlo bajo su supervisión.

Luego de aprobada la propuesta por las autoridades superiores, se procedió con la ejecución de la propuesta, iniciándose con la resignación de direcciones IP y a la configuración de las interfaces de red (en switches L3) para aplicar la segmentación por VLANs, aislando el tráfico crítico de video y voz (IP) del tráfico de datos general. Además, hubo una implementación adicional: Se instaló y configuró un router/gateway en el primer piso (área administrativa) para proporcionarle una conexión estable, para lo que fue necesario crear una subred diferente (VLAN administrativa) para evitar que su tráfico afecte las operaciones críticas de monitoreo.

La Municipalidad de Santa Anita fue creada el 25 de octubre de 1989 mediante la Ley N° 25116, durante el primer gobierno de Alan García y su primer alcalde fue Carlos Alberto Moreyra García-Sayán que conforma Lima Este. Se caracteriza por ser un eje logístico y comercial de la capital. Se encuentra en la zona centro-este de Lima Metropolitana. Sus límites son por el norte con el distrito de El Agustino y Ate; por el sur con Ate; por el este con Ate y por el oeste con El Agustino.

El actual alcalde de Santa Anita es el Lic. Olimpio Alegría Calderón, asimismo cuenta con el Concejo Municipal, el cual está compuesto por 11 regidores, quienes actúan como el órgano normativo y fiscalizador.

La misión de la Municipalidad de Santa Anita es "Promover la prestación de servicios públicos, el desarrollo integral, sostenible y armónico del distrito, de manera eficiente y transparente, mejorando la calidad de vida de sus vecinos." (Municipalidad Distrital de Santa Anita, 2024). Asimismo, busca "Ser un distrito moderno, seguro, con un desarrollo económico sólido y una gestión transparente, donde los ciudadanos convivan en un entorno saludable y ordenado." (Municipalidad Distrital de Santa Anita, 2024)

Sus valores institucionales son: Transparencia: Gestión clara de los recursos; Vocación de Servicio: Orientación constante hacia el vecino; Integridad: Actuar bajo principios éticos; Responsabilidad: Compromiso con el desarrollo local.

La municipalidad ofrece servicios críticos como lo son: Seguridad Ciudadana (Serenazgo): Gestión del Centro de Video Vigilancia (donde se centra tu proyecto); Gestión Ambiental: Limpieza pública y mantenimiento de parques; Desarrollo Económico: Licencias de funcionamiento y fiscalización comercial; Servicios Sociales: Registro Civil (RENIEC),

OMAPED, DEMUNA y CIAM; Administración Tributaria: Recaudación de arbitrios e impuestos.

La Municipalidad de Santa Anita cuenta con una fuerza laboral diversa distribuida en varios regímenes laborales, lo que influye en la cantidad de usuarios que se conectan a la red: Regímenes Laborales como lo son D.L. 276 (Carrera Administrativa), D.L. 728 (Régimen Privado, mayormente obreros), y D.L. 1057 (CAS). Esta distribución supera los 1,000 trabajadores entre personal administrativo (que usa la red de datos interna) y personal operativo (serenos y operarios de limpieza).

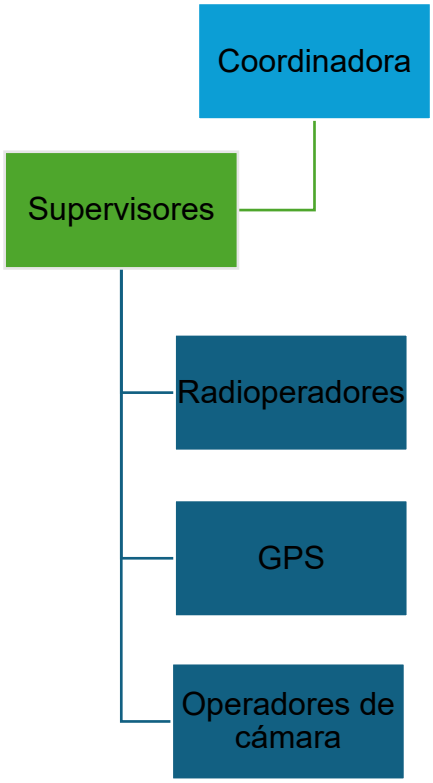
Respecto a la digitalización del distrito, la gestión actual busca migrar hacia el Gobierno Digital, lo que aumenta la carga de datos en los servidores y la necesidad de una infraestructura de red sólida para soportar sistemas de trámite documentario y monitoreo.

Figura 1

Municipalidad de Santa Anita

Figura SEQ Figura * ARABIC 2

Organigrama de la Central



CAPÍTULO II. MARCO TEÓRICO

A manera de introducción del Trabajo de Suficiencia Profesional se presentan los antecedentes y evolución de los servicios de videovigilancia en el mundo, desde sus orígenes en la década de 1940, cuando Siemens AG desarrolló un sistema de cámaras para monitorear lanzamientos de cohetes durante la Segunda Guerra Mundial, que funcionaban con tecnología analógica y conexiones cableadas (Plataforma virtual Otec Uno, s/f). En las décadas siguientes, especialmente a partir de los años 90, la tecnología avanzó hacia los sistemas digitales y el uso de cámaras IP, que permiten la conexión a redes digitales facilitando el monitoreo remoto y la integración con otros sistemas de seguridad (Intelion / ISID, 2024).

A nivel municipal en Perú, varios gobiernos han adoptado sistemas de videovigilancia IP para mejorar la seguridad ciudadana, considerando la flexibilidad, escalabilidad y eficiencia que ofrecen estos sistemas(CONICET, 2025). En ciudades latinoamericanas, por ejemplo, los municipios han implementado centralizadas redes inteligentes de videovigilancia para el monitoreo en tiempo real y la gestión integrada de datos (Universidad Militar Nueva Granada, 2022). En Perú, la implementación de sistemas de videovigilancia IP en municipios ha sido una herramienta clave para la prevención del crimen, optimizando recursos mediante la conectividad IP (SupraBT, 2025)

El rediseño de las IP’s en un sistema de vigilancia no solo mejora la eficiencia técnica como el ancho de banda y la estabilidad de la conexión- sino que también permite una mejor gestión de la seguridad informática, reduciendo vulnerabilidades ante ciberataques y facilitando la integración con nuevas tecnologías tales como inteligencia artificial para reconocimiento facial y detección de incidentes (Servicio de Alarmas, 2025).

El rediseño de las direcciones IP (Protocolo de Internet) en una Central de Video Vigilancia es un proceso crucial para optimizar la gestión, la seguridad y la eficiencia de los sistemas de vigilancia digital. La tecnología de videovigilancia IP permite la conexión de cámaras digitales a redes IP, facilitando el monitoreo remoto, la integración con otros dispositivos de seguridad (como sistemas de alarma y control de acceso) y el uso de software avanzado para análisis de imágenes, lo que mejora la capacidad de prevención y respuesta en entornos urbanos (Suprabt, 2025). Sin embargo, esta tecnología también implica desafíos como la necesidad de un ancho de banda adecuado y la estabilidad de la red para asegurar una transmisión fluida y de calidad de las imágenes (SupraBT, 2025).

En el ámbito universitario de Ingeniería de Sistemas, la innovación educativa implica abordar estos sistemas con un enfoque interdisciplinario que combina conocimientos en redes, seguridad informática y análisis de datos. La actualización o rediseño de las IP’s en un sistema de vigilancia municipal debe considerarse desde el punto de vista técnico y organizativo, asegurando que la red sea robusta, escalable y segura para minimizar vulnerabilidades y mejorar el rendimiento del sistema (Mendoza & Angel, s/f).

Los antecedentes revelan implementaciones similares en Perú y Latinoamérica, como sistemas interconectados con la Policía Nacional del Perú (PNP) desde 2018, que exigen protocolos estandarizados para videovigilancia municipal. En ciudades como Santiago, la adopción de IP desde 2000 mejoró la cobertura urbana, pero destacó limitaciones en privacidad y escalabilidad. Estudios peruanos en repositorios universitarios confirman que rediseños IP elevan la eficiencia en un 30-50%, integrando IA para detección de anomalías.

Las bases teóricas que respaldan el rediseño de direcciones IP en sistemas de videovigilancia están asociadas al direccionamiento IP, la gestión de redes, la seguridad informática y la innovación tecnológica en vigilancia digital.

Primero se debe mencionar que es una IP o mejor conocida como Internet Protocol Address, es un identificador numérico único de 32/128 bits que permite enrutamiento y comunicación entre dispositivos en redes TCP/IP, esencial en videovigilancia para asignar cámaras, NVR y servidores PNP en subredes segmentadas, usando IPv4 (192.168.x.x) o IPv6 para escalabilidad masiva(SupraBT, 2025). En sistemas municipales como Santa Anita, IPs estáticas garantizan conectividad permanente de cámaras fijas (ej. 192.168.10.50), mientras reservas DHCP evitan conflictos en dispositivos dinámicos, optimizando ancho de banda mediante máscaras /24 (255.255.255.0) para 254 hosts por subred(RedesZone, 2024).

Una base teórica relacionado al concepto principal sería el direccionamiento IP el cual es fundamental para organizar y gestionar los dispositivos en una red de videovigilancia. En sistemas de cámaras IP y grabadoras (NVR/VMS), la asignación de direcciones IP estáticas o dinámicas mediante DHCP permite controlar y optimizar el flujo de datos, evitando conflictos de direcciones y ampliando la cantidad de dispositivos mediante máscaras de subred apropiadas (Tecnoseguro, 2023). La gestión de subredes y puertas de enlace es vital para mantener la estabilidad y escalabilidad de la red, especialmente en instalaciones masivas en entornos urbanos (Tecnoseguro, 2023).

También se destaca la base teórica del problema, el cual es el conflicto de IP que ocurre cuando dos o más dispositivos en la misma subred asignan direcciones IP duplicadas, generando interrupciones en la conectividad, pérdida de paquetes y fallos en el streaming de cámaras IP, crítico en sistemas municipales donde IPs estáticas mal configuradas pueden

desconectar NVR de múltiples cámaras simultáneamente(RedesZone, 2024). En videovigilancia IP, conflictos se detectan mediante logs ARP ("Duplicate IP address") o comandos arp -a, resueltos asignando rangos exclusivos por VLAN (ej. 192.168.10.x para cámaras, 192.168.20.x para NVR) y configurando reservas DHCP para evitar colisiones automáticas(Tecnoseguro, 2023).

Otro concepto para usar es el comando ping o también conocido como Packet Internet Groper, este es una herramienta fundamental de diagnóstico de red basada en ICMP Echo Request/Reply qué mide latencia (RTT), pérdida de paquetes y conectividad entre dispositivos IP, esencial para verificar disponibilidad de cámaras y NVR en sistemas municipales antes y después de rediseños IP (Kurose, 2020). En videovigilancia IP, ping serial identifica bottlenecks en switches/routers mediante pruebas iterativas (ping -t, ping -l tamaño), optimizando MTU y QoS para streaming RTP/RTSP continuo, con umbrales <50ms críticos para monitoreo en tiempo real (Comer, 2021)

Otra base teórica que se puede destacar es la conectividad en redes IP que se define como la capacidad de dispositivos (cámaras, NVR, servidores PNP) para intercambiar datos continuamente mediante protocolos TCP/UDP confiables, midiendo métricas como latencia (<50ms), jitter (<30ms) y pérdida de paquetes (<1%) críticas para streaming RTP/RTSP sin interrupciones en monitoreo urbano (Intelion, 2025) . En sistemas municipales, la conectividad PoE+ (Power over Ethernet) integra alimentación y datos en cables Cat6, soportando cámaras 4K a 100m con switches managed que aplican QoS para priorizar video sobre tráfico administrativo, esencial post-rediseño IP en Santa Anita (Ajax Systems, 2025).

También se debe mencionar a las redes de datos modernas en la rama de videovigilancia IP se basan en arquitecturas definidas por software (SDN) que permiten

control centralizado del tráfico, optimizando QoS para streams de video en tiempo real y reduciendo latencia mediante segmentación dinámica de flujos (Peterson, 2021).

La convergencia 5G/Wi-Fi 6 en redes municipales habilita edge computing para procesamiento distribuido de datos de cámaras IP, incrementando throughput hasta 10 Gbps y soportando miles de dispositivos simultáneos sin congestión (Gupta, 2023).

Otra base, serían los dispositivos de conexión, como routers y bridges, que buscan facilitar la interconexión entre redes locales (LAN) y amplias (WAN), enrutando paquetes IP mediante tablas de rutas para evitar congestión en sistemas de videovigilancia con múltiples cámaras (CCNA desde Cero, 2025). En videovigilancia IP, los routers dividen subredes y establecen puertas de enlace seguras hacia la PNP, alineados con RM 485-2018-MININTER, reduciendo colisiones en un 50% (Redes IT SB, 2022).

Una base teórica importante seria la máscara de subred 255.255.255.0 (/24 en notación CIDR) el cual, es un filtro binario (11111111.11111111.11111111.00000000) que separa en una dirección IP la porción de red fija (primeros 24 bits) de la porción de host variable (últimos 8 bits), permitiendo 256 direcciones (254 utilizables) por subred en sistemas municipales como Santa Anita (Microsoft, 2025). En rediseño IP de videovigilancia, 255.255.255.0 segmenta cámaras (192.168.10.0/24) de NVR/PNP (192.168.20.0/24), evitando broadcasts excesivos y optimizando enrutamiento ARP, con operación AND lógico que determina si destinos son locales o requieren Gateway (Jeffry Chaves, 2025).

También se debe mencionar el nombre de dominio, el cual es una cadena de texto legible por humanos (ej. pnp.gob.pe, santa-anita.gob.pe) que representa jerárquicamente una dirección IP mediante el Sistema de Nombres de Dominio (DNS), estructurado como subdominio.dominio.tld (TLD = Top Level Domain), facilitando acceso remoto a servidores

VMS/NVR municipales sin memorizar IPs numéricas (Cloudflare, 2024).

En el caso del rediseño IP Santa Anita, nombres como vms.santa-anita.gob.pe resuelven a 192.168.20.10 (NVR principal) vía DNS 8.8.8.8, permitiendo integración con portales PNP nacionales y alertas automáticas por email/SMS, con registros A (IPv4), CNAME (alias) y MX (correo) esenciales para operación continua (Kinsta, 2025).

Otra base teórica a mencionar son las direcciones IP numéricas son identificadores únicos de 32 bits en IPv4 expresados en notación decimal punteada, ej. (192.168.1.50), que permiten enrutamiento preciso de paquetes TCP/IP entre dispositivos de red sin requerir resolución DNS, fundamentales para configuraciones estáticas en cámaras IP y NVR municipales donde la estabilidad 24/7 es crítica (Hostinger, 2025). En el rediseño IP de Santa Anita, algunos ejemplos de direcciones numéricas estáticas segmentan tráfico: cámaras (192.168.10.0/24), servidores PNP (192.168.20.0/24), facilitando ping directo, SNMP monitoring y acceso VMS sin latencia DNS, con rangos clase privada RFC 1918 optimizados para 254 hosts por subred (Fortinet, 2024).

También se define al DNS 8.8.8.8 (Google Public DNS), el cual es un resolvedor DNS recursivo público que traduce nombres de dominio (ej. pnp.gob.pe) a direcciones IP mediante consultas jerárquicas (root → TLD → autoritativo), con caché global anycast que reduce latencia <20ms, ideal como DNS secundario en NVR municipales para acceso remoto estable a servidores PNP post-rediseño IP (Captain DNS, 2025). En videovigilancia Santa Anita, configurar 8.8.8.8 / 8.8.4.4 como DNS primario/secundario evita fallos por DNS ISP lento, soporta DoH/DoT para cifrar consultas y acelera resolución

de dominios dinámicos en aplicaciones VMS, manteniendo conectividad 24/7(RedesZone, 2025).

Una base teórica que va relacionada con la anterior sería la de Google Public DNS (8.8.8.8 / 8.8.4.4), es un servicio de resolución DNS recursivo gratuito y de alta disponibilidad que utiliza red Anycast global para consultas <20ms, resolviendo dominios como pnp.gob.pe a IPs mediante jerarquía root -TLD- autoritativa con soporte DNS-over-HTTPS (DoH) y DNS-over-TLS (DoT) para cifrar tráfico DNS en NVR municipales, evitando envenenamiento DNS y MITM (Google Developers, 2025). En Santa Anita, Google Public DNS como resolvedor secundario asegura acceso remoto estable a portales VMS/PNP cuando fallan DNS ISP locales, cacheando respuestas frecuentes (TTL) y soportando IPv6 para futura escalabilidad de 1000+ cámaras, con 99.99% uptime garantizado (Infobae, 2025).

También podemos hablar de los servidores de comunicaciones, o Network Video Recorders (NVR), que actúan como núcleos centrales que gestionan almacenamiento masivo, procesamiento en tiempo real y análisis de feeds IP de cámaras, soportando hasta 570 Mbps de grabación en setups municipales (Genetec, 2025a). Estos servidores integran software VMS para monitoreo remoto y alertas IA, garantizando disponibilidad bajo la tríada CIA (PCFIX, 2024).

Un dispositivo del cual podemos hablar y que incluso forma parte de nuestro día a día es la red WiFi (Wireless Local Area Network - WLAN) es un sistema de comunicación inalámbrica basado en estándares IEEE 802.11 que utiliza ondas de radio en bandas 2.4/5/6 GHz para interconectar dispositivos electrónicos (cámaras IP, laptops, smartphones) en un área limitada (100m interior), formando una WLAN mediante Access Points (AP) que emiten balizas SSID con metadatos de seguridad WPA3 y capacidades(Proofpoint, 2023). En

videovigilancia municipal, redes WiFi segmentadas (VLAN 10: cámaras, VLAN 20: admin) soportan roaming 802.11r entre múltiples AP, entregando throughput 1.2 Gbps (WiFi 6) para streaming 4K simultáneo sin cables, con canales DFS (5GHz) que evitan interferencias urbanas peruanas (Telefónica, 2025).

Otro instrumento importante del que podemos hablar es de los switches de red los cuales conectan múltiples cámaras CCTV a un NVR mediante puertos PoE, gestionando tráfico VLAN con QoS para priorizar video crítico y soportar altas velocidades (hasta Gigabit) en instalaciones con docenas de dispositivos (TodoElectrónica, 2025). En Santa Anita, switches managed evitan broadcasts innecesarios, elevando eficiencia en un 40% vía segmentación IP (Hikvision, 2025).

También se debe mencionar a las redes de comunicación, los cuales son sistemas interconectados de dispositivos (cámaras IP, NVR, switches, routers) que intercambian datos mediante protocolos TCP/IP estandarizados, clasificadas por alcance en LAN (Local Area Network, <1km), MAN (Metropolitan, ciudad) y WAN (Wide Area, nacional), optimizando throughput, latencia y fiabilidad para streaming continuo en entornos municipales (Universidad El Bosque, 2025). En Santa Anita, la red de comunicación híbrida combina LAN cableada PoE (Gigabit Ethernet) para cámaras fijas con WLAN WiFi 6 para cobertura periférica, interconectada vía MAN municipal a servidores PNP nacionales mediante fibra óptica 10 Gbps, soportando 500+ cámaras con QoS priorizado para video RTP/RTSP (UAM Iztapalapa, 2023).

Otra base que mencionar es el ancho de banda se define como la capacidad máxima teórica de una conexión de red para transmitir datos en ambas direcciones, medida en bits por segundo (bps, Mbps, Gbps), representando el "tamaño de la tubería" que determina cuánta

información puede fluir simultáneamente sin congestión (Paessler, 2023). Sus características principales son :Medición: bps (10^9), Mbps (10^6), Gbps (10^9); distingue capacidad máxima vs throughput real; Factores limitantes: Latencia, jitter, pérdida paquetes, overhead protocolos (TCP/IP 20-40%); Requisitos videovigilancia: Cámara 4K H.265 = 8-15 Mbps; 100 cámaras = 1-1.5 Gbps mínimo; Optimización: QoS prioriza RTP/RTSP sobre HTTP; compresión H.265 reduce 50% vs H.264 (RedesTelecom, 2024).

Otro concepto para tener en cuenta sería el de los hacks de comunicaciones, como ataques Man-in-the-Middle (MITM) o exploits en protocolos RTSP débiles, comprometen integridad de streams IP interceptando paquetes no cifrados, comunes en videovigilancia expuesta (Scribd, 2025). La mitigación de hacks de comunicaciones en videovigilancia IP se basa en esquemas de autenticación segura y mutua, donde tanto el cliente como el servidor validan sus identidades antes de intercambiar datos, combinando cifrado simétrico fuerte como AES con protocolos de autenticación robustos para impedir ataques Man-in-the-Middle y suplantación de dispositivos en redes IP expuestas(International Organization for Standardization, 2022b).

Una herramienta para tener una comunicación con los dispositivos de redes de datos son los cables Ethernet son cables de par trenzado de cobre (UTP/STP) clasificados por categorías (Cat5e, Cat6, Cat6a, Cat7, Cat8) que transmiten señales eléctricas digitales según estándares TIA/EIA-568, soportando velocidades de 100 Mbps (Cat5e) hasta 40 Gbps (Cat8) con blindaje contra diafonía (NEXT) e interferencias EMI, esenciales para conexiones PoE+ en cámaras IP municipales (Telefónica, 2023). Sus características técnicas principales: Cat5e: 1 Gbps, 100 MHz, 100m, PoE básico (15.4W); Cat6: 10 Gbps (55m), 250 MHz,

100m@1Gbps, PoE+ (30W); Cat6a: 10 Gbps (100m), 500 MHz, blindaje S/FTP, PoE++ (90W); Construcción: 4 pares trenzados AWG 23-24, conectores RJ45 T568B ; Videovigilancia: Cat6a soporta 4K H.265 + PoE para cámaras PTZ (The Network Installers, 2025).

Otra base que se puede mencionar, es la de Videovigilancia, que como Servicio (VSaaS) es un modelo de gestión de seguridad basado en la computación en la nube, que permite el almacenamiento, procesamiento y monitoreo de video de forma remota a través de internet. A diferencia de los sistemas tradicionales que dependen de grabadores locales (NVR o DVR), la VSaaS traslada la inteligencia y el almacenamiento a servidores centralizados del proveedor. Según (Bosch, 2024), este paradigma permite a las organizaciones reducir los gastos de capital (CapEx) al eliminar la necesidad de infraestructura física compleja en el sitio, permitiendo que las cámaras IP sean el único hardware necesario para la transmisión directa a la nube. Asimismo, la VSaaS se caracteriza por su alta escalabilidad y la integración de Inteligencia Artificial (IA) tanto en el borde como en la nube, lo que facilita la detección automática de patrones de comportamiento y la gestión de alertas en tiempo real desde cualquier dispositivo móvil o web (Genetec, 2025b). Este modelo es fundamental para ciudades inteligentes y centrales de videovigilancia modernas, ya que garantiza la continuidad del servicio y la actualización constante de protocolos de ciberseguridad sin intervención manual del usuario.

Con relación a la regulación, en Perú el Decreto Legislativo N° 1218 y el Reglamento aprobado por Decreto Supremo regulan el uso de cámaras de videovigilancia públicas y privadas, estipulando estándares técnicos como la nitidez de imágenes, la conectividad continua vía IP, y la interoperabilidad con plataformas nacionales de seguridad(Decreto

Supremo N° 007-2020-IN, 2020). Además, las leyes de protección de datos aseguran la privacidad y el manejo adecuado de las imágenes captadas (Decreto Supremo N° 016-2024-JUS - Reglamento Ley 29733, 2024).

Estas bases evidencian que el rediseño de IPs en videovigilancia contribuye a la mejora técnica, operativa y normativa del sistema, facilitando una red estable, segura y conforme a estándares vigentes.

Algunos de los aspectos reglamentarios y normativos son: la RM 485-2018-MININTER exige interconexión con PNP y protocolos de videovigilancia estandarizados. Ley 29733 (Protección de Datos Personales) regula grabaciones, prohibiendo invasión de privacidad en espacios públicos; Profesionales (Ingeniería de Sistemas): Código de Ética del CIP (Colegio de Ingenieros del Perú) demanda auditorías de seguridad y cumplimiento normativo; ISO 27001 para gestión de riesgos en redes IP (Colegio de Ingenieros del Perú, 2018); Otros: Autorización municipal para cámaras en vías públicas; GDPR-like en Perú limita retención de videos a 30 días.

La norma ISO/IEC 27001 es el estándar internacional de referencia para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI). Su objetivo central es garantizar la confidencialidad, integridad y disponibilidad de los activos de información mediante la aplicación de un proceso de gestión de riesgos (International Organization for Standardization, 2022). En el contexto de infraestructuras críticas como las centrales de videovigilancia, este estándar permite establecer controles técnicos y organizativos que protegen la red de datos contra accesos no autorizados y fallos sistémicos. De acuerdo con (Alan Calder, 2022), la implementación de la ISO 27001 no se limita únicamente a soluciones tecnológicas, sino que promueve un enfoque

de gobernanza que alinea la seguridad de la información con los objetivos estratégicos de la organización. Al adoptar este marco, las entidades públicas pueden asegurar una respuesta resiliente ante incidentes cibernéticos, validando que el rediseño de las arquitecturas de red cumpla con estándares globales de protección y cumplimiento legal.

En el caso de las limitaciones que se tuvieron en el trabajo de suficiencia profesional serían: En la parte técnica sería el alto consumo de ancho de banda genera cuellos de botella; limitación de 100m en cables Ethernet requiere switches intermedios. Interferencias Wi-Fi por clima o inhibidores afectan señales inalámbricas.; En el caso de la escalabilidad sería el crecimiento de cámaras exige hardware costoso; VSaaS limita rendimiento por número de dispositivos; Con respecto a la ciberseguridad se consideró la vulnerabilidad a hacks por conexión IP; falsas alarmas en analíticas IA.; En la parte operativa la dependencia de NVR específicos complica software alternativo; costos de almacenamiento elevado.

CAPÍTULO III. DESCRIPCIÓN DE LA EXPERIENCIA

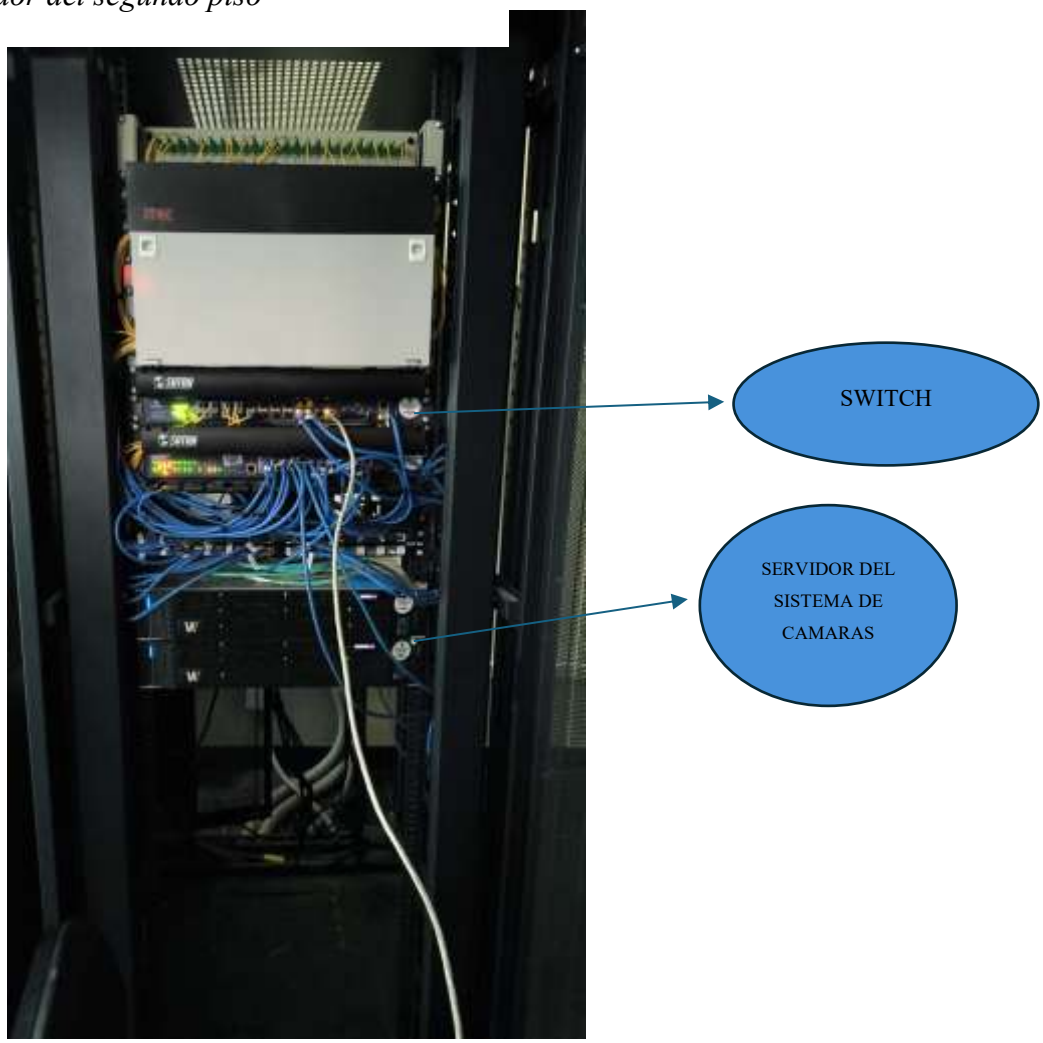
El presente trabajo de suficiencia profesional (TPS) se desarrolló en la Central de Control y Videovigilancia de la Municipalidad Distrital de Santa Anita, ubicada en el distrito de Santa Anita, Lima. Para la selección del puesto para laborar en la municipalidad mencionada, el autor del presente trabajo de suficiencia profesional se entrevistó primero con el gerente de Seguridad Ciudadana para conocer sus habilidades para el puesto, en este caso el de supervisor, por lo que el gerente dio el visto bueno para que pueda ir a entrevistarse con el subgerente de Seguridad Ciudadana de ese entonces, para que se de conformidad de que el autor del presente trabajo de suficiencia profesional pueda asumir el cargo, una vez dada la conformidad, el sub gerente llamó al encargado de la Central para que se acerque y lleven al autor del presente trabajo de suficiencia profesional para que conozca las instalaciones y cómo va a ser el trabajo a realizar. Una vez allá, se le explicó al autor del presente trabajo de suficiencia profesional como funcionaba el sistema de las cámaras, las redes de comunicaciones, como era la dinámica laboral, terminada la explicación, al autor le dijeron que regresen en dos días porque ahí ya empezaría sus labores de manera oficial.

Ya había pasado un año y el autor del presente trabajo de suficiencia profesional ya se encontraba laborando en la Central, sin embargo se empezaban a presentar problemas con la red de comunicación ya que comenzaba a desconectarse y volver a conectar de un momento a otro, por lo que al inicio el encargado del área tecnológica hace un diagnóstico de la red y encuentra dos alternativas, puede ser un conflicto de IP y otra alternativa podría ser con el proveedor de internet, por lo cual se gestionó las dos opciones. Por lo que se tenía como objetivo el rediseñar las IP’s de la Central de Video Vigilancia de la Municipalidad

de Santa Anita, Lima en 2024. La función principal del autor consistió en verificar y corregir la configuración de direcciones IP de las estaciones de trabajo, con el fin de restablecer la conectividad general del sistema de videovigilancia. El proceso se desarrolló de manera secuencial y metodológica, el tiempo de realización para realizar el proyecto en mención fue de menos de una (01) semana. Lo que se realizó fue un cambio de IP's en la Central para que estén separadas la de cámaras y la de red de comunicaciones, debido a que se encontraban generando conflicto y evitaba un buen desempeño, por lo que el encargado del área tecnológica gestiono el cambio de empresa proveedora de red de comunicaciones con el área de sistemas de la municipalidad.

Figura 3

Servidor del segundo piso

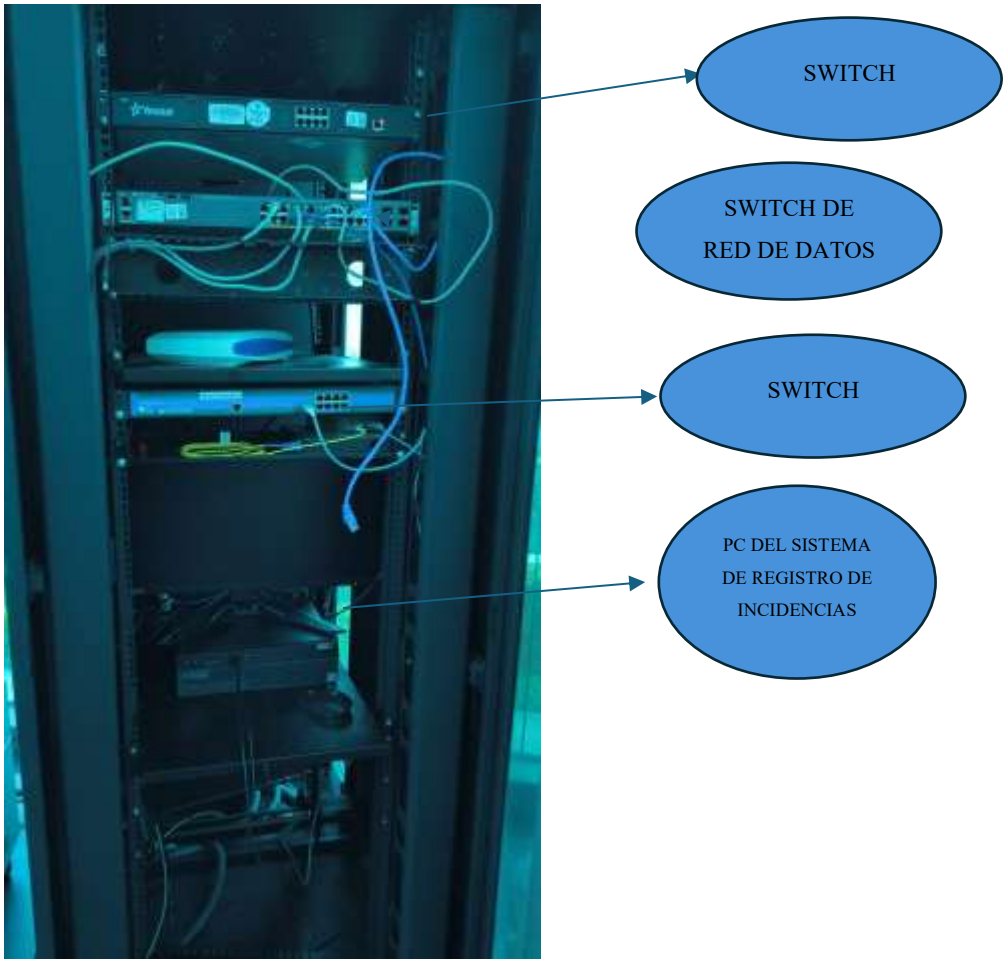


En paralelo, y con el apoyo del autor del presente trabajo de suficiencia profesional, se procedió a verificar una por una, las estaciones (computadoras) que en total son 13 del segundo piso y 5 del primer piso, para esto se procedió a comprobar la conectividad mediante el comando ping a cada una de las IP's, asimismo se comprobó que durante la ejecución del comando ping no contaban con máscaras de sub red, una vez hecho eso, se llegó a la conclusión que ninguna de las IP's estaba dando conectividad, hasta que llegamos

a la estación de supervisor (172.20.40.260), la cual no tuvo ningún problema y seguía conectada a la red con el servidor de cámaras activo.

Figura 4

Servidor del 1er piso



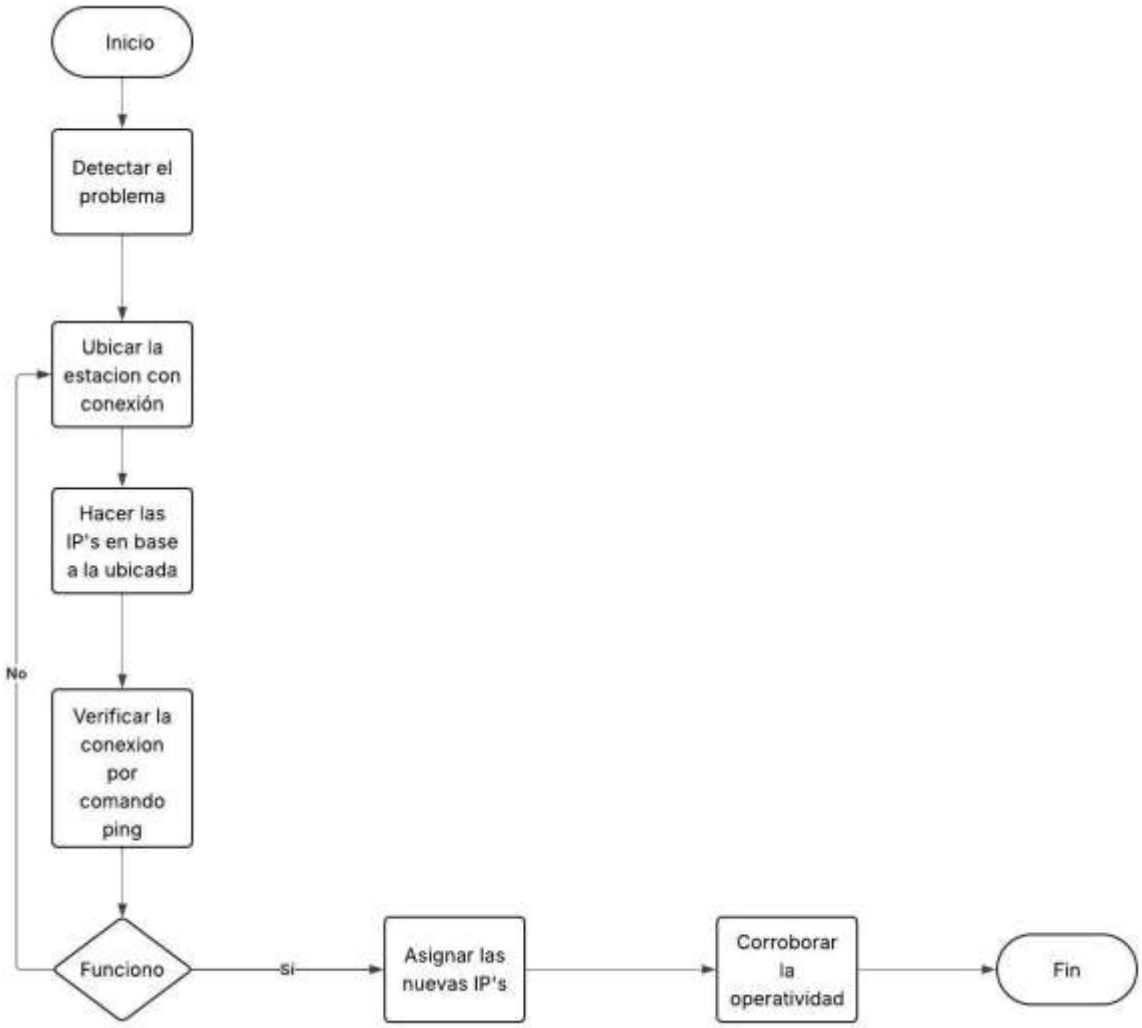
Por lo cual, al encontrar una IP con conectividad exitosa, se hizo una continuación, previa prueba con el comando ping, para que las IP's no presenten ningún problema, verificadas las IP's se procedió a colocar cada una de ellas en las estaciones con su respectiva mascara de subred (255.255.255.0), principalmente porque es la más universal y

ofrece un balance simple entre el número de dispositivos y la facilidad de administración, también el DNS (8.8.8.8), porque es una de las direcciones de los servidores públicos de Google Public DNS, además de que es fundamental porque traduce los nombres de dominio que escribimos (como google.com) a las direcciones IP numéricas que las computadoras realmente usan para comunicarse. Al haber establecido tanto la máscara de subred y el DNS, empezó a haber conexión en la red, aparte el encargado del área tecnológica creo una nueva IP que solamente se encarga del servidor de cámaras, separándolo de la IP de redes de comunicación (172.20.40.10), además se dejó una red Wifi externa para que en caso de caídas de la red de comunicaciones principales. Finalmente se implementó en el primer piso un router para que tenga conexión a la nueva red, así como el acceso al sistema de cámaras.

Los pasos que se siguieron durante el desarrollo de este rediseño serían los siguientes:

Figura 5

Diagrama de flujo sobre el rediseño de las IP'S



Nota: El diagrama de flujo representa el proceso del rediseño de las IP'S de la red de datos en la central de control y video vigilancia

Las funciones que se desempeñaron fueron la detección del conflicto de IP, la eliminación de tráfico con la nueva asignación de IP's, la implementación de una red de comunicaciones inalámbrica (Wifi) de emergencia, en caso de que la principal presente algún

problema, implementación del router del primer piso para el área administrativa, así como de las demás estaciones del proyecto módulo 2, en el cual se contempla el funcionamiento del primer piso para asignación de operadores de cámaras y sala de reuniones entre el gerente de seguridad ciudadana y la policía nacional del Perú (PNP).

CAPÍTULO IV. RESULTADOS

Objetivo General: Rediseñar las IP’s de la red de datos de la central de control y video vigilancia de la Municipalidad de Santa Anita, Lima.

Resultado: Se cumplió de manera exitosa, suprimiendo los conflictos de IP’s y las caídas frecuentes de conectividad que afectaban tanto a la red de datos.

Objetivo Especifico: Diagnosticar el estado actual del direccionamiento IP y la infraestructura de red de la Central de Control y Videovigilancia.

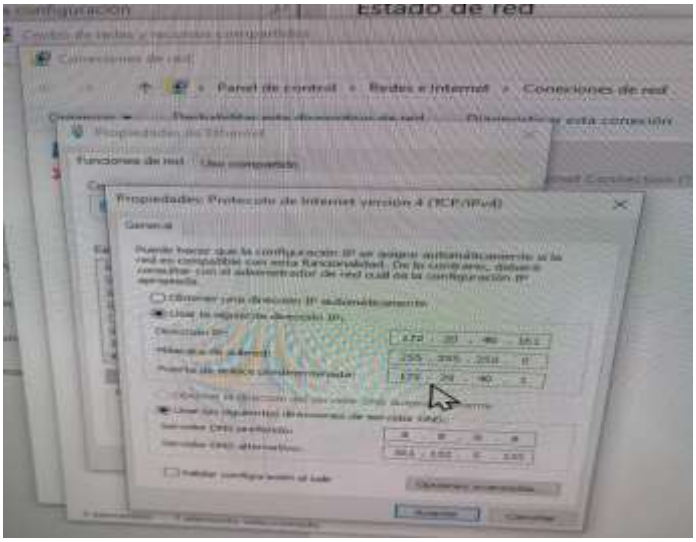
Resultado: Se procedió a verificar cual es el problema con la red de datos y porque los constantes fallos de conexión, así como el tráfico de red y si se presentaban cuellos de botellas o duplicidad de IP’s.

Objetivo Especifico: Ordenar de manera lógica las direcciones IP en subredes dedicadas (VLANs).

Resultado: Se procedió a verificar estación por estación para verificar si alguna de las IP’s presentaba conexión a la red de datos, se comprobó por medio de comando ping, para verificar si había caída de paquetes o no, siendo la estación de supervisor la que no presentaba ninguna caída de paquetes durante la ejecución del comando ping.

Figura 6

Dirección IP actual



Nota: Dirección IP actual de una de las estaciones de operadores de cámaras

Objetivo Específico: Medir el impacto del rediseño de la red en la capacidad de operatividad de la central de control y video vigilancia.

Resultado: Se logró eliminar los conflictos de IP, dando un mayor orden y fluidez para las conexiones a las estaciones, así como la oportunidad de separar la red de datos tanto de las estaciones dedicadas a la parte operativa (estaciones de operadores de cámaras, radio, GPS, redes) y la parte administrativa.

Tabla 1

Asignación de las IP's

Estación	IP asignada
1	172.20.40.161
2	172.20.40.162
3	172.20.40.163
4	172.20.40.164
5	172.20.40.165
6	172.20.40.166
7	172.20.40.167
8	172.20.40.168
9	172.20.40.169
10	172.20.40.170
Radio	172.20.40.171
GPS	172.20.40.172
Redes Sociales	172.20.40.173

Nota: Elaboración propia. Direcciones IP'S asignadas a las estaciones en mención en base a la dirección IP de la estación de supervisor (172.20.40.160)

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Objetivo General: Rediseñar las IP's de la red de datos de la central de control y video vigilancia de la Municipalidad de Santa Anita, Lima.

Conclusión: Se logró rediseñar con éxito el esquema de direccionamiento IP de la Central de Control y Videovigilancia de Santa Anita, cumpliendo el objetivo principal al eliminar definitivamente los conflictos de duplicidad y las caídas frecuentes de conectividad que afectaban la red.

Objetivo Específico: Ordenar de manera lógica las direcciones IP en subredes dedicadas (VLANs).

Conclusión: luego de establecer el orden lógico de los IP's, se dió la segmentación eficiente del tráfico de red, en la Central de Control. Logrando aislar de manera estricta el flujo masivo de datos de las cámaras de videovigilancia respecto a los servicios de radio, GPS y administración, eliminando así, la saturación por tráfico de broadcast y reduciendo la latencia en la transmisión.

Objetivo Específico: Diseñar un nuevo esquema de direccionamiento lógico para optimizar el uso de los recursos de red.

Conclusión: Se concluyó que el diseño del nuevo esquema de direccionamiento lógico permitió la optimización integral de los recursos de red mediante la elaboración de una propuesta técnica basada en la metodología VLSM (Máscara de Subred de Longitud Variable), logrando un uso eficiente del espacio de direcciones. Además, a través del comando ping se logro ver con cual IP iba a ser la base para el rediseño.

Objetivo Específico: Medir el impacto del rediseño de la red en la capacidad de operatividad de la central de control y video vigilancia.

Conclusión: Se concluye que el rediseño tuvo un impacto positivo (a través de encuestas verbales con el personal usuario involucrado directamente en la validación del tráfico de red) con respecto a la parte operativa de la Central de Control y Videovigilancia, y principalmente por garantizar una mejor fluidez en la red de datos, para el monitoreo en tiempo real, así como la eliminación de conflictos de direcciones IP y caídas frecuentes de conectividad.

Lecciones aprendidas

1. Aprender a usar comandos de red en los equipos de la red, ej. comando ping
2. Usos de la segmentación lógica
3. Conectividad con un servidor
4. La implementación de VSML (Máscara de Subred de Longitud Variable)

Recomendaciones

Para futuros rediseños de red en infraestructuras similares a las de la Municipalidad de Santa Anita, se recomienda:

1. Optimización del direccionamiento IP y VLSM esto principalmente por el uso de la máscara de subred /24 (255.255.255.0) es un buen punto de partida, pero la optimización con Variable Length Subnet Masking (VLSM) es necesaria para redes grandes. Además, se debería aplicar VLSM ya que al utilizar VLSM para calcular subredes de tamaño justo para cada área, evitando desperdicio de direcciones IP y limitando el tamaño de los dominios de broadcast.

2. Documentación rigurosa, para mantener un registro detallado y actualizado del nuevo esquema de direccionamiento IP para evitar conflictos (duplicidad esporádica) y facilitar el diagnóstico de fallas (troubleshooting).

3. Fortalecimiento de la ciberseguridad dado que la videovigilancia IP es vulnerable a *hacks* y ataques por conexión IP, es vital reforzar la seguridad de la red por lo que se recomiendan que deben configurar *Firewalls* y AES, además de implementar *firewalls* para segmentar y proteger las subredes, y utilizar cifrado (AES) para los *streams* IP críticos, también buscar una autenticación mutua esto con el fin de aplicar protocolos de autenticación robustos en los dispositivos de red (cámaras, NVRs, *switches*) conforme a los estándares de seguridad (ej. ISO 27001). También deberían realizar auditorías de seguridad con el fin de cumplimiento normativo.

4. Reemplazo preventivo del cableado deteriorado para evitar fallas operativas futuras y asegurar el cumplimiento de la limitación de 100m en cables Ethernet. Además de tener en cuenta la infraestructura *PoE* con el fin de asegurar que los *switches* de red sean *Power over Ethernet* (PoE) para alimentar directamente las cámaras CCTV, simplificando la infraestructura y la gestión.

Competencias Aplicadas

1. Dominio de redes, esto para poder entrar a la configuración en las estaciones y verificar desde las direcciones IP' asignadas hasta las máscaras de subred.
2. Conexión de cables de red, esto para verificar si los cables que se encontraban dañados presentaban fallas para poder conectar el puerto a la red de datos.

3. Trabajo en equipo, ya que se coordinó con el área tecnológica de la Central de Control y videovigilancia para el desempeño del proyecto y la evaluación de efectividad y conformidad.
4. Diagnóstico y Resolución de Problemas (Troubleshooting) principalmente para identificar los problemas críticos de infraestructura, como conflictos de IP y saturación de dominios de broadcast, utilizando herramientas de diagnóstico como el comando ping e ICMP.
5. Gestión de Proyectos de TI que es la capacidad para planificar y ejecutar un proyecto de manera secuencial y metodológica

REFERENCIAS

Ajax Systems. (2025). *¿Cuándo aparecieron las cámaras de seguridad? Un completo historial de videovigilancia*. https://ajax.systems/es/blog/when-did-security-cameras-come-out/.

Alan Calder. (2022). *ISO27001/ISO27002: A pocket guide* (3a ed.). IT Governance Publishing.

Bosch. (2024, febrero). *La video vigilancia como un servicio llega para crear nuevas formas de negocio*. https://www.bosch.com.pe/noticias-e-historias/noticias/la-video-vigilancia-como-un-servicio-llega-para-crear-nuevas-formas-de-negocio/.

Captain DNS. (2025, diciembre 7). *DNS 8.8.8.8 de Google: Ventajas, inconvenientes y alternativas*. https://www.captaindns.com/es/blog/dns-8888-google.

Cloudflare. (2024). *¿Qué es un nombre de dominio? | Dominio vs. URL*. https://www.cloudflare.com/es-es/learning/dns/glossary/what-is-a-domain-name/.

Colegio de Ingenieros del Perú. (2018). *Código de ética del Colegio de Ingenieros del Perú*.

Comer, D. E. (2021). *Computer networks and internets* (6th ed.). Pearson.

CONICET. (2025). *Ciudades, cámaras de seguridad y video-vigilancia: Estado actual y tendencias.* https://ri.conicet.gov.ar/bitstream/handle/11336/71428/.

Decreto Supremo N° 007-2020-IN, Pub. L. No. DL 1218 (2015), https://www.gob.pe/institucion/mininter/normas-legales/1081739-007-2020-in (2020).

Decreto Supremo N° 016-2024-JUS - Reglamento Ley 29733, Pub. L. No. Ley 29733, https://img.lpderecho.pe/wp-content/uploads/2025/05/Opion-Consultativa-20-2025-DGTAIPD-LpDerecho.pdf (2024).

Fortinet. (2024). *¿Qué es una dirección IP? ¿Cómo funciona?* https://www.fortinet.com/lat/resources/cyberglossary/what-is-ip-address.

Genetec. (2025a). *Servidor de videovigilancia y seguridad Streamvault | Genetec*. https://www.genetec.com/es/productos/seguridad-unificada/streamvault.

Genetec. (2025b). *Videovigilancia como servicio (VSaaS)*. https://www.genetec.com/es/productos/seguridad-unificada/vsaas.

Google Developers. (2025). *Public DNS | Google for Developers*. https://developers.google.com/speed/public-dns.

Gupta, R. ; T. S. ; T. S. ; K. N. (2023). Tactile internet and its applications in 5G networks: A comprehensive review. *IEEE Internet of Things Journal*, *10*(3).

Hikvision. (2025). *Network Switches – Hikvision*. https://www.hikvision.com/es-la/products/transmission/Network-Switches/.

Hostinger. (2025, diciembre 17). *Qué es una dirección IP: Definición, funcionamiento y tipos*. https://www.hostinger.com/es/tutoriales/que-es-una-direccion-ip.

Infobae. (2025, septiembre 24). *Glosario de tecnología: Qué significa Google Public DNS*. https://www.infobae.com/tecno/2025/09/24/glosario-de-tecnologia-que-significa-google-public-dns/.

Intelion. (2025, julio 8). *Tecnología para ciudades seguras: De la vigilancia a la IA*. https://intelion.isid.com/es/evolucion-de-la-tecnologia-para-ciudades-seguras-de-la-videovigilancia-a-las-ciudades-inteligentes/.

Intelion / ISID. (2024, septiembre 16). *Evolución de la tecnología para ciudades seguras: De la videovigilancia a las ciudades inteligentes*. https://intelion.isid.com/es/evolucion-de-la-tecnologia-para-ciudades-seguras-de-la-videovigilancia-a-las-ciudades-inteligentes/.

International Organization for Standardization. (2022a). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC Standard No. 27001:2022)*. https://www.iso.org/standard/27001.

International Organization for Standardization. (2022b). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems*

— *Requirements*.

Jeffry Chaves. (2025, octubre 5). *Máscara de subred: Guía práctica con tabla CIDR*. 2025.

Kinsta. (2025, septiembre 30). *¿Qué es DNS? Nombres de servidores explicados*. https://kinsta.com/es/blog/que-es-dns/.

Kurose, J. R. K. (2020). *Computer networking: A top-down approach* (8th ed.). Pearson.

Mendoza, F., & Angel, M. (s/f). *UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE FACULTAD DE INGENIERÍA ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS ESTUDIO Y DISEÑO PARA LA IMPLEMENTACIÓN DE SISTEMA DE SEGURIDAD CON CÁMARAS IP EN EL*.

Microsoft. (2025, enero 14). *Direccionamiento y subredes TCP/IP*. https://learn.microsoft.com/es-es/troubleshoot/windows-client/networking/tcpip-addressing-and-subnetting.

Municipalidad Distrital de Santa Anita. (2024). *Plan Estratégico Institucional (PEI) 2024-2027: Misión y Visión Institucional*.

Paessler. (2023). *¿Qué es el ancho de banda?* https://www.paessler.com/es/it-explained/bandwidth.

PCFIX. (2024). *Qué son los Servidores para cámaras de seguridad y en qué se utilizan en las empresas*. https://pcfix.cl/que-son-los-servidores-para-camaras-de-seguridad-y-en-que-se-utilizan-en-las-empresas/.

Peterson, L. L. ; D. B. S. (2021). *Computer networks: A systems approach* (Morgan Kaufmann, Ed.; 6a ed.).

Plataforma virtual Otec Uno. (s/f). *Historia y evolución de la videovigilancia. .* https://virtual.otecuno.cl/pluginfile.php/598/mod_resource/content/4/1.%20Historia%20y%20Evoluci%C3%B3n%20de%20la%20Videovigilan.

Proofpoint. (2023, diciembre 23). *¿Qué es el WiFi? Tipos de conexiones WiFi y seguridad*. https://www.proofpoint.com/es/threat-reference/wifi.

Redes IT SB. (2022, septiembre 6). *Dispositivos de conexión*. https://redesietsb.school.blog/dispositivos-de-conexion/.

RedesTelecom. (2024, diciembre 26). *Qué es la banda ancha: características, ventajas y más*. https://www.redestelecom.es/especiales/descubre-todo-sobre-la-banda-ancha-caracteristicas-y-ventajas/.

RedesZone. (2024). *Cómo montar sistema de videovigilancia IP*. https://www.redeszone.net/reportajes/tecnologias/montar-sistema-videovigilancia-ip/.

RedesZone. (2025, julio 9). *Qué es el protocolo DNS y por qué es tan importante*. //www.redeszone.net/tutoriales/internet/que-es-protocolo-dns/.

Scribd. (2025). *Ataques y contramedidas M8*.

Servicio de Alarmas. (2025, marzo 5). *Evolución de la videovigilancia: Cámaras inteligentes y alarmas*. https://serviciodealarmas.com/evolucion-de-la-videovigilancia-camaras-inteligentes-y-alarmas/.

SupraBT. (2025). *Videovigilancia IP: soluciones tecnológicas para tu seguridad*. https://www.suprabt.com/blog/videovigilancia-ip/.

Tecnoseguro. (2023, marzo 23). *Conceptos técnicos clave: Direccionamiento de red en videovigilancia*. https://www.tecnoseguro.com/tutoriales/pro/conceptos-tecnicos-clave-direccionamiento-red-videovigilancia.

Telefónica. (2023, junio 21). *Qué es Ethernet y qué tipos de cables existen*. https://www.telefonica.com/es/sala-comunicacion/blog/que-es-ethernet-tipos-cables/.

Telefónica. (2025, abril 7). *Qué es el WiFi*. https://www.telefonica.com/es/sala-comunicacion/blog/wifi-que-es/.

The Network Installers. (2025, septiembre 23). *Clasificación de cables Ethernet: Guía completa (2025)*. https://thenetworkinstallers.com/es/blog/clasificaciones-de-gatos-para-ethernet/.

UAM Iztapalapa. (2023, marzo 26). *Redes de Comunicaciones*.

https://pcyti.izt.uam.mx/?page_id=191.

Universidad El Bosque. (2025, marzo 31). *¿Qué son las redes y telecomunicaciones?* https://www.unbosque.edu.co/blog-universidad-el-bosque/que-son-las-redes-y-telecomunicaciones.

Universidad Militar Nueva Granada. (2022). *Sistemas de video vigilancia y su aporte a la evolución estratégica de ciudades*.