

CAPITULO I

INTRODUCCION

1.1 INTRODUCCION

La seguridad en espacios destinados al cuidado infantil, como guarderías o centros integrales, constituye un elemento esencial para proteger tanto a los menores como al personal responsable. En el ámbito universitario, estos espacios desempeñan un rol fundamental al brindar un entorno seguro para los hijos de los estudiantes, contribuyendo así a reducir la deserción académica asociada al cuidado infantil. No obstante, garantizar un monitoreo efectivo y continuo de todas las actividades que se desarrollan dentro del Centro Integral de Niños representa un desafío, especialmente al no contar con herramientas tecnológicas adecuadas.

Ante esta necesidad, la implementación de un sistema moderno de videovigilancia se plantea como una solución eficaz para fortalecer la seguridad, mejorar la supervisión y optimizar la capacidad de respuesta ante situaciones de riesgo que se pueda dar en el centro integral. En este contexto, el presente trabajo tiene como objetivo **diseñar un sistema integral de videovigilancia basado en cámaras IP y dispositivos de red**, orientado a cubrir las necesidades específicas del Centro Integral de Niños de la UAJMS.

La propuesta incluye la selección de cámaras IP, grabadores de video en red (NVR), switches PoE y un esquema de red optimizado que garantice la cobertura total de las áreas internas y externas del centro. Asimismo, se analizan las características técnicas de los dispositivos y componentes involucrados, tomando en cuenta conceptos fundamentales como videovigilancia digital, tipos de cámaras, almacenamiento de video, redes de datos y protocolos de comunicación.

La metodología utilizada responde a un enfoque aplicado y descriptivo. Por una parte, se realiza la recolección de requisitos del entorno, identificando las necesidades reales de seguridad del centro; y por otra, se efectúa un análisis técnico que permite definir las especificaciones necesarias para el diseño del sistema de videovigilancia.

Finalmente, es importante destacar que **el diseño planteado es escalable, flexible y plenamente compatible con la infraestructura tecnológica actualmente utilizada**

en el campus universitario, lo cual facilita su integración, expansión o adaptación a otras áreas de la UAJMS.

1.2 ANTECEDENTES

La implementación de sistemas de videovigilancia se ha convertido en una herramienta esencial para garantizar la protección y el bienestar de los niños, lo que subraya la importancia de un diseño confiable y estructurado que sirva como base para una futura implementación.

Este trabajo de investigación se centra en el diseño de un sistema de video vigilancia utilizando cámaras IP, que ofrecen ventajas significativas en términos de calidad de imagen y facilidad de integración con otros sistemas de seguridad.

Si bien la UAJMS cuenta con personal de seguridad el cual se encuentra repartido en todo el campus universitario, el centro Integral de niños se encuentra alejado al final del campus y la presencia del personal de seguridad no es constante en todas las áreas y horarios, generando puntos vulnerables y vacíos de seguridad que exponen a los niños. También es importante mencionar que las instalaciones del centro integral cuentan con algunas cámaras de vigilancia, solo 2 cámaras para toda la infraestructura. No son cámaras adecuadas para los espacios que tiene el centro ya que no cubren la totalidad de las áreas a vigilar. También existen área de cunas para los más pequeños, cursos de enseñanza y un patio para recreación de todos los niños en donde pueden suceder varios accidentes ya que los niños son traviesos e inquietos. Tanto el ingreso principal como el de la parte de atrás, no cuentan con vigilancia mediante cámaras esto ocasiona que no se vea quien entra ni quien sale por los ingresos. De ahí que se realiza este trabajo de investigación para mejorar la seguridad en el centro integral de la UAJMS.

1.3 PLANTEAMIENTO DEL PROBLEMA

El centro integral de niños de la UAJMS carece actualmente de un sistema de videovigilancia adecuado. Lo que impide una supervisión efectiva y compromete la

seguridad de los niños durante su permanencia en el establecimiento. Esta carencia genera varias preocupaciones:

Seguridad de los Niños: **La vulnerabilidad de los niños** ante posibles accidentes, emergencias o situaciones de riesgo, debido a la dificultad de monitorear todas las áreas en tiempo real.

Control y Supervisión: **La limitada supervisión y control** sobre las actividades de los niños y personal, lo que puede derivar en situaciones de indisciplina o manejo inadecuado de recursos y espacios.

Confianza de los Padres: Los padres confían en la guardería para el cuidado y protección de sus hijos. La falta de un sistema de video vigilancia **puede disminuir la confianza** de los padres en la institución, afectando su reputación y la inscripción de nuevos niños y provocando la deserción del alumnado.

Prevención de Incidentes: La **dificultad de prevenir y resolver incidentes** como extravío de objetos, conflictos entre niños o comportamientos inapropiados del personal, al carecer de un registro visual objetivo.

Asimismo, la creciente inseguridad externa en las inmediaciones de los centros infantiles, donde los niños son particularmente vulnerables, genera una preocupación latente por posibles intentos de secuestro, sin que exista un monitoreo adecuado que sirva como disuasión o fuente de evidencia.

➤ **Problema de Investigación**

¿Cómo diseñar un sistema de videovigilancia en el centro integral de niños de la Universidad Autónoma Juan Misael Saracho?

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Diseñar un sistema integral de videovigilancia sobre red IP para el Centro Integral de Niños de la UAJMS, *para mejorar la seguridad y supervisión de los menores, mediante la selección adecuada de tecnologías, dispositivos y arquitectura de videovigilancia compatibles con la infraestructura del campus universitario.*

1.4.2 OBJETIVOS ESPECIFICOS

1. Identificar las necesidades de vigilancia del Centro Integral y los estándares técnicos requeridos, para establecer los criterios funcionales y operativos del sistema, mediante la recolección y el análisis de requisitos del entorno.
2. Diseñar la infraestructura tecnológica del sistema de videovigilancia, para asegurar una cobertura óptima y un funcionamiento eficiente, mediante la definición de la ubicación estratégica de cámaras, los equipos necesarios y sus características técnicas.
3. Definir los requerimientos y la arquitectura del sistema de almacenamiento y grabación de video, para garantizar la seguridad, disponibilidad y escalabilidad del registro visual, mediante el dimensionamiento del NVR, cálculo de capacidad y diseño del esquema de red.
4. Seleccionar el software de monitoreo y gestión del sistema, para permitir la supervisión en tiempo real y la notificación oportuna de eventos relevantes, mediante la evaluación de plataformas compatibles con el sistema de videovigilancia y las necesidades del personal del centro.

1.5 JUSTIFICACION

La seguridad y el bienestar de los niños en centros integrales representan prioridades fundamentales tanto para los padres como para el personal responsable de su cuidado. Dado que los menores pasan una parte significativa de su jornada en estas instalaciones, resulta indispensable contar con mecanismos que garanticen su protección, supervisión continua y respuesta oportuna ante cualquier eventualidad.

La implementación de un sistema moderno de videovigilancia basado en cámaras IP y tecnologías actuales ofrece múltiples beneficios para el Centro Integral de Niños de la UAJMS. Entre ellos se destacan: el fortalecimiento de la seguridad infantil, el incremento de la confianza de los padres, la posibilidad de supervisar adecuadamente al personal, la prevención y resolución eficiente de incidentes, y la disuasión de posibles actos delictivos en las inmediaciones del establecimiento.

Asimismo, el diseño de este sistema responde a la necesidad institucional de adoptar soluciones tecnológicas compatibles con la infraestructura del campus universitario, permitiendo una futura integración o expansión hacia otras áreas que aún carecen de sistemas de seguridad. Desde una perspectiva académica y profesional, este proyecto contribuye al desarrollo de propuestas tecnológicas aplicadas a la protección de personas, constituyendo un aporte significativo para la carrera de Ingeniería de Sistemas.

En consecuencia, los beneficios mencionados justifican plenamente la realización del presente diseño de sistema de videovigilancia, orientado a mejorar las condiciones de seguridad del Centro Integral y a promover un entorno confiable y adecuado para el desarrollo infantil.

1.5.1 JUSTIFICACION ACADEMICA

Desde una perspectiva académica, la existencia de un Centro Integral de Niños con un sistema de videovigilancia confiable es crucial para el **continuidad y éxito de la formación universitaria** de los estudiantes. Al proporcionar un entorno seguro y supervisado para sus hijos, la universidad elimina una barrera significativa que a menudo obliga a muchos estudiantes a **interrumpir o abandonar sus estudios** debido a la falta de recursos económicos para costear guarderías particulares (Loera, 2020). Este proyecto, por tanto, contribuye directamente a la **retención estudiantil y al fomento de la permanencia académica**, asegurando que los futuros profesionales puedan concentrarse en su formación teórico-práctica sin la preocupación constante por el cuidado de sus hijos

1.5.2 JUSTIFICACION SOCIAL

El presente proyecto, beneficiara a toda la población universitaria que tengan hijos/as y necesiten un centro integral que este al cuidado de ellos, brindándoles más seguridad y resguardando la integridad física de los niños y niñas

1.5.3 JUSTIFICACION ECONOMICA

Desde el punto de vista económico, este proyecto de diseño es fundamental porque permitirá realizar un análisis exhaustivo de las condiciones de seguridad y riesgo del

Centro Integral. La información recabada será clave para definir de manera precisa la ubicación óptima y la cantidad exacta de cámaras de vigilancia, así como las especificaciones técnicas del equipamiento necesario. Esto asegurará una **optimización de los recursos** al momento de una futura implementación, **evitando gastos innecesarios** en equipos sobredimensionados o insuficientes y garantizando una inversión eficiente y estratégica.

1.5.4 JUSTIFICACION TECNOLÓGICA

La justificación tecnológica reside en la **constante evolución de los sistemas de videovigilancia**, que ofrecen hoy en día soluciones más inteligentes, eficientes y fiables. Este proyecto busca diseñar un sistema que incorpore estas **tecnologías de vanguardia**, permitiendo a la Universidad Autónoma Juan Misael Saracho, como institución pública y formadora de profesionales, estar a la altura de la demanda y los avances tecnológicos en materia de seguridad.

1.6 ALCANCES Y LIMITACIONES

1.6.1 ALCANCES

El presente proyecto se **enfocará en el diseño** detallado de un sistema integral de videovigilancia IP para el Centro Integral de Niños de la UAJMS. El alcance incluye:

- La determinación de la cantidad y ubicación estratégica de las cámaras IP.
- La selección del tipo y características técnicas de los dispositivos (cámaras, switches PoE, NVR o servidor de almacenamiento).
- El dimensionamiento de la capacidad de almacenamiento y el análisis del tráfico de video esperado.
- La propuesta de un software de monitoreo y gestión acorde a las necesidades del centro.
- Diagramas y especificaciones técnicas necesarias para una futura implementación.

Este diseño se desarrollará considerando la compatibilidad con la infraestructura tecnológica existente en el campus universitario, permitiendo una futura integración o expansión del sistema.

1.6.2 LIMITACIONES

El presente proyecto **no contempla la instalación física, configuración o puesta en marcha** del sistema de videovigilancia, ya que su alcance se limita exclusivamente al diseño técnico.

Asimismo, no incluye el desarrollo completo de una arquitectura integral de seguridad de red ni la configuración específica de VLANs, direccionamiento o políticas de acceso. Sin embargo, **se incorporarán recomendaciones técnicas** relacionadas con:

- la segmentación de la red, (Recomendaciones técnicas pág. N° 40)
- la seguridad física de los equipos,
- y las buenas prácticas de protección de la infraestructura, con el objetivo de proporcionar lineamientos que orienten una implementación futura más segura y eficiente.

1.7 HIPOTESIS

El diseño propuesto de un sistema de videovigilancia IP para el Centro Integral de Niños de la UAJMS permitirá mejorar significativamente la seguridad y el bienestar de los niños, mediante la reducción efectiva de incidentes como accesos no autorizados o conflictos suscitados en el centro, el aumento de la supervisión, y el consecuente fomento de la confianza de los padres en los ambientes del centro integral.

1.8 CONCEPTUALIZACION DE LAS VARIABLES

- **Variables Independientes:** Tipo de cámaras, ubicación, sistema de almacenamiento, software de monitoreo.
- **Variables Dependientes:** Nivel de seguridad, efectividad del monitoreo, satisfacción de padres y personal.

CAPITULO II

MARCO TEORICO

2.1 MARCO TEORICO

El presente marco teórico tiene como finalidad sentar bases conceptuales y tecnologías necesarias para el diseño del sistema de videovigilancia propuesto. Se abordarán definiciones teóricas y las tecnologías actuales relevantes, incluyendo sistemas de videovigilancia, redes de datos (modelo OSI y TCP/IP), tipos de cámaras IP, NVR y sistemas de alarmas.

2.2 TECNOLOGÍAS APLICADAS A LA PROTECCIÓN DE PERSONAS

Las tecnologías aplicadas a la protección de personas comprenden un conjunto de herramientas diseñadas para prevenir riesgos, mejorar la supervisión y garantizar la integridad de individuos dentro de un entorno físico. Estas tecnologías combinan dispositivos electrónicos, sistemas de comunicación, software inteligente y plataformas de monitoreo con el objetivo de reducir amenazas, responder ante emergencias y mejorar la seguridad institucional.

Entre las tecnologías más utilizadas en entornos educativos y centros infantiles se encuentran:

Sistemas de videovigilancia IP

Constituyen una de las herramientas más efectivas para la supervisión continua. Incluyen cámaras IP, cámaras PTZ, cámaras panorámicas y equipos con capacidad de analítica de video. Estos sistemas permiten monitorear actividades en tiempo real, registrar eventos y detectar comportamientos inusuales.

Analítica de video basada en inteligencia artificial (IA)

Las cámaras modernas incorporan funciones avanzadas como detección de movimiento, intrusiones, merodeo, líneas virtuales, conteo de personas y seguimiento automático. Estas herramientas permiten una respuesta más rápida y precisa ante situaciones de riesgo.

Sistemas de almacenamiento y gestión de video (NVR/VMS)

Los grabadores de video en red (NVR) y los sistemas de gestión de video (VMS)

permiten organizar, almacenar y revisar de forma segura las grabaciones generadas por las cámaras IP, garantizando trazabilidad y evidencia visual confiable.

Infraestructura de red con tecnología PoE

El uso de switches PoE (Power over Ethernet) facilita la alimentación eléctrica y transmisión de datos a través de un solo cable, mejorando la eficiencia y reduciendo riesgos asociados a cableado adicional.

En el presente trabajo de grado, la tecnología aplicada a la protección de personas corresponde específicamente a la implementación de un **sistema de videovigilancia IP**, que integra cámaras IP, analíticas de video, almacenamiento en red y una infraestructura de comunicación segura. Esta tecnología permite supervisar las actividades dentro del Centro Integral de Niños de la UAJMS, reducir riesgos, mejorar la capacidad de respuesta y garantizar condiciones adecuadas de seguridad para los menores y el personal a cargo.

2.3 MARCO HISTÓRICO O DE ANTECEDENTES

Diversas instituciones educativas y centros destinados al cuidado infantil han implementado sistemas de videovigilancia para mejorar la seguridad y supervisión en sus instalaciones. Estos antecedentes permiten sustentar la pertinencia del diseño propuesto en el presente trabajo y evidencian que la videovigilancia constituye una práctica ampliamente adoptada a nivel institucional.

En el ámbito universitario, varias instituciones han desarrollado proyectos orientados al diseño e implementación de sistemas de seguridad basados en cámaras IP. Por ejemplo, universidades como la Universidad Mayor de San Andrés (UMSA) y la Universidad Autónoma Gabriel René Moreno (UAGRM) han ejecutado planes de modernización de infraestructura que incluyen sistemas de videovigilancia para el control de accesos, monitoreo de áreas comunes y protección del personal y estudiantes. Estos proyectos han demostrado mejoras significativas en la gestión de incidentes y en la percepción de seguridad dentro del campus.

Asimismo, en instituciones educativas de nivel inicial y centros infantiles se han elaborado diseños específicos de videovigilancia orientados a garantizar el bienestar de los niños. Varias guarderías municipales y centros de desarrollo infantil en diferentes ciudades del país han incorporado sistemas IP con grabación centralizada para supervisar aulas, patios de recreación y áreas de descanso, permitiendo una respuesta más rápida ante emergencias y un mejor control operativo.

Estos antecedentes evidencian que el uso de sistemas de videovigilancia constituye una práctica efectiva y validada en entornos similares al Centro Integral de Niños de la UAJMS. Por lo tanto, el diseño de un sistema de videovigilancia para dicha institución se encuentra alineado con tendencias actuales en seguridad infantil y prácticas adoptadas en otras entidades educativas, respaldando así la relevancia y viabilidad del presente proyecto.

2.4 MARCO LEGAL O JURÍDICO

El diseño e implementación de un sistema de videovigilancia en espacios destinados al cuidado infantil debe enmarcarse en la normativa nacional e institucional que regula la protección de datos personales, la privacidad y el uso responsable de tecnologías de monitoreo. A continuación, se presentan las principales disposiciones legales y lineamientos aplicables al presente proyecto:

2.4.1 Constitución Política del Estado (CPE)

La CPE establece principios fundamentales relacionados con la privacidad y la protección de la dignidad humana:

- **Artículo 21, numeral 2:** Garantiza el derecho a la intimidad y privacidad.
- **Artículo 15:** Protege el derecho a la integridad física, psicológica y sexual, especialmente de niñas y niños.
- **Artículo 59:** Establece el deber del Estado y las instituciones de proteger los derechos de la niñez y garantizar condiciones adecuadas para su desarrollo.

El sistema de videovigilancia propuesto debe operar respetando estos derechos, evitando el uso indebido de imágenes o la vulneración de la privacidad.

2.4.2 Código Niño, Niña y Adolescente (Ley 548)

Esta ley, aplicable directamente a la población del Centro Integral, indica:

- **Artículo 10:** Protección de la imagen, identidad y privacidad de niñas y niños.
- **Artículo 12:** Protección contra toda forma de violencia, omisión o negligencia.

El sistema de videovigilancia constituye una herramienta de prevención y seguridad, siempre que su uso sea responsable y no implique exposición indebida de imágenes.

2.4.3 Ley 164 – Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación

Regula el uso adecuado de tecnologías digitales:

- **Artículos 73 y 74:** Establecen principios sobre protección de datos personales y tratamiento adecuado de información digital.
- El manejo de grabaciones debe cumplir los principios de:
 - **finalidad,**
 - **proporcionalidad,**
 - **seguridad,**
 - **confidencialidad,**
 - **acceso restringido.**

El almacenamiento de video debe estar protegido contra accesos no autorizados.

2.4.4 Ley 1178 – Responsabilidad por la Función Pública

Aplicable a instituciones estatales, incluyendo la universidad. Obliga a garantizar la seguridad de bienes, servicios y personas bajo responsabilidad institucional.

El uso de videovigilancia contribuye al cumplimiento de este deber.

2.4.5 Normativa sobre videovigilancia en instituciones educativas

Si bien Bolivia no cuenta con una ley específica para videovigilancia en centros educativos, se aplican principios derivados de:

- Buenas prácticas de videovigilancia (ISO/IEC 27001, ISO 22301).
- Lineamientos internacionales sobre uso responsable de cámaras en ambientes infantiles.
- Principio de supervisión adulta continua (educación inicial).

Estas guías recomiendan:

- Ubicar cámaras solo en áreas permitidas (no baños, no cambiadores).
- Mantener accesos restringidos al personal autorizado.
- Establecer plazos de retención de grabaciones.

2.4.6 Políticas institucionales de la UAJMS

Aunque la UAJMS no posee una normativa pública específica sobre videovigilancia, sí promueve lineamientos generales relacionados con:

- **Uso ético de las Tecnologías de Información,**
- **Protección y bienestar de la comunidad universitaria,**
- **Ambientes seguros para estudiantes y personal,**
- **Protocolos de seguridad y prevención** en unidades académicas y centros dependientes.

El sistema de videovigilancia diseñado se alinea con estos principios institucionales, garantizando:

- el uso responsable de imágenes,
- la protección de la identidad de los niños,

- la administración segura del sistema,
- y la supervisión adecuada por parte de personal autorizado.

2.5 SISTEMAS DE VIDEO VIGILANCIA

Existen en la actualidad 2 tipos de sistemas de video vigilancia los CCTV analógicos y los sistemas digitales sobre IP. Gracias a los avances de las tecnologías los primeros, ya no son tan usados ni buscados debido a que no ofrecen ventajas ni en la parte técnica ni en los costos de implementación ante los sistemas digitales IP, pero a fin de conocer los inicios de la video vigilancia se los menciona en el presente trabajo.

2.5.1 CCTV Analógicos

Los sistemas de video vigilancia analógicos han sido la opción tradicional durante muchos años. Estos sistemas utilizan cámaras que capturan las imágenes en formato analógico y las transmiten mediante cables coaxiales a un dispositivo de grabación, como un DVR (Digital Video Recorder). Una de las principales características de los sistemas analógicos es su sencillez y costo más bajo en comparación con los sistemas modernos.

Sin embargo, las cámaras analógicas tienen limitaciones en términos de calidad de imagen, generalmente ofreciendo resoluciones más bajas en comparación con los sistemas digitales. Además, las imágenes analógicas deben ser convertidas a formato digital para su almacenamiento, lo que puede reducir la calidad y ocupar más espacio de almacenamiento. A pesar de estas limitaciones, muchos sistemas de CCTV analógicos aún se utilizan debido a su fiabilidad y menor complejidad tecnológica (Rose, 2019).

Otra desventaja significativa de los sistemas analógicos es la limitada flexibilidad. Las cámaras están conectadas directamente a una unidad de grabación mediante cables, lo que dificulta la expansión o integración de otros sistemas de seguridad. Además, el acceso remoto a las imágenes no es nativo en estos sistemas, lo que requiere equipos adicionales para habilitar la visualización remota (Blyth, 2020).

2.5.2 Sistemas Digitales sobre IP

Los sistemas de video vigilancia digitales basados en IP (Internet Protocol) llegan a ser una evolución tecnológica sobre los sistemas analógicos. En los sistemas de CCTV IP, las cámaras capturan imágenes en formato digital desde el primer momento, lo que permite una transmisión directa a través de redes IP, como Internet o redes locales (Ethernet). A diferencia de los sistemas analógicos, las cámaras IP ofrecen una mayor flexibilidad, ya que pueden conectarse a la red sin la necesidad de cables coaxiales, permitiendo una infraestructura más escalable (Wood, 2021).

Una de las ventajas clave de los sistemas IP es su alta calidad de imagen, con cámaras que pueden alcanzar resoluciones de hasta 4K, lo que permite una mayor claridad y detalle en las grabaciones. Además, estos sistemas ofrecen funcionalidades avanzadas, como análisis de video, detección de movimiento, y fácil acceso remoto desde dispositivos móviles o computadoras, sin necesidad de equipo adicional (Cheng, 2018).

Otra ventaja importante es la capacidad de almacenar las grabaciones en sistemas de almacenamiento en la nube, lo que permite un acceso más flexible y seguro a los archivos de video. La integración con otros sistemas de seguridad también es más sencilla en los sistemas IP, lo que los convierte en una solución más robusta para instalaciones grandes o con requisitos complejos de seguridad (Davis, 2021).

2.5.3 Comparación de los Sistemas Analógicos y Digitales sobre IP

Calidad de Imagen: Los sistemas IP ofrecen imágenes de alta resolución (HD, 4K) en comparación con la calidad limitada de los sistemas analógicos.

- **Escalabilidad:** Los sistemas IP son más fáciles de escalar, mientras que los sistemas analógicos requieren más infraestructura (cableado).
- **Acceso Remoto:** Los sistemas IP permiten un acceso remoto más sencillo y nativo, mientras que en los sistemas analógicos se necesitan adaptaciones.

- **Costo:** Los sistemas analógicos suelen ser más económicos en la instalación inicial, pero los sistemas IP ofrecen mejores opciones a largo plazo debido a su flexibilidad y calidad.

2.6 REDES DE DATOS

Las redes de datos, son un conjunto de sistemas que permiten la interconexión entre dispositivos, como ser computadoras, servidores, impresoras, cámaras y otros equipos de red permitiendo compartir recursos, elementos y transmitir información a través de medios físicos o inalámbricos incrementando así la eficiencia de los procesos. Estas redes pueden clasificarse de acuerdo con su tamaño y alcance geográfico son usadas desde redes domésticas hasta grandes infraestructuras empresariales.

Una definición general según (Wetherall, 2019), una red de datos se define como “un sistema que permite la transmisión de datos entre dos o más dispositivos, utilizando medios de transmisión como cables o enlaces inalámbricos”.

2.6.1 Clasificación de las redes de datos

- **LAN (Local Area Network):** Redes de área local, que conectan dispositivos dentro de una ubicación geográfica limitada, como una casa, oficina o campus. Estas redes suelen ser rápidas y de bajo costo, siendo las más comunes en entornos domésticos y pequeñas empresas (Forouzan B. , 2017).
- **WAN (Wide Area Network):** Redes de área amplia, que abarcan grandes distancias geográficas y conectan múltiples LAN. Un ejemplo clásico de WAN es Internet, que interconecta redes a nivel global (Kurose, Computer networking: a top-down approach, 2021).
- **MAN (Metropolitan Area Network):** Redes de área metropolitana, que conectan dispositivos en una ciudad o área metropolitana, ofreciendo servicios de comunicación de alta velocidad en áreas más extensas que una LAN, pero más pequeñas que una WAN (Stallings, Data and Computer communications, 2020).

2.6.2 Componentes de las redes de datos

Los componentes básicos de las redes de datos incluyen dispositivos como routers, switches, y puntos de acceso, que ayudan a dirigir el tráfico de datos entre dispositivos de manera eficiente. Además, las redes utilizan protocolos de comunicación, como TCP/IP, que establecen reglas para la transmisión de datos entre dispositivos y garantizan que la información se envíe y reciba correctamente (Kurose, Computer networking, 2021).

2.6.3 Normas y estándares

Para que una red de datos funcione de manera eficiente y segura, es necesario que siga ciertos estándares y normas. Entre los más conocidos se encuentran las normas desarrolladas por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), como el estándar IEEE 802.3 para redes Ethernet y IEEE 802.11 para redes inalámbricas (Wi-Fi). Estos estándares permiten la interoperabilidad entre diferentes fabricantes y garantizan la compatibilidad y seguridad en las redes (Forouzan, Data communications and networking, 2017).

2.6.4 Modelo OSI

El **modelo OSI (Open Systems Interconnection)** es un marco de referencia estándar desarrollado por la **Organización Internacional de Normalización (ISO)** para la interconexión de sistemas de comunicación abiertos. Este modelo se divide en siete capas que describen cómo los diferentes protocolos y tecnologías de red interactúan y funcionan entre sí para permitir la comunicación de datos en una red. El modelo OSI facilita la interoperabilidad entre productos y tecnologías de diferentes fabricantes y proporciona una base estructurada para el diseño y comprensión de redes.

Definición general

Según (Forouzan, Data Communications and networking, 2017), el modelo OSI es un "modelo de referencia que organiza las funciones de una red en siete capas distintas,

con el fin de estandarizar la interacción entre dispositivos y aplicaciones en una red de datos". Este modelo proporciona una arquitectura en la cual cada capa realiza funciones específicas y se comunica con la capa inmediatamente superior o inferior.

Las 7 capas del modelo OSI

1. **Capa Física:** Es la primera capa y define los aspectos físicos del hardware que interconecta dispositivos en una red, como cables, conectores, voltajes, señales eléctricas y características de transmisión (Stallings, Data and Computer Communications, 2020).
2. **Capa de Enlace de Datos:** Proporciona medios para la transferencia de datos confiable entre nodos en una red local, gestionando errores de transmisión, sincronización y control de flujo. Esta capa está subdividida en dos subcapas: control de acceso al medio (MAC) y control de enlace lógico (LLC) (Tanenbaum, Computer networks, 2019).
3. **Capa de Red:** Encargada del enrutamiento de paquetes de datos a través de la red. Determina la mejor ruta para que los datos lleguen de un dispositivo a otro y gestiona las direcciones lógicas, como las direcciones IP (Kurose, Computer networking: A top-down approach, 2021).
4. **Capa de Transporte:** Asegura la transferencia confiable de datos entre sistemas, estableciendo, manteniendo y finalizando conexiones. Proporciona mecanismos para el control de errores y la retransmisión de paquetes perdidos (Forouzan, Data communications and networking, 2017).
5. **Capa de Sesión:** Establece, gestiona y finaliza sesiones o conexiones entre aplicaciones en dispositivos diferentes. Esta capa permite la comunicación entre dispositivos y asegura que las sesiones se mantengan activas mientras dure la transmisión de datos (Stallings, Data and Computers communications, 2020).
6. **Capa de Presentación:** Se ocupa de la traducción, cifrado y compresión de datos. Su función principal es garantizar que los datos enviados por la capa de aplicación de un sistema puedan ser comprendidos por la capa de aplicación de otro (Tanenbaum, Computer networks, 2019).

7. **Capa de Aplicación:** Es la capa más cercana al usuario, proporcionando servicios de red directamente a las aplicaciones, como correo electrónico, navegación web y transferencia de archivos. Interactúa con aplicaciones de usuario final para proporcionarles acceso a los servicios de la red (Kurose, Computer networking, 2021).

Importancia del Modelo OSI

El modelo OSI es fundamental en la estandarización de los sistemas de comunicación porque divide las funciones de red en diferentes capas, lo que permite que los ingenieros y desarrolladores trabajen en partes específicas del sistema sin necesidad de entender todo el sistema en su conjunto. Además, permite la interoperabilidad de equipos y software de diferentes fabricantes, ya que cada uno puede desarrollar soluciones compatibles con las funciones de una o varias capas del modelo (Stallings, Data and Computer communications, 2020).

2.6.5 Modelo TCP/IP

El **modelo de red TCP/IP** (Transmission Control Protocol/Internet Protocol) es una arquitectura de protocolos diseñada para la interconexión de sistemas informáticos y la transmisión de datos en redes. Es el modelo básico sobre el cual está construido Internet y se utiliza ampliamente para la comunicación de datos a nivel global. A diferencia del modelo OSI, el modelo TCP/IP tiene cuatro capas principales que definen cómo los datos se transmiten entre dispositivos en una red.

Definición general

Según (Kurose, Computer networking: A top-down approach, 2021) Kurose, el modelo TCP/IP es "una arquitectura de red diseñada específicamente para la interconexión de redes heterogéneas, permitiendo que los datos se transmitan de manera eficiente entre dispositivos sin importar las diferencias en el hardware o

software subyacente". TCP/IP establece las reglas y procedimientos que deben seguirse para que los datos puedan viajar a través de la red de manera confiable.

Capas del modelo TCP/IP

Este modelo se compone en 4 etapas, que se detalla a continuación:

1. **Capa de Enlace de Datos:** Esta capa es responsable de la transmisión física de los datos entre dispositivos conectados a una misma red. Incluye tanto los medios de transmisión (como cables o conexiones inalámbricas) como los protocolos que determinan cómo los datos se codifican y transmiten. Los protocolos específicos de esta capa pueden variar según el tipo de red utilizada, como Ethernet o Wi-Fi (Forouzan, Data communications and networking, 2017).
2. **Capa de Internet:** Proporciona el direccionamiento lógico y el enrutamiento de paquetes entre redes. En esta capa se encuentra el **Protocolo de Internet (IP)**, que se encarga de dirigir los paquetes a través de múltiples redes hasta su destino final. Otros protocolos importantes en esta capa son ICMP (Internet Control Message Protocol) y ARP (Address Resolution Protocol). Esta capa es comparable a la capa de red en el modelo OSI (Tanenbaum, Computer networks, 2019).
3. **Capa de Transporte:** Proporciona comunicación confiable entre aplicaciones que se ejecutan en diferentes dispositivos. Los principales protocolos de esta capa son el **Protocolo de Control de Transmisión (TCP)** y el **Protocolo de Datagramas de Usuario (UDP)**. TCP ofrece un servicio de transmisión confiable, orientado a la conexión, con control de errores y de flujo. Por otro lado, UDP es un protocolo no orientado a la conexión, que ofrece un servicio más rápido, pero sin garantías de entrega (Kurose, Computer networking, 2021).
4. **Capa de Aplicación:** Es la capa más alta del modelo TCP/IP y proporciona servicios directamente a las aplicaciones de usuario, como la transferencia de archivos, el envío de correos electrónicos y la navegación web. Algunos de los protocolos más importantes de esta capa son **HTTP (HyperText Transfer Protocol)**, **FTP (File Transfer Protocol)**, **SMTP (Simple Mail Transfer Protocol)**.

Protocol) y **DNS (Domain Name System)**. Estos protocolos permiten la interacción de las aplicaciones de usuario final con la red (Forouzan, Data communications and networking, 2017).

Comparación con el modelo OSI

El modelo TCP/IP es más simple que el modelo OSI, que tiene siete capas, mientras que TCP/IP tiene solo cuatro. En el modelo OSI, las funciones de la capa de enlace de datos y la capa física están separadas, mientras que en el modelo TCP/IP, ambas están combinadas en la Capa de Enlace de Datos. Además, las capas de sesión y presentación del modelo OSI están incluidas en la Capa de Aplicación de TCP/IP (Stallings, 2020).

Importancia del Modelo TCP/IP

El modelo TCP/IP es fundamental para la operatividad de Internet y otras redes modernas. Su diseño flexible y escalable permite que dispositivos heterogéneos se comuniquen de manera eficiente, independientemente del hardware o software que utilicen. Además, TCP/IP ha demostrado ser adaptable a lo largo del tiempo, soportando el crecimiento masivo de Internet y la aparición de nuevas tecnologías de red (Tanenbaum & Wetherall, 2019).

2.7 VIDEO IP

El video IP o video vigilancia IP, al igual que muchos otros tipos de comunicaciones como por ejemplo el correo electrónico, servicios web, se realiza mediante redes, ya sean cableadas o inalámbricas. Todo el flujo de audio/video se efectúa a través de la misma infraestructura de red común, lo cual conlleva multitud de ventajas sobre los sistemas CCTV tradicionales. Las aplicaciones que se pueden tener con el video en red son ilimitadas siempre dentro del ámbito de la vigilancia y seguridad o la supervisión remota de personas, algunas posibles soluciones pueden ser:

- Reconocimiento de placas
- Monitorización de tráfico
- Vigilancia en condiciones de absoluta oscuridad, usando luz infrarroja
- Vigilancia de niños en el hogar, en la escuela, parques, guarderías
- Análisis facial para identificación de criminales en áreas públicas
- Aplicaciones educativas, Etc.

2.7.1 Cámaras de red

Existen varios tipos de **cámaras IP** que se utilizan en sistemas de video vigilancia. Cada tipo está diseñado para cumplir con diferentes requisitos de seguridad, entorno y funcionalidad. A continuación, se mencionan algunos de los tipos más comunes con una breve descripción:

1. Cámara IP Fija

- Descripción: Estas cámaras están montadas en una ubicación estática, capturando imágenes en una sola dirección. Son simples de instalar y se utilizan comúnmente para vigilar áreas específicas. No ofrecen movimiento panorámico o de inclinación.
- Referencia: Según Forouzan (2017), las cámaras IP fijas son ideales para áreas donde la cobertura de una dirección es suficiente

2. Cámara IP PTZ (Pan-Tilt-Zoom)

- Descripción: Permiten el movimiento remoto (horizontal y vertical) y zoom, ofreciendo una cobertura flexible. Son útiles en grandes espacios donde se necesita monitoreo dinámico.
- Referencia: Tanenbaum y Wetherall (2019) señalan que las cámaras PTZ proporcionan un control remoto efectivo, adaptándose a entornos de seguridad avanzada.

3. Cámara IP Domo

- Descripción: Montadas en una carcasa con forma de cúpula, son más discretas y resistentes al vandalismo. Pueden ser fijas o PTZ, y se usan tanto en interiores como en exteriores.
- Referencia: Kurose y Ross (2021) destacan que las cámaras domo son populares debido a su diseño compacto y su capacidad para ser más discretas.

4. Cámara IP Bala

- Descripción: Estas cámaras tienen un diseño cilíndrico y son fáciles de instalar en paredes o techos. Son comúnmente utilizadas para exteriores debido a su resistencia a la intemperie.
- Referencia: Stallings (2020) menciona que las cámaras tipo bala son ideales para áreas donde se requiere vigilancia visible y disuasoria.

5. Cámara IP Ojo de Pez (Fisheye)

- Descripción: Con una lente gran angular, proporcionan un campo de visión de 180° o 360°, lo que permite monitorear áreas extensas sin necesidad de mover la cámara.
- Referencia: Kurose y Ross (2021) describen las cámaras de ojo de pez como efectivas para áreas grandes, donde se busca minimizar la cantidad de cámaras necesarias.

6. Cámara IP para Visión Nocturna (Infrarroja)

- Descripción: Equipadas con LED infrarrojos, permiten la vigilancia en condiciones de poca o nula luz, capturando imágenes en blanco y negro durante la noche.
- Referencia: Según Forouzan (2017), las cámaras infrarrojas son fundamentales para la seguridad nocturna y en ambientes oscuros.

7. Cámara IP PoE (Power over Ethernet)

- Descripción: Utilizan el mismo cable Ethernet para transmitir datos y alimentación eléctrica, lo que simplifica la instalación y reduce la necesidad de cables adicionales.
- Referencia: Tanenbaum y Wetherall (2019) señalan que las cámaras PoE son eficientes en términos de costos y fáciles de implementar en instalaciones complejas.

8. Cámara IP Oculta

- Descripción: Diseñadas para ser discretas y difíciles de detectar, estas cámaras están integradas en objetos cotidianos o camufladas en el entorno.
- Referencia: Stallings (2020) describe las cámaras ocultas como ideales para la vigilancia encubierta, siendo difíciles de detectar por el público.

9. Cámara IP Térmica

- Descripción: Capturan imágenes basadas en la radiación térmica emitida por los objetos, lo que les permite detectar movimiento y presencia en la oscuridad total.
- Referencia: Kurose y Ross (2021) destacan que las cámaras térmicas son usadas principalmente en aplicaciones de seguridad perimetral y en ambientes con poca luz.

10. Cámara IP con Audio Bidireccional

- Descripción: Permiten la comunicación en tiempo real entre el operador y las personas capturadas por la cámara, gracias a la integración de micrófonos y altavoces.
- Referencia: Según Forouzan (2017), estas cámaras son útiles para el control de acceso en tiempo real y la comunicación directa con personas en el área vigilada.

2.8 PROTOCOLO ONVIF

La interfaz ONVIF (Open Network Video Interface Forum) permite la interconexión de productos de video en red, sin importar el fabricante, lo que facilita al usuario final, de los sistemas de video en red, la integración de sus sistemas y le da una mayor flexibilidad y efectividad en el costo de posibles aplicaciones. La ventaja principal de este estándar es que facilita la integración de diferentes marcas de equipo de video en red, con el fin de ayudar a los fabricantes y desarrolladores de software a manejar de manera integrada los productos y a los usuarios darle una mayor flexibilidad en la elección de productos de diferentes fabricantes que les permitan desarrollar sistemas que incluyan sus necesidades. ONVIF también se apoya en estándares de compresión de video como H.264, MPEG-4 y M-JPEG y audio como G.711, G.726, AAC y unidireccional de acuerdo a Nuñez y Pila (2014).

2.9 GRABADORES

Las **videograbadoras para videos en red**, también conocidas como **NVR (Network Video Recorders)**, son dispositivos especializados que se utilizan para grabar y gestionar los flujos de video generados por cámaras IP en una red. A diferencia de las grabadoras de video digital (DVR) que funcionan con cámaras analógicas, las NVR funcionan exclusivamente con cámaras IP, lo que permite la grabación y el acceso a video a través de redes IP, generalmente Ethernet.

Descripción general

Según Stallings (2020), las NVR son "sistemas de grabación centralizados que almacenan video en formato digital directamente desde cámaras de vigilancia IP a través de una red, permitiendo el acceso y la gestión remota de las grabaciones". Las videograbadoras en red se utilizan ampliamente en sistemas de video vigilancia modernos debido a su escalabilidad y flexibilidad, ya que pueden manejar múltiples cámaras IP de manera simultánea.

Funciones clave:

- **Grabación y almacenamiento:** Las NVR graban video en discos duros locales o en almacenamiento en red (NAS). Algunas ofrecen almacenamiento redundante para garantizar la seguridad de los datos.
- **Acceso remoto:** Estas videograbadoras permiten el acceso a las grabaciones de video desde cualquier dispositivo conectado a la red, como computadoras o smartphones.
- **Gestión de cámaras:** Las NVR permiten configurar, controlar y monitorear múltiples cámaras IP conectadas en una misma red, facilitando la administración del sistema de video vigilancia desde un solo punto (Forouzan, 2017).
- **Compatibilidad:** Aunque la mayoría de los sistemas NVR están diseñados para cámaras IP, algunos modelos pueden funcionar con cámaras híbridas (analógicas y digitales), lo que proporciona flexibilidad en la instalación.

Importancia

Kurose y Ross (2021) afirman que las NVR son esenciales en la video vigilancia moderna, ya que su capacidad de grabar y gestionar video a través de redes IP permite una integración eficiente con sistemas más grandes, como los de seguridad o de monitoreo empresarial. Además, son más flexibles que los DVR porque no requieren una conexión directa con las cámaras, permitiendo que las cámaras IP estén ubicadas en diferentes lugares, siempre que estén conectadas a la red.

2.10 ALARMAS

2.10.1 Tipos de sistemas de alarmas

Se pueden clasificar según la aplicación en alarmas de: incendios, robos, procesos industriales, entre muchas otras. Cada uno de estos utilizan sensores para las variables específicas que estas detectan. También se pueden clasificar por el tipo de salida en cableados o inalámbricos. Los sistemas cableados o guiados pueden tener salida digitales o estar conectados en una red, los inalámbricos transmiten la señal por medios

no guiados, en ambos casos mediante estándares de transmisión de datos y de protocolos de comunicación. (López 2007).

2.10.2 Módulo de procesamiento de alarmas

Es un dispositivo que recibe las señales de las variables que establecen las condiciones de alarma y las procesan, si la variable indica que hay una situación anormal, activa los elementos finales de acción para avisar el evento de acuerdo a López (2007). Estos módulos inicialmente eran diseñados con dispositivos analógicos y/o discretos en el procesamiento. Actualmente, están basados en microcontroladores mediante un conjunto de instrucciones, almacenadas en una memoria, realizan todas las funciones de procesamiento de alarmas y del manejo del sistema. Estos módulos generalmente tienen un teclado y algún dispositivo de visualización que conforman la interfaz hombre máquina (HMI) para programar la configuración y la forma como debe actuar el sistema de alarma, según los requerimientos del usuario.

2.10.3 Sensores de alarmas

En general, un sensor es dispositivo que permite transformar una variable de un tipo de energía a otro mediante un transductor. La salida de los sensores es un tipo de señal eléctrica, que pueden ser digital, analógica y algunos disponen de dispositivos especiales que generan señales de comunicación cableadas o inalámbricas. Un sensor muy utilizado es el detector de movimientos que utiliza un transmisor y receptor de luz infrarroja y basado en el tiempo de regreso determina si hay cambios de ubicación de los objetos o personas en la zona observada. Otro es la detección de apertura de puertas y/o ventanas con sensores magnéticos, estos consisten de un interruptor que se activa al acercarse a un imán. Los sensores pueden ser cableados o inalámbricos. (Juan 2010)

CAPITULO III

MARCO METODOLOGICO

3.1 TIPO DE INVESTIGACIÓN

El presente proyecto corresponde a una **investigación aplicada y descriptiva**.

- **Investigación aplicada:** porque busca resolver un problema real —la ausencia de un sistema de videovigilancia en el Centro Integral de Niños— mediante el diseño de una solución tecnológica concreta.
- **Investigación descriptiva:** porque describe las características del entorno físico, las necesidades de seguridad, los requisitos técnicos y las condiciones actuales del centro, para fundamentar el diseño del sistema.

Este tipo de investigación permite comprender la situación actual, identificar las necesidades reales y proponer un diseño coherente con la infraestructura disponible.

3.2 ENFOQUE METODOLÓGICO

Se adopta un **enfoque mixto (cualitativo–cuantitativo)**:

a) Enfoque cualitativo:

Utilizado para comprender el funcionamiento del centro, sus riesgos y necesidades reales. Incluye:

- entrevistas con la directora del centro,
- observación directa,
- análisis de áreas críticas,
- identificación de problemas de seguridad.

b) Enfoque cuantitativo:

Utilizado para dimensionar los componentes técnicos del sistema:

- cantidad de cámaras,
- distancias de cableado,

- consumo eléctrico,
- ancho de banda,
- almacenamiento de video.

Este enfoque combinado permite obtener una visión integral del problema y diseñar una solución eficiente.

3.3 DISEÑO METODOLÓGICO

El proceso para desarrollar el proyecto se estructuró en **cuatro fases principales**, descritas de forma clara, objetiva y completa:

3.3.1 Fase 1: Recolección de información

Objetivo: comprender las necesidades, riesgos y limitaciones del centro.

Actividades:

1. **Entrevista semiestructurada** con la directora del Centro Integral (Anexo 1).
 - Se identificaron preocupaciones, áreas vulnerables y necesidades de supervisión.
2. **Inspección técnica del sitio.**
 - Se recorrieron los tres niveles del edificio.
 - Se identificaron accesos, pasillos, aulas, áreas de juego, patios, zonas sin supervisión y obstáculos que afectan visibilidad.
3. **Análisis de planos.**
4. **Revisión de normativas aplicables** (privacidad, seguridad infantil, uso de videovigilancia).

3.3.2 Fase 2: Análisis técnico y definición de requerimientos

Objetivo: traducir las necesidades identificadas en requisitos técnicos concretos.

Actividades:

1. Determinación de **cantidad, tipo y ubicación preliminar de cámaras**.
2. Identificación de **estándares técnicos necesarios** (ONVIF, H.265, PoE, IP66, etc.).
3. Evaluación de **disponibilidad eléctrica y de red** del edificio.
4. Identificación de zonas críticas y puntos ciegos.
5. Establecimiento de **requerimientos de almacenamiento y grabación** según normativas y necesidades del centro.

3.3.3 Fase 3: Diseño del sistema de videovigilancia

Objetivo: desarrollar un diseño integral, detallado y coherente con las necesidades identificadas.

Actividades:

1. **Diseño físico y lógico** de la red del sistema.
 - Topología, ubicación de switches, rutas, conexiones al NVR/servidor.
2. **Selección técnica de equipos** (cámaras, NVR, switches, UPS, software VMS).
3. **Elaboración del plano de ubicación de cámaras** (Anexo 2).
4. **Cálculo del ancho de banda requerido** para el tráfico de video.
5. **Cálculo de almacenamiento** según número de cámaras, resolución, códec y tiempo de retención.
6. **Diseño de la arquitectura de energía y protección eléctrica** (UPS, supresores).

3.3.4 Fase 4: Validación y documentación del diseño

Objetivo: asegurar que el diseño propuesto sea viable, escalable y compatible con la infraestructura institucional.

Actividades:

1. Verificación de compatibilidad con tecnologías actualmente presentes en el campus universitario.
2. Ajustes según recomendaciones técnicas de fabricantes y estándares internacionales.
3. Revisión del cumplimiento de normativas de seguridad, privacidad y protección de datos.

3.4 POBLACIÓN Y MUESTRA

- **Población:** instalaciones, personal y niños del Centro Integral.
- **Muestra:**
 - Directora del centro (para entrevista);
 - Infraestructura física del edificio (para inspección técnica);
 - Equipos actuales presentes en el área.

3.5 LIMITACIONES METODOLÓGICAS

- No se realizó implementación física.
- No se hizo medición real de tráfico, solo cálculos teóricos.
- Las entrevistas se limitaron a la autoridad del centro debido a restricciones institucionales.

CAPITULO IV

RESULTADOS

4.1 PRESUPUESTO DEL SISTEMA PROPUESTO

4.1.1 Presupuesto Referencial del Sistema de Videovigilancia Propuesto

El siguiente cuadro presenta el costo estimado del sistema de videovigilancia diseñado para el Centro Integral de Niños de la UAJMS. Los valores corresponden a precios promedio del mercado boliviano y latinoamericano (2024–2025), y se consideran únicamente para fines de planificación y referencia, dado que la tesis no contempla la implementación del sistema.

Tabla 1. Presupuesto Equipamiento Cámaras IP

Ítem	Cantidad	Descripción	Precio unitario (Bs.)	Subtotal (Bs.)
Cámara PTZ 2 MP, Zoom óptico 25x, PoE	1	Para vigilancia dinámica del ingreso principal	5.000	5.000
Cámara Panorámica 180° 4 MP	1	Para ingreso posterior	2.800	2.800
Cámara Fisheye 360° 6 MP	1	Para patio de recreo	2.200	2.200
Cámara Bullet 4 MP Exterior IP66	1	Para patio jardín	1.000	1.000
Cámaras Domo Interior 2 MP	12	Para aulas, pasillos y áreas internas	450	5.400
Subtotal Equipos de Video	—	—	—	16.400

Tabla 2. Presupuesto Grabación y Almacenamiento

Ítem	Cant.	Descripción	Precio Unit. (Bs.)	Subtotal (Bs.)
NVR de 32 canales con soporte H.265	1	Compatible con ONVIF	3.500	3.500
Disco Duro de vigilancia 4 TB	1	WD Purple / Seagate Skyhawk	850	850
Subtotal Grabación	—	—	—	4.350

Tabla 3. Presupuesto Red y Comunicaciones

Ítem	Cant	Descripción	Precio Unit. (Bs.)	Subtotal (Bs.)
Switch PoE 24 puertos	1	Para alimentar las 16 cámaras	2.500	2.500
Patch Panel 24 puertos	1	TIA/EIA-568	350	350
Patch cords (1 m)	24	Para interconexión	15	360
Cable UTP Cat6 (caja 305 m)	1	Color azul estándar	680	680
Conectores RJ-45 Cat6	50	Para terminación	1,5	75
Tubería PVC y canaletas	Global	Para conducción	—	500
Subtotal Red	—	—	—	4.465

Tabla 4. Presupuesto Energía y Protección

Ítem	Cant	Descripción	Precio Unit. (Bs.)	Subtotal (Bs.)
UPS 1500 VA (para Rack)	1	Autonomía para NVR + Switch	1.800	1.800
Supresor de picos/Protección eléctrica	2	Para NVR y switch	250	500
Subtotal Energía	—	—	—	2.300

Tabla 5. Presupuesto Infraestructura

Ítem	Cant	Descripción	Precio Unit. (Bs.)	Subtotal (Bs.)
Rack de Piso 22U	1	Con ventilación	2.500	2.500
Bandejas y accesorios para rack	Global	Soportes y gestión de cables	—	300
Tornillería y accesorios	Global	Material menor	—	200
Subtotal Infraestructura	—	—	—	3.000

Después de tener el presupuesto por áreas, se puede sacar un presupuesto total de todo el proyecto quedando de la siguiente manera:

Tabla 6. Presupuesto General

Categoría	Subtotal (Bs.)
Equipos principales de videovigilancia	16.400
Sistema de grabación y almacenamiento	4.350
Equipos y materiales de red	4.465
Energía y protección	2.300
Infraestructura (rack y accesorios)	3.000
TOTAL ESTIMADO DEL SISTEMA	30.515 Bs.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES Y RECOMENDACIONES

5.1.1 Conclusiones

1. **El Centro Integral de Niños de la UAJMS requiere un sistema de videovigilancia** debido a la ausencia total de cámaras de vigilancia para la supervisión y seguridad. Esta carencia expone a los niños, al personal y a la infraestructura a riesgos prevenibles, situación confirmada mediante inspecciones y entrevistas.
2. **El análisis técnico permitió identificar las áreas críticas del centro**, así como los puntos ciegos y los flujos de actividades diarias. Estos elementos fueron fundamentales para diseñar una propuesta que garantiza cobertura total en zonas internas y externas.
3. **El diseño elaborado cumple con criterios de seguridad, eficiencia, escalabilidad y compatibilidad tecnológica con el actual sistema de videovigilancia que tiene la UAJMS**, integrando cámaras IP, NVR, switches PoE, almacenamiento adecuado. Además, se asegura la compatibilidad con tecnologías existentes en el campus universitario.
4. **Los estándares técnicos y normativos fueron considerados en todo el proceso**, incluyendo buenas prácticas de videovigilancia, regulaciones sobre privacidad, derechos de la niñez y normas de protección de datos. Esto garantiza una propuesta responsable, ética y legalmente adecuada.
5. **El proyecto demuestra que la implementación de un sistema de videovigilancia es técnica y económicamente viable**, con un presupuesto accesible en comparación con los beneficios que aporta en seguridad, prevención y control institucional.
6. Aunque el proyecto se limita al diseño, **constituye una base sólida para su implementación futura**, ya que define especificaciones claras, equipos compatibles y procedimientos estandarizados que pueden adoptarse sin modificaciones sustanciales.

5.1.2 Recomendaciones

1. **Implementar el sistema de videovigilancia propuesto** siguiendo el diseño presentado, priorizando cámaras en áreas críticas como accesos principales, patios de recreación, pasillos y puntos exteriores vulnerables.
2. **Adoptar políticas institucionales específicas sobre uso de videovigilancia y tratamiento de grabaciones**, para garantizar el cumplimiento de la normativa sobre privacidad, protección de datos y derechos de la niñez.
3. **Mantener la segmentación de la red recomendada**, aislando el tráfico de videovigilancia del resto de la red institucional, a fin de mejorar el rendimiento, la seguridad y la administración.
4. **Garantizar la capacitación del personal responsable del monitoreo**, tanto en el uso del software de gestión como en protocolos de actuación ante incidentes.
5. **Establecer un plan de mantenimiento preventivo** que incluya limpieza de cámaras, verificación de conectores, respaldo de grabaciones y revisión del NVR, garantizando la continuidad del sistema.

5.1.3 Recomendaciones técnicas

Segmentación de la Red del Sistema de Videovigilancia

La implementación de un sistema de videovigilancia IP requiere un diseño de red que garantice un funcionamiento estable, seguro y aislado del resto del tráfico institucional. Aunque este proyecto se centra únicamente en el diseño del sistema y no en su instalación, es fundamental considerar lineamientos de segmentación que aseguren la eficiencia del sistema durante una futura implementación.

1. Justificación de la segmentación

El tráfico generado por cámaras IP puede ser elevado, especialmente cuando se manejan resoluciones superiores a 1080p, transmisión continua y almacenamiento centralizado. Por esta razón, se recomienda que el sistema de videovigilancia opere dentro de un segmento de red independiente para:

- **Evitar congestión** en la red del campus universitario.
- **Garantizar un ancho de banda exclusivo** para el tráfico de video.
- **Mejorar la estabilidad y confiabilidad** del sistema de videovigilancia.
- **Aumentar la seguridad**, restringiendo el acceso solo al personal autorizado.
- **Facilitar la administración y monitoreo** del sistema desde el NVR o VMS.

2. Propuesta técnica de segmentación

Se recomienda que la red de videovigilancia sea implementada en una **VLAN (Virtual Local Area Network)** independiente, definida sobre el switch PoE principal del sistema. Esta VLAN deberá cumplir las siguientes características:

- **Tráfico completamente aislado** del resto de la red institucional.
- **Acceso restringido** únicamente al NVR, a las cámaras y al personal autorizado.
- **Asignación de un rango de direcciones IP dedicado**, por ejemplo:
 - VLAN 20 – *Videovigilancia*
 - Subred sugerida: **192.168.20.0/24**
- **Políticas de firewall** para permitir únicamente comunicación entre cámaras ↔ NVR ↔ estación de monitoreo.
- **Bloqueo de accesos externos** no autorizados.

3. Beneficios de esta segmentación

Implementar la segmentación propuesta permitirá:

- Garantizar el rendimiento óptimo del sistema de videovigilancia.
- Evitar que la red académica o administrativa afecte el flujo de video.
- Reducir riesgos de ataques o accesos indebidos.
- Facilitar el mantenimiento, monitoreo, auditoría y gestión del sistema.

4. Consideraciones finales

Aunque este proyecto se limita al diseño del sistema, la segmentación de la red es una práctica recomendada internacionalmente (IEEE, ONVIF, ISO 27001) y debe ser aplicada durante la fase de implementación. La creación de una VLAN para videovigilancia es una medida esencial para garantizar la seguridad, escalabilidad y estabilidad del sistema propuesto.

CAPITULO VI

CRONOGRAMA

6.1 CRONOGRAMA DE ACTIVIDADES

Fase del proyecto	Actividad	Duración	Inicio	Finalización
1. Análisis de requisitos del sistema	Realizar entrevistas y reuniones con personal del centro Integral	2 semanas	1 ^{er} semana de febrero	2 ^{da} semana de febrero
	Revisión de normativa de seguridad	1 semana	3 ^{er} semana de febrero	3 ^{er} semana de febrero
	Elaborar documento de requisitos	1 semana	4 ^{ta} semana de febrero	4 ^{ta} semana de febrero
	Identificación de las necesidades funcionales	1 semana	1 ^{er} semana de marzo	1 ^{er} semana de marzo
2. Diseño conceptual del sistema	Desarrollo de planos de los bloques	2 semanas	2 ^{da} semana de marzo	3 ^{da} semana de marzo
3. Diseño detallado del sistema	Creación de planos técnicos y diagramas de red	2 semanas	4 ^{ta} semana de marzo	1 ^{ra} semana de abril
	Diseño de gabinete	1 semana	2da semana de abril	2da semana de abril
	Calculo y selección de UPS	1 semana	3er semana de abril	3er semana de abril
	Integración de alarmas con sistema de monitoreo	1 semana	4ta semana de abril	4ta semana de abril
	Especificaciones técnicas de hardware y software	1 semana	1 ^{ra} semana de mayo	1 ^{ra} semana de mayo
4. Validación del sistema	Revisión técnica	1 semana	2 ^{da} semana de mayo	2 ^{da} semana de mayo
	Ajustes y mejoras basados en revisiones	1 semana	3 ^{ra} semana de mayo	3 ^{ra} semana de mayo
5. Documentación final	Redacción del manual de diseño	1 semana	4 ^{ta} semana de mayo	4ta semana de mayo
	Elaboración de guías de instalación y configuración	1 semana	1 ^{ra} semana de junio	1 ^{ra} semana de junio
	Revisión final y ajustes a la documentación	1 semana	2 ^{da} semana de junio	2 ^{da} semana de junio

CAPITULO VII

INGENIERIA DEL PROYECTO

7.1 INGENIERIA DEL PROYECTO

7.1.1 Diseño del Sistema de videovigilancia

El objetivo general es Diseñar un sistema integral y seguro de videovigilancia, para ello, la ingeniería se enfocará en definir cada componente y su interacción entre ellos. Este diseño incluye: alcance, requerimientos funcionales y técnicos, propuesta de cobertura (puntual y por zonas) cálculos de ancho de banda y almacenamiento, arquitectura de red, lista de materiales recomendada. No incluye implementación.

7.1.2 Consideraciones de Integración

El sistema de videovigilancia propuesto en el presente proyecto está diseñado para atender de manera específica las necesidades de seguridad y supervisión del Centro Integral de niños de la Universidad Juan Misael Saracho, esto quiere decir que puede funcionar como un sistema propio e independiente. No obstante, el diseño técnico del sistema contempla criterios de compatibilidad y estandarización que permiten su posible integración con el sistema general de videovigilancia de la UAJMS. En ese sentido, el diseño se fundamenta en el uso de tecnologías estándar de videovigilancia IP, arquitectura de red compatible con la del campus universitario y normativas de uso de cámaras de vigilancia.

7.2 ANÁLISIS DE REQUERIMIENTOS Y ESTÁNDARES

7.2.1 Análisis de requerimientos

Antes de seleccionar cualquier componente, es crucial realizar un análisis exhaustivo para que el diseño sea preciso y eficiente.

Levantamiento de Requerimientos:

- Entrevistas: Se realizó una entrevista con la directora del centro integral dando a conocer sus preocupaciones, las necesidades que ella detecta como autoridad del centro integral y su punto de vista en cuanto a las áreas críticas que requieren supervisión. El detalle de la entrevista se presenta en **Anexo 1**

Inspección del Sitio:

- Se realizó un recorrido por el centro integral para poder identificar: áreas de alto tráfico como ser pasillos, escaleras, entradas, también áreas vulnerables como ser lugares de juego, salón de clases, accesos al centro integral y posibles obstáculos como paredes, columnas que puedan limitar la visibilidad.

Con esta información se pudo calcular la cantidad de cámaras y el tipo de cámaras a utilizar para tener una cobertura integral de todas las áreas a proteger y monitorear. Quedando de la siguiente manera:

7.2.2 Propuesta de distribución:

Planta baja

- Ingreso principal – 1 cámara tipo PTZ
- Ingreso posterior – 1 cámara panorámica para vista amplia
- Patio de recreo – 1 cámara fisheye
- Preescolares – 1 cámaras domo interior
- Maternales B – 1 cámara domo interior
- Pasillo multiuso – 1 cámara domo interior
- Sala multiuso – 1 cámara domo interior
- Recepción admisión – 1 cámara domo interiores
- Patio jardín – 1 cámara bullet

Primer piso

- Maternales A – 1 cámara domo interior
- Pasillo – 3 cámaras domo interior
- Lactantes – 1 cámara domo interior

Segundo piso

- Terraza – 2 cámaras domo exterior

Total cámaras propuestas 16

Tabla 7. Cantidad de cámaras consideradas para el Centro Integral

BLOQUE	Ojo de pez	Interior domo	Exterior domo	Bullet	Panorámica	PTZ	Total bloque
Planta baja	1	5		1	1	1	9
Primer piso		5					5
Segundo piso			2				2
TOTAL	1	10	2	1	1	1	16

7.2.3 Definición de Requerimientos Técnicos

- Cámaras compatibles ONVIF; preferir H.265 para reducir almacenamiento.
- Resolución recomendada: 2 MP (1080p) o 4 MP para zonas críticas según necesidad.
- Alimentación PoE (IEEE 802.3af/at según consumo).
- Switches PoE gestionables (VLANs, QoS).
- NVR/Servidor con RAID para grabación.
- Red: VLAN separada para cámaras; uplink gigabit (1 Gbps) entre core y NVR.
- UPS para sala de servidores y switches PoE.
- Cableado Cat6 para tramos ≤ 100 m; fibra para tramos largos o enlaces a distancia.

7.3 DISEÑO DE LA INFRAESTRUCTURA Y SELECCIÓN DE EQUIPOS

7.3.1 Diseño Lógico y Físico

- Diagrama de Topología de Red: Se muestra un diagrama que muestre la interconexión de todos los dispositivos. Esto incluye la ubicación del switch, el NVR y la conexión al servidor de la UAJMS.



- Plano de ubicación de cámaras: Se utilizará un plano del centro integral para marcar la ubicación estratégica de cada cámara.

7.3.2 Topología de Red

Para el diseño del sistema de videovigilancia IP del Centro Integral de Niños de la UAJMS se recomienda la **topología de red estrella tradicional**, debido a las características y necesidades actuales del centro integral. En esta topología, todos los dispositivos del sistema (cámaras IP, NVR, etc.) se conectan directamente a un único switch PoE, que actúa como punto central de distribución.

Esta elección es técnicamente adecuada porque:

- El centro integral requiere un número limitado de cámaras, suficiente para cubrir las áreas críticas.
- La distancia entre los dispositivos y el rack central se mantiene dentro de los 100 metros, límite acorde con cableado UTP.
- El entorno físico es compacto y no requiere segmentar zonas ni distribuir equipos en múltiples salas.
- La cantidad de tráfico de video generada puede ser manejada eficientemente por un solo switch PoE compatible.

Por estas razones, la topología estrella ofrece simplicidad, eficiencia de costos y facilidad de implementación, cumpliendo plenamente con los requerimientos del diseño actual del proyecto.

7.3.3 Selección de equipos

Equipamiento Cámaras

- a) **Cámaras IP:** Se recomiendan modelos específicos de acuerdo a la infraestructura del Centro Integral, como ya se mencionó en el punto anterior la cantidad de cámaras a utilizar considerando su funcionalidad y ubicación
- b) **Cámara PTZ:** Es una cámara PTZ Normal, Este tipo de cámara ya se encuentra instalado en bloques del campus de la Universidad, y se propone en este proyecto utilizar cámaras tipo PTZ con Zoom óptico mayor a 25x y de 2 megapíxeles, las mismas que son motorizadas y giran de acuerdo a requerimiento del operador.
- c) **Cámara Panorámica:** Es una cámara Panorámica de 180°, Es para tomar escenas panorámicas de 180° en ambientes exteriores, como frontis de bloques, teniendo una imagen completa de todos los eventos presentes en su radio de acción.
- d) **Cámara ojo de Pez:** Es una Cámara Interior Panorámica de 360°, comúnmente conocida como ojo de pez, se consideró este tipo de cámara por su gran alcance de escenas y además para optimizar la cantidad de equipos instalados.
- e) **Cámara Interior Tipo domo:** Este tipo de cámara es de lente fijo para interiores con infrarrojo.
- f) **Cámara Exterior Tipo domo:** Este tipo de equipo se propone que sea de 4 Megapíxeles de resolución, tendrá lente fijo y mínimamente protección IP66.

7.3.4 Justificación de cantidades en planos del centro integral

El centro integral de la UAJMS cuenta con una infraestructura adecuada para el cuidado de los niños, fue pensado y diseñado con ese propósito de albergar niños. Esto quiere decir que cuenta con diversos ambientes como ser: área de cunas, área de juegos, salas de curso y/o actividades, patio de recreación y por su puesto oficinas administrativas. Estos ambientes se encuentran repartidos en 3 diferentes pisos

De acuerdo al recorrido en el lugar y a lo conversado con la directora del centro integral se vio por conveniente la ubicación de las cámaras y para mayor y mejor apreciación se detalla esta información en los planos arquitectónicos del centro integral los cuales se encuentran en el **ANEXO 2**

7.3.5 Justificación de cantidades de cámaras de acuerdo a:

a) Angulo de visión (Field of View - FOV)¹

A continuación, se muestran valores de referencia de FOV horizontal para cada tipo de cámara.

Tabla 8. Cuadro de FOV referencial de cada cámara

Tipo de cámara	FOV Horizontal típico	Observación sobre uso
PTZ	Variable 1°-360° (pan 360°) FOV óptico variable	Cubre grandes áreas mediante paneo; se justifica en entradas principales por patrullaje dinámico
Panorámica	120° - 180°	Buena para obtener visión amplia sin punto ciego lateral, ideal ingreso posterior
Fisheye (360°)	180° - 360°	Cobertura de 360° desde un solo punto (ideal para patios) puede usarse deswarpe en VMS para vistas múltiples
Domo interior (fijo)	70° - 110°	Útil en aulas pasillos cortos y oficinas
Bullet (exterior)	60° - 90°	Foco más estrecho, mayor alcance y zoom; buena para perímetros y accesos.

¹ FOV= Campo de visión

Domo exterior	50° - 120°	Útiles para lugares abiertos, resistentes a inclemencias del tiempo.
---------------	------------	--

b) Áreas críticas justificación por zona

Ingreso principal — 1 PTZ

- Justificación: El ingreso principal requiere vigilancia dinámica (seguir personas, ampliar para identificación). Un PTZ con paneo 360° puede patrullar y hacer zoom a sospechosos; un solo PTZ cubre múltiples ángulos que con cámaras fijas requerirían 2–3 unidades.
- FOV/uso: paneo 360° + zoom óptico permite cubrir toda la entrada con posibilidad de acercamiento para identificación.

Ingreso posterior — 1 panorámica

- Justificación: El ingreso posterior habitualmente necesita visión amplia fija para detectar accesos no autorizados. Una cámara panorámica de 120–180° ofrece vista amplia sin necesidad de movimiento.
- Colocación: montada sobre dintel o poste, altura 3–4 m, orientada hacia el acceso.

Patio de recreo — 1 fisheye

- Justificación: El patio es un área amplia y central; una fisheye 360° colocada en centro o techo alto permite cobertura total desde un punto, minimizando equipos. Con VMS se generan vistas deswarpe (múltiples ventanas).

Preescolares, Maternales B, Maternales A, Lactantes — 1 domo interior por sala

- Justificación: Aulas y salas infantiles requieren cobertura estable y discreta. Un domo interior (FOV ~90°) colocado en esquina cubre la mayor parte del aula.
- Si el aula es muy grande, justificaría 2 cámaras (una por extremo).

Pasillo multiuso (primer piso) — 3 cámaras domo interior (y en general pasillos)

- Justificación: Los pasillos son líneas largas; se coloca una cámara cada cierto tramo para seguimiento continuo. 3 cámaras justificadas si el pasillo es largo o tiene intersecciones.
- Método de cálculo (sin medidas): estimar distancia visual efectiva de cada domo a la resolución requerida y fijar puntos de montaje con 10–20% de solapamiento entre campos de visión.

Sala multiuso — 1 domo interior

- Justificación: Cobertura para multiuso; actividad variable, pero espacio cerrado que un domo puede cubrir.

Recepción/admisión — 1 domo interior

- Justificación: Punto crítico por control de acceso y documentación; domo con 90–110° FOV orientado hacia acceso y mostrador.

Patio jardín — 1 bullet

- Justificación: Bullet para exteriores y mayor alcance; orientada a perímetro/jardín para identificar movimientos a distancia.

Primer piso — Pasillo (3 domos), Maternales A (1), Lactantes (1)

- Justificación: Igual que primer piso: pasillos con varias cámaras por longitud y zonas sensibles (lactantes) con cámara dedicada.

Segundo piso — Terraza (2 domos exterior)

- Justificación: Terrazas más abiertas y con ángulos variables; dos domos exteriores para cubrir ángulos opuestos y evitar puntos muertos, además redundancia en exterior.

c) Reducción de puntos ciegos

Para la reducción de puntos ciegos se tomó en cuenta lo siguiente:

- Solapamiento entre FOV contiguos, esto significa que donde termina el FOV de una cámara comienza la cobertura de la cámara vecina.
- Selección de tipo de cámaras, es un uso combinado de modelos por ejemplo para el patio se usó una cámara bullet +PTZ. entre estas 2

cámaras se complementan para una mayor y mejor cobertura en alcance y zoom.

- Cobertura frente a obstáculos, mediante la verificación in situ se identificó pilares, mobiliario y elementos que generan zonas de sombra.

Tabla 9. Resumen justificativo por cámara

Ubicación	Tipo de cámara	FOV aprox.	Razón y cantidad	Medida para evitar puntos ciegos
Ingreso principal	PTZ (1)	Paneo 360°	Patrullaje dinámico y zoom para identificación	PTZ patrullara la entrada principal
Ingreso posterior	Panorámica (1)	120°-180°	Visión amplia del acceso posterior	Orientación central
Patio de recreo	Fisheye (1)	180°-360°	Cobertura central con deswarpe	Espacio abierto
Preescolares	Domo interior (1)	90°	Cobertura discreta en aula	Montaje en esquina 45°
Maternales A/B	Domo interior (1) cada ambiente	90°	Área sensible, vigilancia constante	Montaje estratégico para cubrir mayor espacio
Pasillo multiuso	Domo – total 3	90°	Longitud y cruces requieren varias cámaras	Colocar cámaras con 15% overlap y en intersecciones
Sala multiuso	Domo (1)	90°	Actividad variable	Orientación central
Recepción	Domo (1)	90°-110°	Control acceso y atención	Vista al mostrador y acceso
Patio jardín	Bullet (1)	60°-90°	Mayor alcance exterior y visibilidad a distancia	Montaje alto y angulado hacia perímetro
Terraza	Domo exterior (2)	90° c/u	Cobertura de ángulos opuestos	Solapamiento y montaje opuestos para eliminar puntos ciegos

7.4 EQUIPAMIENTO DE RED:

En el siguiente cuadro se muestra la cantidad de switch necesario para interconectar los dispositivos, las cámaras IP que estarán ubicadas en los diferentes lugares del centro integral. Es necesario que este switch sea del tipo PoE y además tenga la capacidad de conectarse con enlaces de fibra de 10GBe para poder estar conectado con los demás bloques del campus universitario.

Tabla 10. Cantidad de switch

Bloque	Cámaras	Switch
Planta baja	9	1
Primer piso	5	
Segundo piso	2	
Total cámaras	16	Para la cantidad de cámaras en el bloque se necesita 1 switch de 24 puertos

7.5 DIMENSIONAMIENTO DEL EQUIPO

7.5.1 Dimensionamiento del gabinete (rack)

Se recomienda un gabinete o armario de piso de **24U**, preferiblemente con puerta frontal y trasera con rejilla, cerradura y paneles laterales desmontables.

Motivo: Aunque el número de equipos no es muy grande (1 switch PoE 24 puertos, NVR, UPS, Patch panel y cableado), se recomienda 24U para:

- Permitir organización adecuada (patch panel, gestión de cables)
- Dejar espacio para crecimiento (cámaras nuevas, segundo switch, futuros módulos)
- Facilitar ventilación y colocación de UPS en rack

Tabla 11. Distribución de altura (U) para 16 cámaras

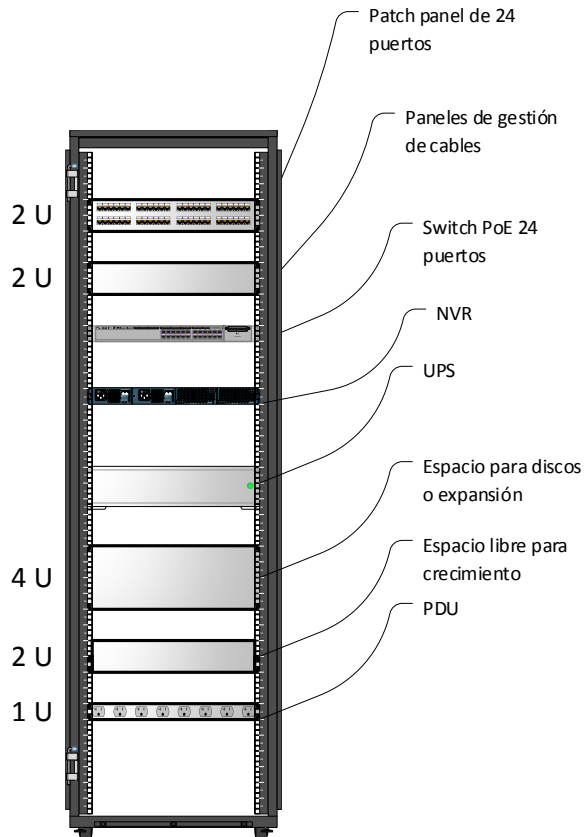
Nº	Equipamiento	U de rack
1	Patch panel 24 puertos	1U
2	Switch PoE 24 puertos	1U o 2U según modelo
3	Paneles de gestión de cables (vertical/horizontal)	1U o 2U
4	NVR/Servidor	2U
5	UPS en rack	2U o 3U
6	Espacio para discos o expansión	0 – 2U
7	Espacio libre para crecimiento y cableado	Mínimo 6U
8	Canales y paneles futuros	2U

Como se muestra en la tabla anterior el **Total aproximado:** 15 – 18 U ocupados en tal caso se recomienda un rack de **24U** para margen y orden.

7.5.2 Diagrama de distribución del equipamiento en Rack

En el siguiente diagrama se muestra la posible ubicación de los componentes que formarían parte en el rack. Como se mencionó anteriormente, se necesitaría un aproximado de 15U a 18U por este motivo se considera un armario de 24U, quedando la posible ubicación en rack de la siguiente manera:

Cuadro diagrama de distribución



Espacio para equipos y accesorios

- **Switch PoE:** debe tener espacio frontal y trasero para ventilación y gestión de cables (entradas SFP si aplica).
- **NVR/Servidor:** ubicar en la parte inferior-media del rack por estabilidad y manejo de cables SATA/SAS.
- **Patch panel:** en la parte superior para facilitar parcheo con los paneles murales y distribución de cables.
- **UPS:** preferible en la parte inferior del rack
- **Bandejas para accesorios** (1U cada una) para herramientas, adaptadores, etc.

Ventilación

- Gabinete con **rejillas frontales y traseras**.
- Para un mejor funcionamiento de los equipos, incluir **ventiladores de extracción** en la parte superior del gabinete (2–4 ventiladores).
- Aconsejar filtros de polvo para ventilación y limpieza periódica.

Normas de organización

- **Cableado estructurado** según **TIA/EIA-568**: color, etiquetado, longitudes de parcheo, pares balanceados y terminaciones RJ-45 correctamente instaladas.
- Uso de **patch panels** y **paneles de gestión de cables** para mantener recorridos menor o igual a 1 m en cara frontal
- Etiquetado en ambos extremos (número de puerto, número de cámara).

7.5.3 Dimensionamiento de UPS

Para calcular el uso de UPS consideraremos *supuestos razonables en base a datos del fabricante*.

Vamos a calcular la potencia y la autonomía en base a equipos previstos y considerados anteriormente: 16 cámaras, switch PoE 24 puertos, NVR y periféricos necesarios en rack.

➤ Cámaras

- 1 x PTZ = 25 W
- 1 x Panorámica = 10 W
- 1 x Fisheye = 8 W
- 1 x Bullet = 8 W
- 12 x Domo = 7 W cada una – $12 \times 7 = 84$
- Total potencia entregada a cámaras = $25+10+8+8+84=135$
- **Switch PoE (consumo propio + PoE)**
- Consumo interno promedio de switch aproximado de 30ª 60 W

- Consideraremos 50 W de consumo interno + entrega PoE equivalente a 135 W – el UPS debe soportar la suma de lo que consume el switch internamente más la potencia que alimenta a las cámaras
- Sin embargo, al dimensionar UPS es práctico contabilizar toda la potencia que sale del UPS, es decir potencia cámaras(135W) + consumo propio del switch (50W)
- NVR/Servidor: 200W (ejemplo servidor con discos)
- Otros periféricos (patch panel, router, etc.):30 W

Potencia total estimada (W)

$$P_{\text{total}} = 135(\text{cámaras}) + 50(\text{switch}) + 200(\text{NVR}) + 30(\text{otros}) = 415 \text{ W}$$

Margen de Holgura

Añadir 20 – 30% de holgura

$$P_{\text{con:margen}} = 415 \times 1.30(\text{margen de holgura}) = 539.5\text{W} \sim \mathbf{540\text{W}}$$

Conversión a VA

- Considerar factor de potencia (PF) del UPS ~0.9

$$\text{VA} = \text{W}/\text{PF} = 540/0.9 \sim \mathbf{600 \text{ VA}}$$

Resultado: Se necesita un UPS con capacidad mínima 600 VA. Por seguridad y futuras expansiones, se recomienda un **UPS de 1000 – 1500 VA**

7.5.4 Elementos de protección eléctrica y física

Protección contra sobretensiones

- **Supresores de sobretensión** instalados en el rack o en la entrada del cuarto de equipos para proteger a todos los equipos que forman parte del gabinete

- También existe la posibilidad de instalar para cada cámara y equipos en exteriores un **protector de sobretensión** si los tramos de cable son largos o propensos a rayos

Puesta a tierra

- Puesta a tierra dedicada para el rack y equipos: barra jabalina con conductor en calibre adecuado según normativa.
- Conectar chasis de racks, carcasas metálicas y paneles a tierra

Canalización y protección

- Se debe usar bandejas porta-cables y tuberías para cables de red y eléctricos, manteniendo separación de cables.
- Ductos y cable canal para tramos expuestos; usara canalización cerrada para fibras ópticas si existen

Seguridad física del gabinete

- Cerraduras con llave en puerta frontal y trasera
- Control de acceso físico al cuarto de equipos (solo personal autorizado)
- Etiquetado de alarmas en gabinete

7.5.5 Climatización

Evaluación de necesidad

- Para un rack con UPS y servidor, si el cuarto **tiene flujo de calor continuo**, se **recomienda aire acondicionado** o al menos ventilación.

Condiciones recomendadas

- La temperatura de operación recomendada para un rack es de 20-24 °C
- La humedad relativa oscila entre el 40-60% donde se debe evitar condensación y estática
- No exponer al polvo o humedad.

7.5.6 Alarmas e integración con el VMS (Video Management System)

Tipos de alarmas recomendadas

Existen muchos tipos de alarmas, pero las más recomendadas para una complementación al sistema de videovigilancia son las siguientes:

- a) **Detección de humo/incendio:** Detectores de humo en cuartos de equipos y en zonas críticas para una detección de incendio a tiempo
- b) **Intrusión:** Sensores de movimiento en entradas y puertas, sensores de apertura en puerta y ventanas de acceso al centro integral.

7.5.7 Integración con el software de videovigilancia (VMS)

Una de las funcionalidades de los sistemas de videovigilancia son las alertas que existen ante determinadas situaciones que son detectadas por el sistema de alarmas, esto quiere decir que, si bien existe un incendio o una intrusión, la alarma alerta al sistema de videovigilancia y de esta manera se activa la cámara más cercana al evento ocurrido. La integración del sistema de alarmas con el de vigilancia puede dar las siguientes situaciones:

- Generar alerta visual y sonora en la central de monitoreo (pantalla, bocina).
- Marcar en la línea de tiempo la grabación como evento crítico.
- Enviar notificaciones por correo/SMS a responsables de seguridad.
- Posibilidad de activar PTZ para hacer auto tracking hacia el evento o presets de posiciones críticas

Para mayor comprensión se ejemplifica mediante un evento:

Detector de apertura y/o movimiento en ingreso

Paso 1 – VMS recibe señal

Paso 2 – en sala de monitoreo suena alarma

Paso 3 – VMS muestra en pantalla la cámara del ingreso y activa grabación a 25 fps

Paso 4 – operador de monitoreo puede tomar control de PTZ

Paso 5 – VMS genera Acta de evento y exporta clip de video si se confirma incidente.

7.6 ARQUITECTURA DE ALMACENAMIENTO

7.6.1 Dimensionamiento del ancho de banda para tráfico.

El ancho de banda necesario viene definido en función de la cantidad de cámaras que se encuentra instalado en el centro integral. Se considera un promedio de 2 Mbps de consumo de ancho de banda por cámara de vigilancia. El bitrate en un códec de cámara de vigilancia es la cantidad de datos (bits) que la cámara transmite o graba por segundo en el video.

Se mide en bits por segundo (bps), kilobits por segundo (kbps) o megabits por segundo (Mbps).

Ancho de Banda total

Bitrate por cámara = 2 Mbps

Numero de cámaras = 16

$$\text{Ancho de Banda Total} = 2 \text{ Mbps} * 16 = 32 \text{ Mbps}$$

7.6.2 Dimensionamiento cantidad de almacenamiento

El almacenamiento, dependiendo el número de cámaras en el bloque del centro integral será calculado considerando el consumo de ancho de banda necesario y utilizando la tecnología de compresión H.264 ya que no todos los modelos en el actual sistema de Seguridad y Vigilancia vigente contemplan el protocolo y algoritmo de compresión de video H.265. por lo que se considera para el cálculo (el peor caso), el uso de la tecnología H.264 con una actividad alta y por el tiempo de 18 horas ya que en horario nocturno el bloque se encuentra cerrado. Para este cálculo se debe de usar el factor de actividad, considerando que el bloque del centro integral está en el campus

universitario de el Tejar el cual tiene una gran población de estudiantes por este caso se usa un factor de actividad de 60%

$$\text{Espacio en Disco TB} = \frac{\text{Ancho de Banda} \times 3.600 \text{ seg} \times 24 \text{ horas} \times 30 \text{ dias}}{1.024 \times 1.024 \times (\text{porcentaje de uso} \times 100)}$$

$$\text{Espacio en Disco TB} = \frac{32 \text{ Mbps} \times 3.600 \text{ seg} \times 24 \text{ horas} \times 30 \text{ dias}}{1.024 \times 1.024 \times (60 \times 100)}$$

Espacio en Disco TB = 1.32 ~ 2TB

Se puede observar que la capacidad de almacenamiento es de por lo menos 2 TB para un histórico de 30 días, pasado este tiempo el sistema automáticamente debe sobrescribir sobre videos ya almacenados.

Selección de NVR (Grabador de Video en Red)

El NVR necesario a instalar de acuerdo al cálculo de almacenamiento no requiere de gran amplitud, suficiente con un NVR que cuente 2 TB de almacenamiento para poder guardar las grabaciones por 30 días.

7.7 DEFINICION DEL SOFTWARE DE MONITOREO

El software de monitoreo viene a ser un componente fundamental dentro del diseño del sistema de videovigilancia, ya que permite la administración, supervisión y control eficiente de las imágenes captadas por las cámaras instaladas en el Centro Integral.

Para el diseño propuesto, el software de monitoreo deberá ser compatible con **sistemas de videovigilancia IP**, soportar protocolos estándar como **ONVIF**, y permitir la integración con grabadores de video en red (NVR), garantizando la interoperabilidad entre dispositivos de diferentes fabricantes en caso de tener cámaras de diferentes marcas.

Entre las principales funciones que debe contemplar el software es, la visualización en tiempo real de las cámaras, la grabación continua, así como la reproducción de grabaciones para la revisión de incidentes u otras situaciones.

En cuanto a la seguridad del sistema, el software deberá incorporar mecanismos de autenticación y control de acceso, permitir la creación de perfiles de usuarios con diferentes niveles de permisos, así como el registro de actividades y accesos al sistema, con el fin de garantizar el uso responsable y confidencial de la información.

Finalmente, el software seleccionado deberá ser **escalable y flexible**, permitiendo la incorporación de nuevas cámaras o la integración futura con otros sistemas de videovigilancia o sistemas de alarmas.

Selección de VMS (Video Management Software):

Se evaluarán opciones de software de monitoreo y gestión, ya sean propietarias del fabricante del NVR o soluciones de terceros.

Funcionalidades del Software:

- **Monitoreo en Tiempo Real:** Visualización simultánea de todas las cámaras.
- **Notificaciones de Eventos:** Alertas automáticas por detección de movimiento, línea virtual cruzada o manipulación de la cámara.
- **Gestión de Usuarios:** Creación de perfiles con permisos de acceso limitados para el personal.