

CAPÍTULO I

GENERALIDADES

Capítulo 1: Generalidades

I.1 Presentación del proyecto

Título del Proyecto: Mejorar la seguridad infraestructural y personal mediante el diseño de una red de cámaras de seguridad para el módulo 2 de la facultad de ciencias integradas de la UAJMS en la ciudad de Bermejo.

Nombre del Postulante: Juan Marcelo Navarro Sanchez.

Celular: 75112831.

Carrera/Unidad: Departamento de Informática y Sistemas.

Facultad: Ciencias y Tecnología.

Institución/Centro Cooperante: Universidad autónoma Juan Misael Saracho ciudad de Bermejo.

Duración del Proyecto: 8 meses.

Área/línea de investigación priorizada: Redes.

I.2 Perfil de proyecto

I.2.1 Introducción

La seguridad hoy en día cubre un papel muy importante en cualquier institución, empresa, supermercados, etc. En cualquier sitio donde se tengan que salvaguardar materiales de valor o brindar por la integridad de una persona.

Entre las herramientas más importantes de seguridad tenemos las cámaras estas son una opción cumplidora en todos los aspectos ya que se asegura de poder monitorear en vivo o para su posterior revisión todo lo que ocurre en las zonas cubiertas por las mismas, de forma estática o remota.

En la universidad Autónoma Juan Misael Saracho en la provincia de Bermejo se abrieron nuevos bloques estos mismos al ser nuevos no tiene designado, ni diseñado algún tipo de sistema de seguridad.

En base a esto se vio la necesidad de diseñar un sistema de cámaras de seguridad completo, el cual cubra efectivamente el bloque y cubra todos los parámetros que se requieran, Lo cual el presente proyecto pretende desarrollar en uno de los bloques nuevos, el cual es modulo dos de la facultad de ciencia integradas.

I.2.2 Justificación del Proyecto

El alto índice de delincuencia y la falta de seguridad, crea la necesidad de poseer un sistema de seguridad el mismo que permita observar en tiempo real e incluso guardar grabaciones para su posterior revisión.

El sistema ayuda en varios aspectos uno de ellos es a controlar el ingreso de personal no autorizado a lugares restringidos, así como también permite inspeccionar el trabajo del personal, este indirectamente hace que también el mismo labore de una manera más eficaz.

Todas las personas que ingresen a los bloques serán vigiladas de manera discreta y sin que la misma incomode a los estudiantes, asegurando la satisfacción de los estudiantes y salvaguardando los bienes de institución ayudando a reducir pérdidas.

I.2.2.1 Justificación Tecnológica:

En cuanto a la tecnología existen la necesaria esta misma trae bastantes opciones que podrían cubrir fácilmente los requisitos que se plantean, así como modelos de cámara específicos para cada bloque o sector según la necesidad del mismo; así también la manera de administrarlos ya sea con la conectividad o el monitoreo el cual hasta puede ser remoto. Para ello se diseñará una red de cámaras de seguridad esta cubrirá el bloque nuevo.

I.2.2.2 Justificación Económica:

Para el presente proyecto se necesitará de una fuerte inversión, pero esta misma además de mejorar la seguridad y la imagen de la universidad Autónoma Juan Misael Saracho, se provee de seguridad a los equipos y de este modo evitar o documentar robos, pérdidas de equipo, vandalismo, etc. Que afectarían de manera directa sobre la economía de la institución.

I.2.2.3 Justificación Social:

El presente proyecto brindara de seguridad a cualquier individuo ya sea personas, estudiante o civil que circulen por los bloques cubiertos. Además de generar vacantes de trabajo.

I.2.3 Planteamiento del problema

La Universidad Autónoma Juan Misael Saracho de la provincia de Bermejo llevo a cabo un proyecto el cual, se crearán nuevos bloques por motivos de capacidad, ubicación, estado infraestructural, etc. y estas en cuanto a seguridad no cuentan con un diseño establecido. Además, una universidad al ser una institución bastante concurrida y este bloque al no contar con un sistema de seguridad es susceptible a hurtos, daños a la infraestructura e incluso disputas sin documentarse ya que no existe un control de entrada y salida.

De esta forma se identificó el problema principal, el cual sería: Deficiencia en la seguridad infraestructural y personal del módulo 2 de la facultad de ciencias integradas de la UAJMS de la ciudad de Bermejo.

Para profundizar y ejemplificar de mejor manera los problemas y objetivos se decidió crear sus respectivos árboles de problemas y objetivos.

I.2.4 Árbol de problemas

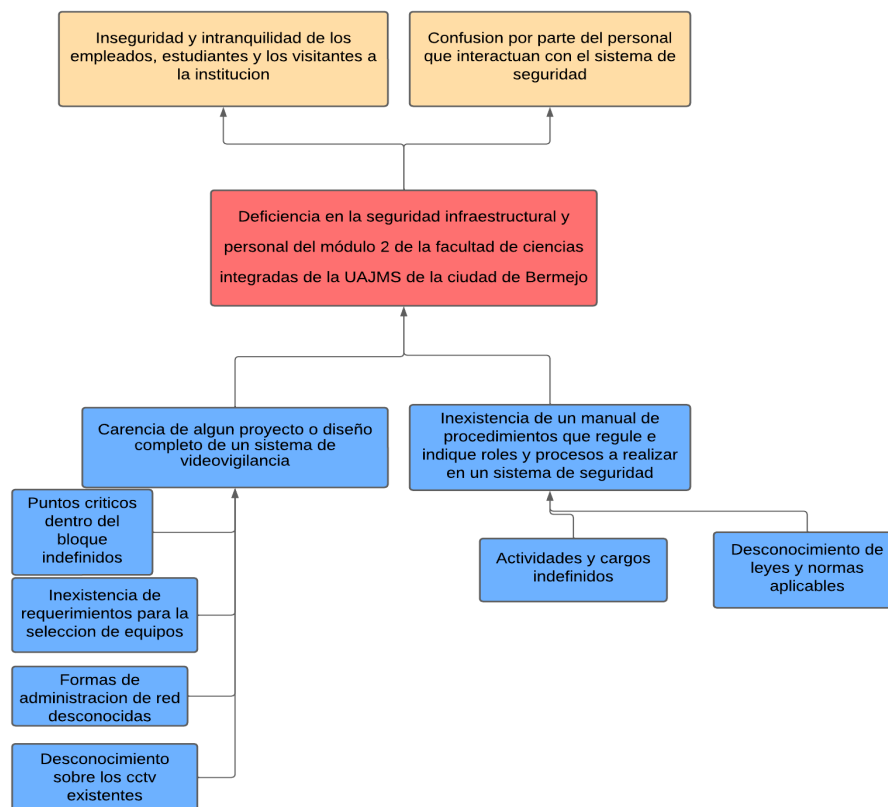


Figura 1. Árbol de problemas

I.2.5 Árbol de objetivos

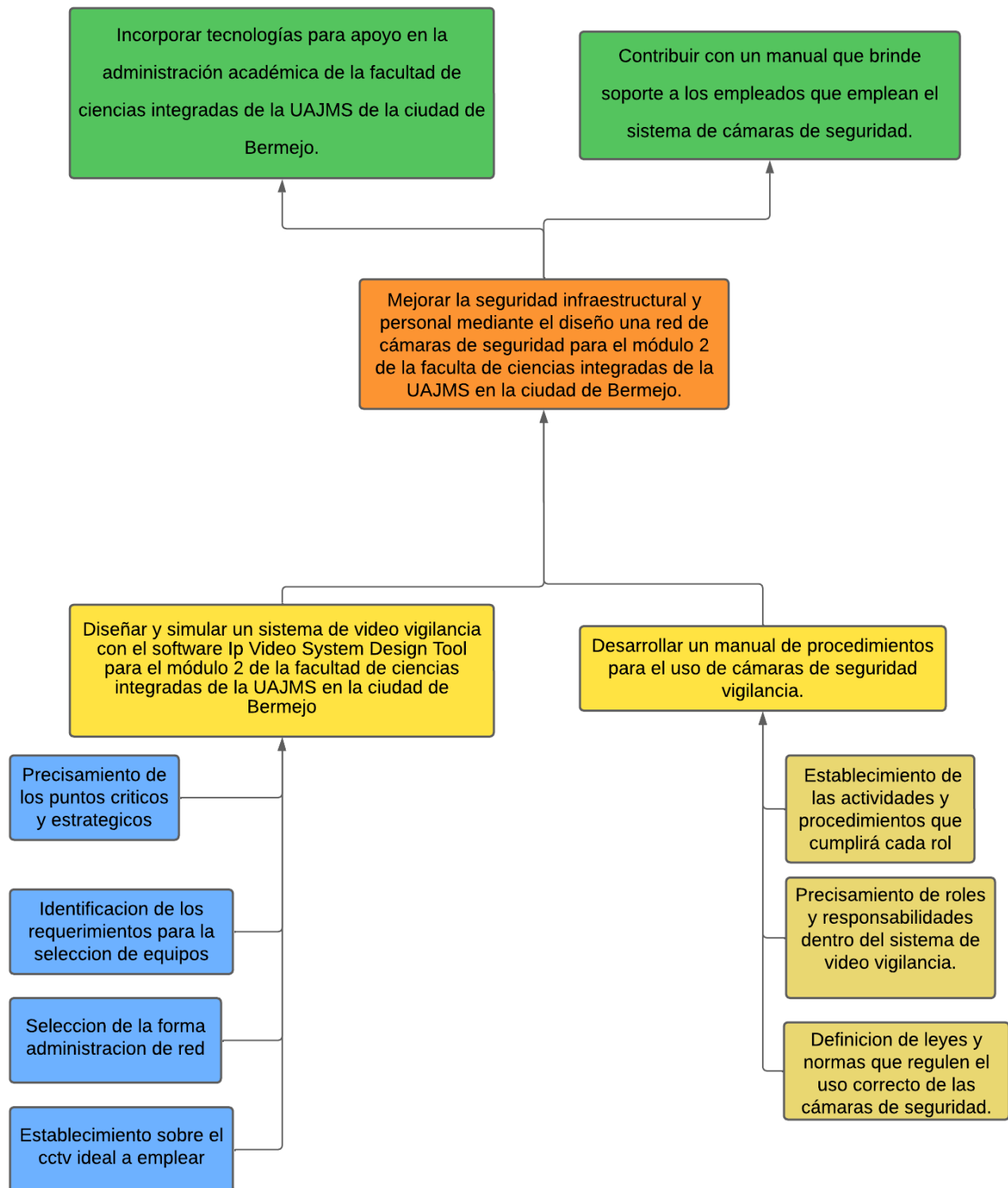


Figura 2. Árbol de objetivos

I.3 Objetivos

I.3.1 Objetivo General

Mejorar la seguridad infraestructural y personal mediante el diseño una red de cámaras de seguridad para el módulo 2 de la facultad de ciencias integradas de la UAJMS en la ciudad de Bermejo.

I.3.2 Objetivos Específicos

- Diseñar y simular un sistema de video vigilancia con el software Ip Video System Design Tool para el módulo 2 de la facultad de ciencias integradas de la UAJMS en la ciudad de Bermejo
- Desarrollar un manual de procedimientos para el uso de cámaras de seguridad y vigilancia.

I.3.3 Metodología de desarrollo del proyecto (detallar las etapas, métodos y técnicas)

I.3.3.1 Top-down

Para el desarrollo de este proyecto se aplicó la metodología top down el cual divide el problema principal en subproblemas que luego se desarrollan para luego conectarlos y así dar solución al problema principal.

Esta metodología consta de 6 fases las cuales serían:

- **Fase 1: Análisis de los requerimientos.**
 - Analizar metas del negocio.
 - Analizar metas técnicas.
 - Analizar red existente.
 - Analizar tráfico existente
- **Fase 2: Desarrollar diseño lógico.**
 - Diseñar topología de red.
 - Diseñar modelos de direccionamiento y hostnames.
 - Seleccionar protocolos para Switching y Routing.
 - Desarrollar estrategias de seguridad.
 - Desarrollar estrategias de administración de red.

- **Fase 3: Desarrollar diseño físico.**
 - Seleccionar tecnologías y dispositivos para redes de campus.
 - Seleccionar tecnologías y dispositivos para redes empresariales.
- **Fase 4: Aprobar, optimizar y documentar diseño.**
 - Probar el diseño de red.
 - Optimizar el diseño de red.
 - Documentar el diseño.
- **Fase 5: Implementar y probar la red.**
 - Realizar cronograma de implementación.
 - Implementación del diseño de red (final).
 - Realizar pila de pruebas.
- **Fase 6: Monitorear y optimizar la red.**
 - Operación de la red en producción.
 - Monitoreo de la red.
 - Optimización de la red.

Cabe mencionar que se desarrollara esta metodología hasta la fase 4 al tratarse de un diseño con posibilidad de implementación.

I.3.3.2 Métodos

Método Deductivo:

Este método se aplica en varias partes de la investigación, como por ejemplo al analizar la información recolectada, se obtuvieron conclusiones en base a las pruebas de cámaras realizadas y Se usó al realizar un desarrollo con fundamentos científicos y teóricos para así obtener resultados validables y efectivos, Para así de esta manera conseguir conclusiones válidas a base de datos concretos.

Método Experimental:

Este método se aplicó al desarrollar pruebas de las cámaras para seleccionar de cual se realizará la implementación con el sistema. También se aplicó en determinar la calidad de grabación de las cámaras para ver el espacio y ancho de banda a usar.

I.3.3.3 Técnicas

Las técnicas que se utilizaron para el desarrollo de la investigación fueron las siguientes:

Técnicas indirectas:

Al realizarse el uso de distintas fuentes como páginas web, textos, manuales, etc. Estas mismas para recabar información.

Técnica Experimental:

Se realiza el análisis experimental para los testeos de cámaras, ancho de banda y espacio de almacenamiento. Esto para obtener los datos que serán analizados e interpretados.

Técnica documental:

Atraves de los tipos de investigación usados, como información recabada como características físicas del sistema como medidas de seguridad, etc. Investigación bibliográfica en la recopilación de redes o sistemas similares que brinden aportes o puntos de vista distintos al empleado.

I.3.4 Población y muestra

I.3.4.1 Población

- La universidad “Juan Misael Saracho de la ciudad de Bermejo.
- Personal labora en la universidad.
- Autoridades, docentes y estudiantes que transiten la universidad.
- Generalmente se podrá instalar este sistema de video-vigilancia en cualquier establecimiento que requiera de protección y seguridad.

I.3.4.2 Muestra

El sistema será ubicado en el interior de la UAJMS de Bermejo en el módulo 2 de la facultad de ciencias integradas.

I.3.5 Descripción de la propuesta

Para el presente proyecto de grado se pretende desarrollar un diseño de red de cámaras de seguridad a uno de los bloques nuevos, el cual es el módulo dos de la facultad ciencia integradas de la UAJMS ubicada en bermejo los cuales al ser relativamente recientes no cuentan con algún diseño previo en cuanto a seguridad.

Este bloque consta de tres plantas en la cual está ubicado el auditorio, en el mismo se ubicarán cámaras de seguridad para interior, exterior. Las necesarias para cubrir eficientemente el bloque y reforzar la seguridad de los materiales tanto como de los docentes y estudiantes.

Al tener un bloque de tres plantas y se propone usar tres switches administrables, uno en cada planta cada uno de 24 puertos, dos se conectarán a la de la primera planta donde se realizará un backbone con topología tipo estrella. De este switch de la primera planta se conectarán al servidor o router que dará servicio al sistema completo. El nvr estará ubicado en el segundo piso donde estará el cuarto de control.

El desarrollo del diseño se determinará teniendo en cuenta los siguientes requerimientos técnicos:

- **Mantenibilidad:** La red debe de ser fácil de mantener y actualizar.
- **Escalabilidad:** El diseño de la red debe de ser adaptable a cambios, estos cambios pueden ser como expansión de la red, adición de nuevos dispositivos, etc.
- **Calidad de Servicios:** La red diseñada tiene que posibilitar priorizar los servicios y aplicaciones.
- **Seguridad:** El diseño debe de cubrir la seguridad tanto física como lógica.
- **Administración:** En base al diseño de la red se obtiene una administración centralizada.

El cumplimiento de estos requerimientos técnicos se medirá en base a las siguientes actividades:

- Investigar y documentar los tipos de sistemas de video vigilancia existentes.
- Investigar y documentar los componentes de un sistema cctv.
- Determinar el tipo de sistema de video vigilancia a usar.
- Analizar y determinar el tipo, modelo y cantidad de cámaras necesarias para cubrir efectivamente el bloque.

- Documentar las especificaciones técnicas de cada equipo seleccionado.
- Realizar la estimación de cuantos puertos de cada switch ocuparan las cámaras y cuantos puertos habrá que reservar tomando en cuenta la escalabilidad del proyecto.
- Investigar y documentar tecnologías y formas que brinden facilidad y optimización en cuanto a una administración de red.
- Investigar y definir la topología a emplear.
- Determinar qué tipo de alimentación se utilizará.
- Definir el software de administración del sistema de video vigilancia
- Examinar y precisar lo necesario en cuanto a ancho de banda, espacio requerido y tiempo de grabación de las cámaras.
- Analizar y determinar los puntos críticos dentro del bloque para la ubicación de las cámaras.
- Precisar las ubicaciones estratégicas de los equipos además de las estaciones de cuarto de equipos y monitoreo.

Por otra parte, se desarrollará un manual de procedimientos para el uso de cámaras de seguridad y vigilancia. Esto a partir de las siguientes actividades:

- Investigar leyes y normas que regulen el uso correcto de las cámaras de seguridad.
- Determinar roles y responsabilidades dentro del sistema de video vigilancia.
- Determinar las actividades y procedimientos que cumplirá cada rol mediante diagramas de procesos.

I.3.6 Beneficiarios

I.3.6.1 Beneficiarios Directos

Los beneficiarios directos son los universitarios, docentes y el personal al estar cubiertos directamente por la red de seguridad. Además, también la universidad al obtener seguridad sobre su infraestructura y equipos, al estar cubiertos por la red de cámaras de seguridad.

I.3.6.2 Beneficiarios indirectos

Algunos de los beneficiarios indirectos serían los civiles o autoridades que recurran al bloque, los empleados contratados debido a las vacantes de empleo que se crearían, la universidad misma al elevarse su estatus al tener una red de seguridad.

I.3.7 Resultados esperados

Se espera una red totalmente escalable y adaptable a cambios.

Una red optima y una simulación completa con todos los parámetros cubiertos y validados mediante reportes del software.

Personal satisfecho en cuanto al diseño nuevo propuesto.

Se espera que el sistema de video vigilancia propuesto satisfaga y asegure al personal que lleva a cabo actividades en el bloque como así también a los visitantes.

Se espera que con el manual de procedimientos el personal sea capaz de identificar su rol, así como también llevar a cabo los procedimientos asignados.

I.3.8 Cronograma de Actividades

N. °	Actividad	N.º días	Fecha inicio	Fecha Finalización	M 1	M 2	M 3	M 4	M 5	M 6	M 7	M 8
1	Fase 1: Análisis de los requerimientos. ✓ Analizar metas del negocio ✓ Analizar metas técnicas ✓ Analizar red existente ✓ Analizar tráfico existente	41	10/03/23	20/04/23								
2	Fase 2: Desarrollar diseño lógico. ✓ Diseñar topología de red ✓ Diseñar modelos de direccionamiento y hostnames ✓ Seleccionar protocolos para Switching y Routing	80	20/04/23	09/07/23								

	✓ Desarrollar estrategias de seguridad											
3	Fase 3: Desarrollar diseño físico. ✓ Seleccionar tecnologías y dispositivos para redes de campus ✓ Seleccionar tecnologías y dispositivos para redes empresariales	59	09/07/23	06/09/23								
2	Fase 4: Aprobar, optimizar y documentar diseño. ✓ Probar el diseño de red ✓ Optimizar el diseño de red ✓ Documentar el diseño Entrega del trabajo al tutor para revisión.	33	06/09/23	9/10/23								

	Realizar correcciones. Entrega del trabajo final.											
	Componente 2: Manual de procedimientos para el uso de cámaras de seguridad y vigilancia - Investigar leyes y normas que regulen el uso correcto de las cámaras de seguridad. - Determinar roles y responsabilidades dentro del sistema de video vigilancia. Determinar las actividades y procedimientos que cumplirá cada rol mediante diagramas de procesos.	30	09/10/23	9/11/23								

Tabla 1. Cronograma de actividades

I.3.9 Presupuesto general

N.º	Finalidad			
	Materiales			
#	Recurso	Cantidad	Precio	TOTAL (Bs)
1	Switch	3	2717,34	8152,02
2	NVR	1	4341.41	4341.41
3	Camara interior tipo 1	8	311,02	2488,16
4	Camara interior tipo 2	12	414,02	4968,24
5	Camara exterior	1	345,66	345,66
6	Camara ojo de pez	6	1382,55	8295,30
7	Disco duro	2	611,96	1264,78
8	Cableado estructurado	869,57 (m)	3	2608,71
	TOTAL			32323,4 Bs
N.º	Finalidad			
	Mano de obra			
#	Recurso	Precio	Cantidad	TOTAL (Bs)
8	Por camara	300	27	8,100
9	Por nvr y switch	380	3	1,200
	TOTAL			9,300
N.º	Finalidad			
	Consultados			
#	Recurso	Aporte Institucional	Cantidad	TOTAL (Bs)
9	Estipendio por desarrollo	1,800(bs)	1	1,800
	TOTAL			1,800

Tabla 2. Presupuesto general

I.4 Marco Teórico

I.4.1 Antecedentes

En el ámbito internacional se consideraron el proyecto de grado “Diseño de un sistema de video-vigilancia para el barrio chaupimolino de pifo”, en este trabajo se tuvo distintos ambientes y se determinaron las opciones más factibles en base a las necesidades de la sociedad teniendo en cuenta el factor económico y social, de esta manera presenta una combinación de tecnologías análogas y ip totalmente funcional y adaptable. (Sarango & Ipiales, 2020)

Otro proyecto en el ámbito nacional que se consideró es “Diseño e implementación de un sistema de video-vigilancia para el salón de eventos medallón”, en este trabajo se plantean escenarios o planos donde se realizan pruebas con las cámaras teniendo en cuenta todos los criterios de un sistema cctv, también se configura el software del nvr el cual muestra numerosas opciones a tomar en cuenta a configurar. En base al análisis se obtuvo un sistema de video-vigilancia eficiente y económico. (Laime, 2019)

I.4.2 Red de cámaras de seguridad

I.4.2.1 Definición

Las cámaras de seguridad o vigilancia constituyen un sistema de seguridad que consiste en realizar vigilancia a través de cámaras de video en diferentes ambientes. Esta tecnología de video-vigilancia es especialmente útil para identificar intrusos o cualquier persona que realice alguna actividad indebida que ponga en riesgo la integridad de un lugar o individuo. El circuito está compuesto por una o varias cámaras de vigilancia que se interconectan a monitores de vídeo o televisores, los cuales reproducen las imágenes captadas por las cámaras. (elcajondeardu, s.f.)

I.4.3 Sistemas de red seguridad existentes

I.4.3.1 Sistemas CCTV

I.4.3.1.1 Definición

(tecnoseguro, s.f.) apunta a que un Circuito Cerrado de Televisión o CCTV es la combinación de varios equipos que, junto con la infraestructura adecuada para su interconexión, permite

visualizar y tener registro en video de las escenas o situaciones que ocurren en un determinado sitio, con el objetivo de minimizar los riesgos ante situaciones de seguridad.

De acuerdo a (tecnoseguro, s.f.) el uso que le podemos dar se divide en dos grupos de aplicaciones:

1. **Supervisión:** es cuando el CCTV implica la implementación de una central de monitoreo que es operada por una o varias personas en tiempo real. Por ejemplo, un CCTV de un centro comercial o de un casino, en donde el personal encargado de monitorear hace uso de las imágenes para alertar, notificar o apoyar a personal en el sitio sobre situaciones anormales. Su objetivo fundamental es mantener la seguridad del sitio.
2. **Verificación:** en este caso el CCTV se usa para validar hechos ya ocurridos, por lo general situaciones extraordinarias que requieren de una verificación después del evento, bien sea para tomar correctivos, hacer evidente una falla de cualquier proceso o tomar las acciones que permitan mitigar el riesgo de materialización de los sucesos.

I.4.3.1.2 Componentes de un CCTV

Según (tecnoseguro, s.f.) indica que todo sistema de CCTV conlleva la instalación de componentes y productos como: cámaras de seguridad, equipos o software de administración y almacenamiento de video (DVR o NVR), equipos de visualización, de alimentación de energía, infraestructura para la interconexión de equipos, y por último la intervención de los usuarios. En detalle son:

1. **Cámaras de seguridad:** son los equipos de generación de señal de video, pueden ser de diferentes tipos según el sitio de aplicación, su función y las especificaciones técnicas.
2. **Sistema de administración y grabación:** se trata de hardware y software para hacer la gestión y administración de las señales de video, así como el almacenamiento de información durante un determinado tiempo.

3. **Equipos de alimentación o suministro de energía:** pueden ser uno por cada cámara o un solo equipo para varias cámaras, según su consumo de energía. Por lo general de 12 o 24 VDC, sin embargo, dependiendo de la tecnología del sistema, varios fabricantes especifican sus equipos para ser usados solo con fuentes o Inyectores PoE (alimentación sobre red Ethernet).

A su vez, estos son soportados por un equipo común a todo el sistema, por lo general es una UPS (Unidad de Suministro de Energía Ininterrumpida) que cumple la función de regulación, protección y soporte de energía por un espacio tiempo en ausencia del fluido eléctrico convencional.

4. **Sistema de visualización:** son los equipos, por lo general monitores de visualización de video, en donde se despliegan las imágenes provenientes de las cámaras.
5. **Infraestructura:** se trata de elementos como cableado, ductos y conectores necesarios y especificados por los fabricantes para la correcta transmisión de las señales de video cuando el medio de transmisión es físico; también puede ser inalámbrico, por medio de señales de radio, en cuyo caso se usan otros elementos como radios, antenas, etc.

Según los alcances y especificaciones de cada implementación se usa cable coaxial o cable par trenzado o cable UTP, según la tecnología del sistema.

6. **Usuario:** es el factor humano, muy importante en cualquier sistema de CCTV, pues son quienes harán uso del sistema y, por lo tanto, deben conocer su operación y administración, desde el simple uso de una aplicación en un teléfono móvil, hasta el funcionamiento de una central de monitoreo compleja. El factor humano en estos proyectos es muy importante y debe asegurarse que los usuarios conozcan y sepan utilizar los sistemas que se implementan.

I.4.3.1.3 Tipos de cctv existentes

Según (tecnoseguro, s.f.) no indican que existen dos tipos de CCTV según la tecnología con la que se implemente el sistema: analógica y digital, este último llamado de forma común CCTV IP, por usar el protocolo TCP/IP para la transmisión de información de la señal de video. Incluso aunque las cámaras analógicas y las cámaras IP tienen el mismo objetivo, son algo diferentes en su

funcionamiento pues emplean un método distinto para transmitir la señal de video y aplican un proceso diferente de codificación de las imágenes.

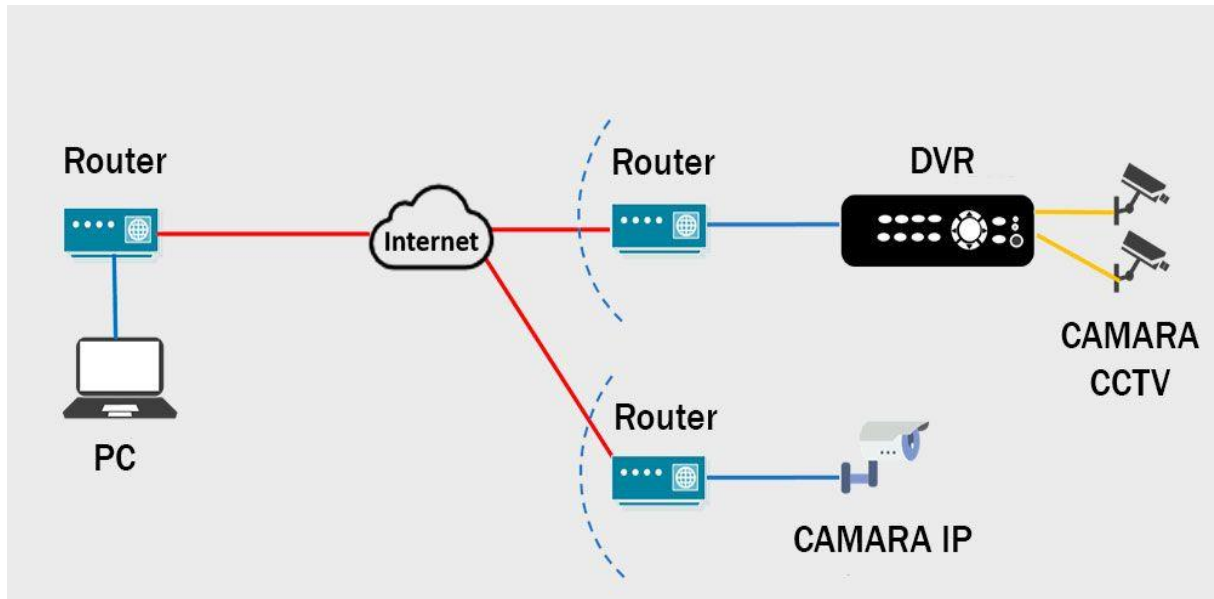


Figura 3. Cctv existentes

I.4.3.1.3.1 Sistemas analógicos

(tecnoseguro, s.f.) indica que la señal de video analógica se produce tras convertir los cambios de la intensidad de la luz en señales eléctricas. En el interior de la cámara se hace un proceso de digitalización, pero antes de transmitirla la convierte, de nuevo, en imagen análoga, para que sea recibida por un monitor o grabador de video por medio de un conductor físico.

Los puertos de DVR indicaran cuantas cámaras pueden ser instaladas, estos puertos estarán conectados mediante cable coaxial a las cámaras. Existen otros métodos para la transmisión de video, pero estos estando quedando obsoletos.



Figura 4. Esquema básico de un cctv analógico

I.4.3.1.3.2 Sistemas Digitales IP

Para este tipo de sistemas según (tecnoseguro, s.f.) las cámaras IP captan los cambios de la intensidad de la luz en señales eléctricas, después las digitaliza, las codifica sobre protocolo de redes Ethernet TCP/IP y las envía hacia el sistema de grabación en red NVR, o al sistema de administración de video.

Estas cámaras ip pueden ser alimentadas mediante tecnología PoE a través del cable utp, pero este cableado está limitado a 100 metros.

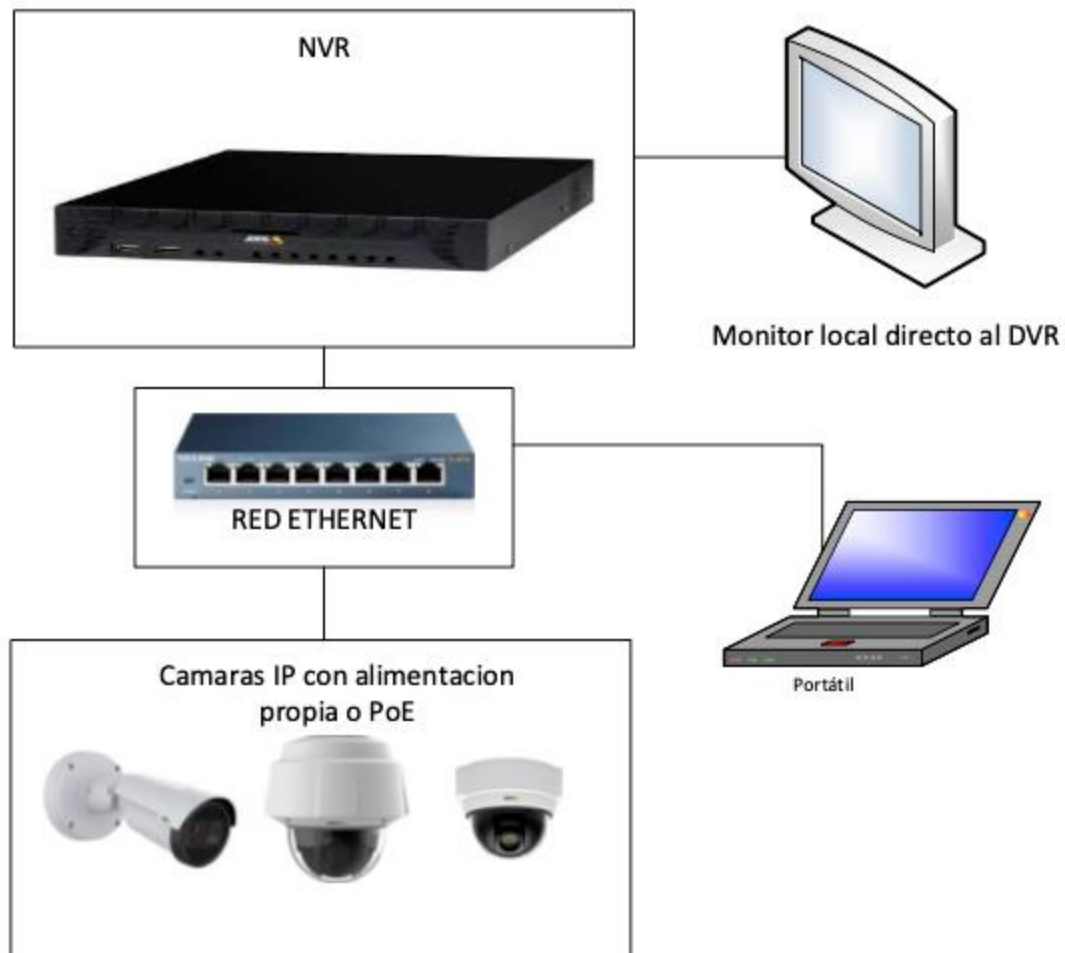


Figura 5. Esquema básico de un cctv ip

Los sistemas de video-vigilancia IP ofrecen resoluciones de video que, por lo general, son superiores a las de los sistemas de analógicos, por ello pueden ofrecen una mejor calidad de video.

También en este tipo de sistemas hay mayores posibilidades de encontrar cámaras inteligentes que incorporen funciones de análisis de contenido de video, sin embargo, hay factores que afectan el buen funcionamiento de estos sistemas: el medio de transmisión, la capacidad y velocidad de transmisión de datos a través de la red y la latencia. (tecnoseguro, s.f.)

I.4.3.1.3.3 Sistema CCTV Analógico/IP

Estos son sistemas donde básicamente existe instalado un sistema analógico y en el mismo se integra el sistema basado en tecnología ip ya que esta es adaptable incluso a sistemas analógicos.

I.4.4 Características de un sistema de video vigilancia

A continuación, según (senstar, s.f.) se detallan las características de un sistema de video-vigilancia:

1. **Imágenes de alta resolución:** se acabaron las imágenes granuladas y difíciles de descifrar. Las cámaras de vigilancia actuales ofrecen imágenes de alta definición, lo que proporciona imágenes nítidas que ayudan a una identificación precisa y una supervisión eficaz.
2. **Capacidad de visión nocturna:** la oscuridad ya no ocultará las actividades ilícitas. Gracias a la capacidad de visión nocturna, estos sistemas mantienen su mirada vigilante incluso en condiciones de poca luz, lo que garantiza una protección permanente.
3. **Detección de movimiento:** al añadir una capa adicional de protección, la detección de movimiento puede alertarle de cualquier movimiento sospechoso en sus instalaciones, respondiendo de forma proactiva a posibles amenazas.
4. **Amplio campo de visión:** diga adiós a los puntos ciegos. Equipadas con objetivos gran angular, estas cámaras de vigilancia pueden cubrir áreas más amplias, minimizando el número de cámaras necesarias y maximizando su seguridad.
5. **Acceso y control remotos:** gestione su seguridad sobre la marcha. Con el acceso remoto, puede ver imágenes en directo o grabadas desde cualquier dispositivo con acceso a Internet.
6. **Diseño resistente a la intemperie:** las cámaras de vigilancia resistentes, robustas y resistentes a la intemperie pueden soportar condiciones meteorológicas adversas, garantizando una seguridad ininterrumpida.

7. **Alertas de manipulación:** vaya un paso por delante de los vándalos. Las cámaras con alertas anti manipulación pueden notificarle si están siendo interferidas, dándole la oportunidad de actuar con prontitud.
8. **Integración con otros sistemas:** aproveche toda la potencia de su sistema de seguridad. Muchos sistemas de vigilancia pueden integrarse perfectamente con sus sistemas de alarma, control de acceso, etc., ofreciendo una solución de seguridad completa.
9. **Escalabilidad:** a medida que crecen sus instalaciones, también lo hace su sistema de vigilancia. La mayoría de los sistemas pueden acomodar fácilmente cámaras adicionales, permitiendo que sus medidas de seguridad se amplíen en consecuencia.
10. **Análisis basados en inteligencia artificial:** aproveche la inteligencia artificial para mejorar la seguridad. Los sistemas avanzados ofrecen funciones como el reconocimiento facial, el seguimiento de objetos y el análisis del comportamiento, lo que lleva sus capacidades de vigilancia al siguiente nivel.

I.4.5 Aplicaciones de los Sistemas de Video Vigilancia

Las aplicaciones de estos sistemas son muy variadas (Anish, 2023) define que para una comprensión fundamental de la video-vigilancia y sus tecnologías asociadas se debe de profundizar en sus distintas aplicaciones y facetas. Estas son:

1. **Seguridad empresarial:** una de las aplicaciones más comunes de la video-vigilancia es la seguridad empresarial. Las empresas, tanto grandes como pequeñas, utilizan la video-vigilancia para disuadir el crimen, monitorear la actividad de los empleados y recopilar evidencia en caso de disputas o incidentes. Esto no solo ayuda a prevenir robos o vandalismo, sino que también ayuda a garantizar la seguridad de los empleados y el cumplimiento de las políticas de la empresa.
2. **Seguridad del hogar:** la seguridad residencial es otra aplicación importante de la video-vigilancia. Los propietarios de viviendas utilizan cámaras de vigilancia para monitorear sus propiedades, disuadir a posibles intrusos y registrar eventos. Los sistemas de vigilancia modernos incluso permiten a los propietarios monitorear sus propiedades de forma remota utilizando teléfonos inteligentes o computadoras.

3. **Monitoreo de tráfico:** la video-vigilancia juega un papel fundamental en la gestión y el control del tráfico. Las cámaras de tráfico capturan imágenes en tiempo real de carreteras e intersecciones, lo que ayuda a los centros de control de tráfico a controlar el flujo de tráfico, detectar incidentes y gestionar la congestión.
4. **Prevención de pérdidas minoristas:** las empresas minoristas utilizan ampliamente la video-vigilancia para la prevención de pérdidas. Las cámaras de vigilancia instaladas en las tiendas pueden disuadir el hurto, monitorear la actividad de los empleados y proporcionar evidencia para el enjuiciamiento si ocurre un robo.
5. **Seguridad Pública:** los espacios públicos como parques, calles y centros urbanos a menudo emplean video-vigilancia para mejorar la seguridad pública. Estas cámaras pueden ayudar a disuadir el crimen, ayudar a las agencias de aplicación de la ley a capturar a los delincuentes y desempeñar un papel crucial en los escenarios de respuesta a emergencias.
6. **Instituciones educacionales:** escuelas, colegios y universidades utilizan video-vigilancia para garantizar la seguridad de sus estudiantes y personal. Las cámaras de vigilancia pueden ayudar a disuadir amenazas potenciales, monitorear el acceso no autorizado y garantizar un entorno de aprendizaje seguro.
7. **Centros de salud:** las instalaciones de atención médica, incluidos los hospitales y los hogares de ancianos, utilizan video-vigilancia para monitorear la actividad del paciente, garantizar la eficiencia del personal y evitar el acceso no autorizado a áreas restringidas.

I.4.6 Tecnologías en video-vigilancia

Los sistemas en cuanto a la video-vigilancia evolucionaron drásticamente, así combinando e incorporando nuevas tecnologías que brindan mejoras a los sistemas.

A continuación, se comentarán las tecnologías de cámara, de almacenamiento, de red y de software. Las cuales son claves según (Anish, 2023) para los sistemas modernos de video-vigilancia.

I.4.6.1 Tecnologías de cámara

- Cámaras analógicas: las cámaras analógicas transmiten señales de video a través de un cable coaxial a un conjunto específico de monitores. Aunque pueden carecer de algunas de las características avanzadas de las cámaras modernas, a menudo son apreciadas por su confiabilidad y rentabilidad.
 - Cámaras IP: las cámaras IP (Protocolo de Internet) envían secuencias de video a través de Internet, lo que permite la visualización y grabación remotas. Ofrecen una resolución más alta que las cámaras analógicas y se pueden integrar fácilmente con otros sistemas en red.
 - Cámaras térmicas: estas cámaras usan calor en lugar de luz para crear una imagen, lo que las hace excelentes para usar en condiciones climáticas adversas o con poca luz.
 - Cámaras con tecnología de IA: Aprovechando la inteligencia artificial, estas cámaras ofrecen funciones avanzadas como reconocimiento facial, detección de objetos y análisis de comportamiento.
 - Cámaras HD: las cámaras de alta definición (HD) brindan una calidad de imagen y detalles superiores, ideales para escenarios donde la identificación de detalles finos es crucial, como el reconocimiento facial o la identificación de matrículas.
 - Cámaras PTZ: las cámaras Pan-Tilt-Zoom (PTZ) ofrecen la flexibilidad de mover la lente, brindando una amplia cobertura de área e inspección detallada de objetos o áreas específicas.
- Estas serían las tecnologías en cámaras según (Anish, 2023).

I.4.6.2 Tecnologías de almacenamiento

- Grabadores de video digital (DVR): los DVR convierten las señales de video analógicas en formato digital para su almacenamiento y revisión. Por lo general, se utilizan con cámaras analógicas.
- Grabadores de video en red (NVR): los NVR capturan y graban transmisiones de video directamente desde la red en la que se encuentran para las cámaras IP. Proporcionan una grabación de mayor calidad y una integración más flexible que los DVR.

- Almacenamiento en la nube: con los avances en la tecnología de la nube, los datos de video ahora se pueden almacenar fuera del sitio en servidores remotos, lo que ofrece escalabilidad y accesibilidad desde cualquier lugar con una conexión a Internet.

Estas serían las tecnologías de almacenamiento según (Anish, 2023).

I.4.6.3 Tecnologías de red

- Ethernet: ethernet es una tecnología de red de uso común en los sistemas de video-vigilancia basados en IP, que admite la transmisión de datos de alta velocidad a través de cables.
- Wi-Fi: este te permite la transmisión inalámbrica de señales de video, lo que ofrece flexibilidad en la ubicación de la cámara sin necesidad de cableado.
- Celular: en ubicaciones remotas sin Internet por cable, las redes celulares se pueden usar para transmitir transmisiones de video.

Estas serían las tecnologías de red según (Anish, 2023).

I.4.6.4 Tecnologías de software

- Software de gestión de video (VMS): VMS es fundamental para administrar, ver y grabar transmisiones de video. Los sistemas VMS avanzados también ofrecen características como análisis de video y acceso móvil.
- Análisis de vídeo: el software de análisis de video utiliza algoritmos para detectar actividad inusual en la transmisión de video, como brechas en el perímetro u objetos desatendidos.
- Integración de Internet de las cosas (IoT): la tecnología IoT se puede utilizar para conectar cámaras de vigilancia con otros dispositivos y sistemas, creando un ecosistema de seguridad cohesivo que puede reaccionar de manera inteligente ante diferentes escenarios. Por ejemplo, si una cámara detecta movimiento en un área restringida, podría activar un sistema de alarma o bloquear las puertas de acceso automáticamente.
- Software de vigilancia basado en la nube: estas plataformas permiten el acceso y control remoto del sistema de vigilancia desde cualquier dispositivo con acceso a internet. También pueden proporcionar actualizaciones y copias de seguridad automáticas, lo que reduce la carga de mantenimiento para el usuario.

- Inteligencia artificial (IA) y aprendizaje automático (ML): los algoritmos de IA y ML pueden analizar transmisiones de video en tiempo real, identificando patrones, anomalías y detalles clave que pueden pasar desapercibidos para el ojo humano. Pueden habilitar funciones avanzadas como reconocimiento facial, reconocimiento de matrículas y análisis predictivo. Estas sería el listado de las tecnologías de software según (Anish, 2023).

I.4.7 Componentes de un sistema de seguridad

Un sistema de seguridad cuenta con una variedad de equipos bastante amplia las cuales nos ofrecen distintas soluciones según la necesidad. En base a esto se decidió hacer un listado de los equipos que componen un sistema de seguridad de una manera más profunda.

I.4.7.1 NVR (network video recorder)

I.4.7.1.1 Definición

(tecnoseguro, s.f.) define que un NVR (network video recorder) o grabador de video en red por sus siglas en inglés, es un equipo que opera dentro de una red de datos Ethernet y cuya principal función es la de almacenar señales de video en forma de datos que provienen de las cámaras IP que se conecten o se configuren en el equipo.



Figura 6. Estructura de un nvr

I.4.7.1.2 Diferencias entre NVR (network video recorder) y DVR (digital video recorder)

Algunas diferencias entre un nvr y un dvr que marcan (tecnoseguro, s.f.) son las siguientes:

- La diferencia principal entre las NVR y las DVR son los métodos de transmisión de video. Las DVR utilizan entradas de video analógicas que después se comprimen digitalmente. Las NVR, por otra parte, utilizan imágenes digitales que son pre comprimidas por una cámara IP.

Esto hace que la DVR requiera más recursos de la CPU, ya que las NVR comparten el trabajo de procesamiento con las cámaras IP.

- Un NVR en lugar de su contendor, por la cantidad de cámaras que pueden admitir, no tienen que estar instalados en el mismo sitio, la instalación puede ser más sencilla si el NVR incorpora puertos PoE, mayor eficiencia en almacenamiento y procesamiento de analíticas de video, entre otras.
- La implementación de los NVR implica que el instalador o quien los configure tenga conocimientos básicos de redes para la configuración de los equipos, en el caso de los DVR la puesta a punto es más sencilla y no requiere mayores conocimientos.
- Otro factor es como la distancia de cableado en los NVR está limitada por el estándar de redes, mientras que en el caso de los DVR se pueden tener distancias de cableado entre el equipo y la cámara mucho mayor dependiendo del tipo de cable.
- El costo de los NVR puede ser un poco más elevado que el de su contendor. De este modo, no en todos los casos será siempre la mejor opción el NVR frente al DVR, que de hecho este último sigue estando muy vigente en especial en el sector retail, residencial y aplicaciones de bajo presupuesto.

I.4.7.1.3 Ventajas del NVR

Algunas ventajas del nvr que marcan (trendnet, 2016) son las siguientes:

- Flexibilidad de instalación de las cámaras en sus ubicaciones.
- Instalaciones de cámara simplificadas empleando su red existente.

- Reducción del consumo de corriente y ahorro, no se requiere una computadora dedicada de alta potencia.
- No se necesita un software de administración de cámaras costoso.
- Administre cómodamente las grabaciones de video de múltiples cámaras desde una sola ubicación.
- Fácilmente escalable para ampliarla en función de sus necesidades cambiantes.
- La mayoría de las empresas y de las viviendas más recientes cuentan con infraestructura Ethernet existente.

I.4.7.1.4 NVR PoE o estándar

Ambos nvr tienen sus propias ventajas. Las nvr PoE transmiten corriente y datos al mismo tiempo mediante el cable ethernet y si son nvr independientes generan una red de cámaras privadas.

En cambio, las nvr estándar se necesita algo de experiencia en la administración de redes, pero esta es más económica.

NVR PoE independiente	NVR estándar
Perfecto para pequeñas empresas.	Perfecto para empresas grandes.
Diseño sencillo de conectar.	Se integra con facilidad a la red.
No requiere red.	Económica.
No requiere un switch PoE adicional.	Requiere un switch PoE
Reconoce y alimenta las cámaras PoE automáticamente.	

Tabla 3. Nvr independiente o estándar

I.4.7.2 Switch

I.4.7.2.1 Definición

Según (pccomponentes, 2022) nos dice que un switch o conmutador de red es un dispositivo informático que permite interconectar dispositivos a través de una red de área local o red LAN. Para ello, el switch dispone de un número de puertos determinados en los que podemos conectar cableado de red tipo Ethernet.

Además (pccomponentes, 2022) enlista algunas de las funciones básicas de un switch de red son:

1. **Compartir archivos:** con los accesos de seguridad correctamente aplicados, es posible compartir ficheros a gran velocidad entre los distintos dispositivos conectados a un switch.
2. **Compartir impresoras:** Es posible conectar a la red una impresora para que todos los dispositivos conectados puedan hacer uso de ella.
3. **Acceso a Internet:** el switch y el router son capaces de intercambiar información para dar acceso a internet a un gran número de dispositivos.

I.4.7.2.2 Switch con PoE

Es un switch de red que aplica la tecnología de alimentación a través de Ethernet (PoE, Power over Ethernet) que lleva a cabo la conectividad de la red y la alimentación de los dispositivos alimentados (PD, powered devices) a través del cable Ethernet. Los switches más comunes son los de 8 puertos, los de 16, los de 24 y los de 48. En cuanto al nivel de control de la red, existen switches PoE administrables y no administrables. Estos dispositivos se pueden utilizar en una amplia diversidad de lugares, desde el hogar hasta la oficina, en interiores o en exteriores. Los switches PoE tienen la capacidad de transmitir datos y alimentar a varios dispositivos a la vez. Normalmente se suelen utilizar para conectar teléfonos VoIP y de vídeo, cámaras IP, puntos de acceso inalámbricos, dispositivos de audio y algunas terminales de control IoT. (Mendez, 2023)

I.4.7.2.3 Switch con PoE vs Switch no PoE

Un switch sin PoE es un switch que solo puede enviar datos a los dispositivos de red y que carece de la habilidad de suministrar energía a través de Ethernet para los usuarios finales.

Para adquirir PoE, sería necesario desplegar un equipo de suministro de energía entre el switch y los dispositivos alimentados.

Este inyector u otros PSE de midspan aportan energía eléctrica mientras reciben señales de datos del cable conectado al switch sin PoE, entonces, entregan tanto datos como energía a los PDs.

En esta aplicación, los módulos PSE requieren un cable para la alimentación. Sin embargo, en una aplicación de switch PoE gigabit, la cosa es más fácil: sólo se necesita un cable de alimentación para el switch y un cable de red para conectar los PD. (Charlene, 2022)

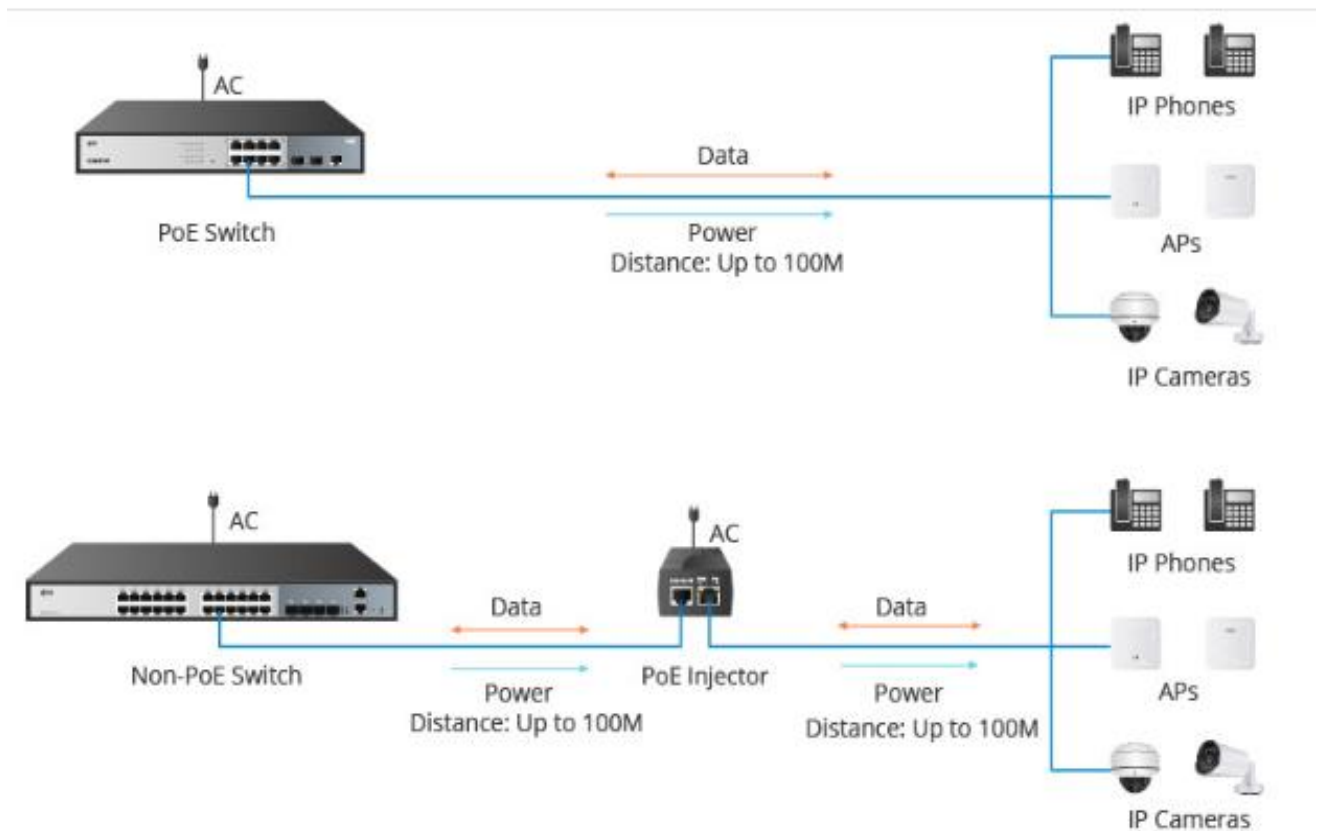


Figura 7. Switch poe vs no poe

I.4.7.2.4 Ventajas y limitaciones del switch con PoE

(Charlene, 2022) señala algunas ventajas y limitaciones del switch PoE:

1. VENTAJAS

Flexibilidad: cómo no necesitan PSEs ni cables de extensión adicionales, los switches PoE ganan una gran flexibilidad en cuanto al cableado de red de los usuarios. Permiten instalar los PD en los lugares necesarios, como las cámaras IP para vigilar un punto concreto, por ejemplo. Además, se puede llegar a lograr un entorno sin cables si se combina el switch PoE con tecnología inalámbrica.

Simplicidad: como no necesitan PSEs y las ubicaciones de instalación son más flexibles, los switches PoE simplifican el despliegue de la red en su totalidad. Además, los switches PoE de buena calidad también soportan el protocolo de gestión de red simple (SNMP, Simple network management protocol), que proporciona una forma más sencilla de monitorear y gestionar el switch.

Rentabilidad: con los switches de red PoE, no es necesario que los usuarios adquieran e instalen cables eléctricos y tomas de corriente adicionales, esto reduce considerablemente los costos y el tiempo de instalación y mantenimiento.

LIMITACIONES

Distancia: los switches PoE suelen tener una distancia máxima de transmisión PoE de 100 metros, esto puede resultar especialmente engorroso para los campus, empresas y restaurantes de gran tamaño. Sin embargo, existen algunos métodos para ampliar el alcance de la PoE, como los extensores de potencia o los cables de fibra alimentados.

Potencia: si necesitas una alta potencia en las redes PoE, debes asegurarte de que la capacidad de potencia de tus switches PoE satisface tus necesidades, ten en cuenta que existe una limitación de potencia basada en los estándares PoE y en los vatios PoE.

I.4.7.2.5 Switch administrable

Según (Acmax, 2020) un switch administrado es un dispositivo que permite realizar la misma función que un switch no administrado pero que, además, permite configurar, administrar y

monitorear los equipos y objetos de la red (LAN) en la que se encuentran conectados. Estas configuraciones y modificaciones nos permiten tener un gran control sobre el flujo de datos de nuestra red, la seguridad y el funcionamiento de la misma.

Así mismo, los switches administrados cuentan con protocolos especiales y funciones avanzadas. Entre estas funciones se encuentra la capacidad de crear VLANs (Virtual local área network). Las VLANs nos permiten segmentar de forma virtual nuestra red para poder aislar el tráfico existente.

Otra función de los switches administrables según (Acmax, 2020) es que nos permite controlar los switches administrados, es el Quality of Service (QoS). Con esta función, nosotros podemos controlar qué servicio tiene mayor prioridad en nuestra red y así asegurar que su funcionamiento sea óptimo. Un ejemplo sería si en la oficina o industria se cuenta con telefonía IP, es muy importante asegurar que el tráfico de la telefonía IP tenga prioridad para evitar que las llamadas se escuchen con retraso o distorsionadas. Lo mismo sucedería con alguna videoconferencia.

En cuanto a las ventajas de usar este tipo de switch (tempelgrouplatam, s.f.) indica algunas de ellas:

- **Control centralizado:** Con un switch administrable, puede configurar y monitorear su red desde una sola ubicación, lo que le permite tener un control completo sobre la red y detectar problemas de forma rápida y eficiente.
- **Seguridad mejorada:** La capacidad de configurar y monitorear la red desde una sola ubicación también permite aumentar la seguridad de la red, restringiendo el acceso a la red y bloquear ataques y amenazas en tiempo real.
- **Mayor eficiencia:** Al tener una red bien configurada y monitoreada, se puede maximizar la eficiencia de la red, asegurándose de que los datos se transmitan de forma rápida y eficiente y evitando cuellos de botella.
- **Facilidad de uso:** La mayoría de los switches administrables vienen con interfaces de usuario fáciles de usar, lo que permite a los administradores configurar y monitorear la red sin tener que ser expertos en tecnología.

De acuerdo con (Worton, 2023) hay varios tipos de los switches gestionables y no gestionables en el mercado como Cisco switches gestionables o no gestionables, Netgear switch gestionables/no gestionable, HP switches gestionables, etc. Y las opiniones sobre las aplicaciones de estos switches

de red varían de persona a persona. A continuación, una tabla con las diferencias entre switch administrables y no administrables.

	Switch Administrable	Switch No Administrable
Flexibilidad en la configuración	Permiten a los clientes personalizar, diseñar y filtrar las LAN. Ayudan a los usuarios a administrar el tráfico de manera eficiente y les permiten crear nuevas LAN y separar dispositivos más pequeños. Sus funciones avanzadas permiten a los usuarios recuperar datos en caso de falla del dispositivo o de la red.	Son fáciles de operar, su configuración preinstalada le impide realizar cambios en las redes.
Rendimiento de la red	Supervise el rendimiento de todos los dispositivos conectados en la LAN utilizando protocolos como SNMP. Permite el control remoto de los dispositivos y la organización asociados, sin necesidad de una intervención real en el switch.	Plug & Play con configuración limitada, como la configuración estándar de QoS
Seguridad	Las características avanzadas de los switches administrados ayudan a identificar y neutralizar rápidamente las amenazas activas mientras protegen y controlan los datos.	La función de seguridad básica de los switches no administrables es el bloqueo de puertos, lo que ayuda a evitar cualquier manipulación directa del dispositivo y garantiza la seguridad básica.
Costes	Caro	Más barato que los switches gestionados.

Aplicaciones	Centro de datos, gran red corporativa	Red de negocios de pequeño tamaño, hogar, laboratorio, salas de conferencias, etc.
--------------	---------------------------------------	--

Tabla 4. Switch administrable vs no administrable

I.4.7.3 Cámaras de vigilancia

Son componentes electrónicos cuya función es captar una imagen continua de todo lo que suceda en un espacio determinado. En materia de seguridad, la cámara de vigilancia no representa una barrera de protección. Sin embargo, en ocasiones, la presencia de cámaras de seguridad desalienta a algunos malhechores a cometer alguna fechoría. (plussegur, s.f.)

I.4.7.3.1 Cámara de vigilancia Poe

Según (trendnet, 2021) Las cámaras de vigilancia PoE son cámaras IP (también llamadas cámaras de red) que utilizan la tecnología PoE y que ofrecen tanto datos como alimentación eléctrica mediante un solo cable. Tenga en cuenta que, aunque todas las cámaras PoE son cámaras IP, no todas las cámaras IP son cámaras PoE. A diferencia de las cámaras CCTV analógicas tradicionales, las cámaras IP (y las cámaras PoE) se pueden utilizar como un dispositivo independiente. Para conectar cámaras analógicas a la red, estas cámaras requieren una DVR con el fin de convertir la señal analógica a IP.

I.4.7.3.1.1 Beneficio de las cámaras Poe

Transmitir datos y energía mediante un solo cable ayuda a ahorrar costes de infraestructura innecesarios y a reducir el tiempo de instalación total. Instalar dos juegos de líneas para ir al mismo lugar añade costes de cableado y de mano de obra, además del coste de los cables y el tiempo necesario para realizar el cableado. Por otro lado, con las cámaras de vigilancia PoE, no tendrá que preocuparse por contar con un enchufe cercano para conectar la cámara a la alimentación eléctrica; el PoE estándar puede prolongarse desde la fuente de alimentación a hasta 100 m (328 pies aprox.). (trendnet, 2021)

I.4.7.3.1.2 Características más importantes de las cámaras PoE

Al tener un amplio catálogo de cámaras PoE a continuación (trendnet, 2021). Destaco las 4 características más fundamentales:

A. Resolución

Una mayor resolución se traducirá en la grabación de un vídeo de vigilancia de mayor calidad en su cámara PoE. Considere también los fps (fotogramas por segundo). Una mayor tasa de fps se traducirá también en unos archivos de vídeo de mayor calidad

B. Visión nocturna

La visión nocturna le permite captar grabaciones de vídeo de vigilancia en la oscuridad. El rango de visión nocturna de las cámaras PoE puede variar. Si necesita seleccionar una cámara con visión nocturna, asegúrese de comprobar las especificaciones técnicas para confirmar si la visión nocturna admite la distancia que le interesa cubrir.

C. Campo visual

El campo visual (FOV) es el área visible que captará su cámara PoE. Algunas de las características de la cámara tendrán un efecto directo en el campo visual de su cámara. El zoom desempeña una función importante en el campo visual de su cámara. El zoom de su cámara puede variar entre zoom óptico o digital, y entre zoom manual o motorizado. Para mayor flexibilidad, considere la posibilidad de contar con una cámara con lente varifocal, que le permite ajustar la distancia focal de su lente.

D. Acceso remoto y aplicación móvil

Uno de los aspectos más importantes de la vigilancia es la capacidad de prevenir el delito, así como de responder a los problemas rápidamente. Ya sea en su hogar o en su negocio, el acceso remoto a sus cámaras PoE es fundamental y le permite actuar de inmediato. Es posible que no cuente con alguien in situ para que vea en vivo y de manera constante los vídeos de vigilancia. Busque marcas de cámara vigilancia PoE que ofrezcan aplicaciones móviles gratuitas con características tales como alertas móviles.

I.4.7.3.2 Tipos de cámara de vigilancia

El mercado está lleno de opciones en cuanto a tipos de cámaras, (ovacen, s.f.) detalla un listado donde se dividen según sus funciones y capacidades:

I.4.7.3.2.1 Cámaras de interior

Son las más sencillas que podemos encontrar en el mercado y las más baratas dado que no necesitan tantos mecanismos y protecciones como las que se utilizan en el exterior.

I.4.7.3.2.2 Cámaras con movimiento y zoom

Se suelen utilizar en espacios de grandes dimensiones con una central de seguridad donde una persona monitoriza y vigila las cámaras. Estas cámaras robóticas que tienen las propiedades de movimiento sobre giro, inclinación y zoom.

I.4.7.3.2.3 Cámara de visión nocturna

Este tipo de instrumentos se utilizan en la vigilancia dónde existen espacios con poca iluminación. Normalmente graban todo el día y por la noche de forma automática enciende sus infrarrojos con una visión en blanco y negro. Son las más caras del mercado por la visión nocturna por LED.

Son utilizadas como cámaras de video-vigilancia dentro de una instalación de CCTV.

I.4.7.3.2.4 Cámaras ocultas

Son las llamadas cámaras espía para monitorear y vigilar una casa, la oficina o el negocio pasando 100% desapercibidos. Se introducen dentro de algún objeto como; sensores de movimiento, detectores de humos, enchufes...etc.

I.4.7.3.2.5 Cámaras ip

La cámara IP, son aquellas que se conectan directamente a Internet mostrando la imagen que visualiza. Son las más utilizadas y vendidas del mercado dado que actualmente además incorporan wifi y puedes manejarlas y ver las imágenes que captan desde tu ordenador, smartphone u tablet.

La principal ventaja de la cámara IP reside en que es un dispositivo de vigilancia a través de vídeo permitiendo ver las imágenes en tiempo real a distancia, a través de la conexión con una dirección IP de Internet.

Las podemos encontrar a la venta con especificaciones técnicas de consumo normal, para casa, o más desarrolladas para profesionales.

I.4.7.3.2.6 Cámaras antivandalicas

Son utilizadas en zonas de tránsito de público vulnerables a robos y a posibles agresiones. Está montada sobre una carcasa fija y resistente. Se suele utilizar mucho en almacenes, parking, discotecas, vías públicas y en general en cualquier espacio exterior.

I.4.7.3.2.7 Cámaras wifi

Son aquellas que no están conectadas directamente por un cable. Normalmente tiene una batería que las hace funcionar y transmiten los datos por medio de Wifi.

Son las utilizadas dentro de casa, por ejemplo, para ver cómo están los niños o el bebé, y también tecnología se ha incorporado a las cámaras IP para trabajar de forma directa con el monitoreo por internet.

I.4.7.3.2.8 Cámaras exteriores

Este tipo de cámaras están diseñadas para resistir las acciones climatológicas (lluvia, viento...etc.) y son utilizadas en espacios al aire libre. Cuando compramos una cámara para exterior normalmente el precio es más caro principalmente por la carcasa de protección.

I.4.7.3.2.9 Cámaras todo en uno

Con los avances de la tecnología se ha producido un abaratamiento sobre el tipo de cámara que puedes encontrar en una tienda, así que han ido incorporando diferentes elementos para que puedan tener más funciones.

Por ejemplo, existen modelos que son tanto para interior como exterior, que utilizan wifi y el monitoreo es por medio de Internet sea en ordenador o el móvil. Al final podemos tener una instalación de seguridad con cámaras todo lo complejo que queramos y más si utilizamos domótica en la instalación de casa.

I.4.7.3.3 Tipos de cámaras de vigilancia más usados

Según (Ugarteburu, 2023) estos son algunos modelos de cámaras más usadas.

1. Cámaras fijas:

son el tipo más común de cámaras de vigilancia en la industria y se utilizan para controlar áreas específicas, como entradas, salidas o zonas de almacenamiento donde no es necesario hacer zoom o mover la cámara para cubrir otros ángulos. Son ideales para situaciones en las que se requiere una vista general de una zona, se pueden utilizar en interiores y exteriores, y se pueden montar con diferentes resoluciones.

2. Cámaras domo:

son un tipo de cámara fija que se caracteriza por su forma redondeada o semiesférica. Pueden monitorear áreas mucho más amplias que las cámaras fijas tradicionales. Además, la mayoría tienen una carcasa protectora que protege la cámara de daños físicos.

3. Cámaras PTZ:

son una versión mejorada de las cámaras fijas porque permiten al usuario controlar la dirección de la cámara, la inclinación y el zoom. Estas cámaras son útiles para monitorear áreas amplias, ya que pueden moverse en diferentes direcciones y ajustar el zoom según sea necesario. Se controlan a través de un joystick o un software de vigilancia remota por lo que también son muy útiles para monitorear objetos o personas en movimiento que la cámara puede seguir.

4. Cámaras IP:

se conectan a una red de Internet y permiten el acceso en remoto. Son útiles para monitorear áreas remotas y permiten a los usuarios ver la transmisión de video en tiempo real desde cualquier lugar con conexión a Internet. Por este motivo pueden resultar muy útiles a los responsables de la seguridad para tomar decisiones más rápidas en situaciones de emergencia. Además, pueden ser configuradas para enviar alertas a dispositivos móviles o correo electrónico cuando se detecta un movimiento en una zona determinada y resultan

ser dispositivos muy versátiles para su uso en una amplia variedad de industrias, siempre que la conexión a internet sea estable.

5. **Cámaras bullet:**

recibe este nombre porque son cámaras cilíndricas y alargadas que se asemejan a una bala. Se utilizan comúnmente para la vigilancia de perímetros, áreas exteriores y áreas de alto tráfico, ya que son resistentes a la intemperie y pueden soportar condiciones climáticas adversas.

6. **Cámaras 360:**

estas cámaras están diseñadas para capturar una vista completa de 360 grados de una zona de vigilancia. Utilizan múltiples lentes y sensores para capturar todo lo que hay alrededor de la cámara y la imagen resultante se puede ver en una pantalla o en un software de visualización que permite al usuario navegar y hacer zoom en la imagen para ver detalles específicos.

7. **Cámaras térmicas:**

son capaces de detectar la radiación infrarroja que emiten los objetos, lo que les permite obtener imágenes en la oscuridad o en condiciones de baja visibilidad, así como detectar la presencia de personas o animales en condiciones de poca luz. Estos dispositivos son útiles para monitorear áreas donde la iluminación es pobre o donde se necesita una visión precisa en condiciones climáticas adversas, son ideales para la vigilancia de zonas en las que se requiere un alto grado de seguridad y también son capaces de detectar incendios o fugas de gas.

8. **Cámaras de reconocimiento facial:**

son cámaras que utilizan la tecnología de reconocimiento facial para identificar a las personas. Usan algoritmos para comparar las características faciales de las personas con las imágenes almacenadas en una base de datos. Son útiles en industrias donde se necesita una seguridad de alto nivel ya que pueden ser programadas para identificar a personas específicas y alertar a los responsables de la seguridad si detectan la presencia de alguien

que no debería estar en un área específica. Por último, pueden identificar personas incluso en multitudes y en situaciones de iluminación variable.

9. Cámaras de lectura de matrículas:

se usan para leer y registrar las matrículas de los vehículos. Al detectar la presencia de un automóvil, las cámaras capturan la imagen de la placa y, una vez analizada y procesada la información, ésta se compara con la base de datos introducida en el sistema. De ese modo el usuario puede autorizar o denegar el acceso a sus instalaciones en función de los criterios previamente establecidos, así como gestionar permisos, listas blancas, negras, etc.

10. Cámaras ocultas:

son cámaras que están diseñadas para pasar desapercibidas y pueden parecer objetos cotidianos como detectores de humo, enchufes, lámparas u otros dispositivos eléctricos comunes. Son ideales para la vigilancia encubierta y pueden ser muy útiles para monitorear el comportamiento de los empleados o para detectar posibles robos o vandalismo en las empresas.

I.4.8 Fuente de alimentación del sistema PoE

Según (trendnet, 2021) la tecnología Power over Ethernet o PoE le permite utilizar un solo cable tanto para los datos y como para la alimentación eléctrica. Sin PoE, necesitaría dos cables independientes: uno para la conexión de red y otro para la alimentación. El uso de varios cables aumenta tanto los costes de infraestructura como los costes de mano de obra. La posibilidad de utilizar un cable le permite ni más ni menos matar dos pájaros con un solo tiro.

Las conexiones con la tecnología PoE suelen ser simples y organizadas además de reducir gastos. A continuación, se muestra unos ejemplos donde se ve cómo trabaja el PoE con el switch, nvr y cámaras.

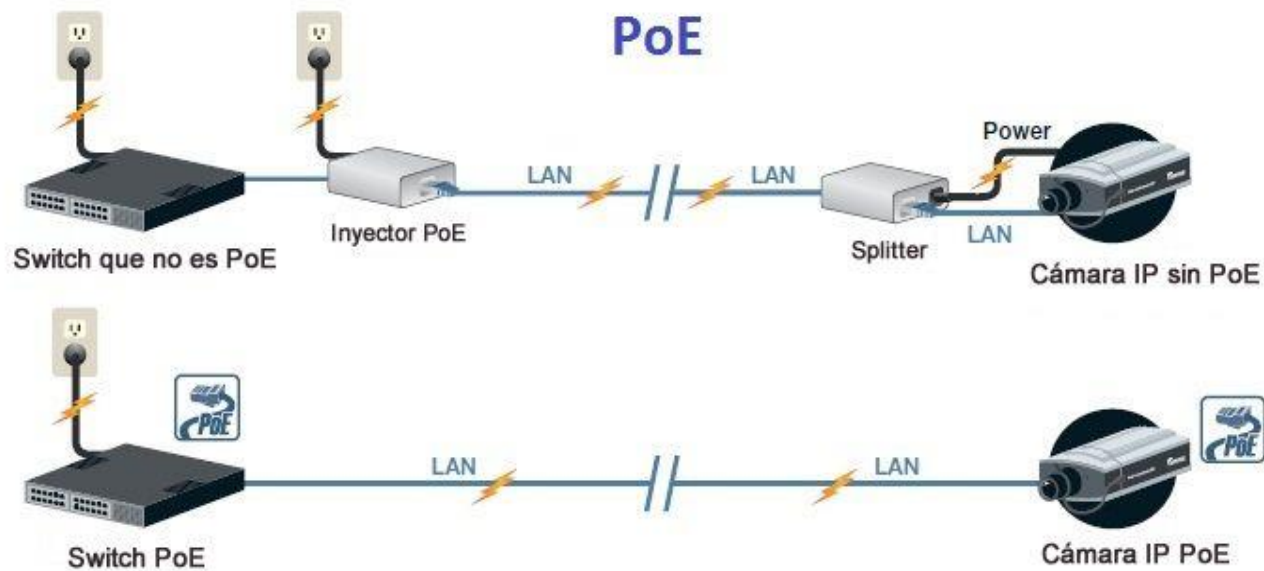


Figura 8. Switch y cámara con y sin poe

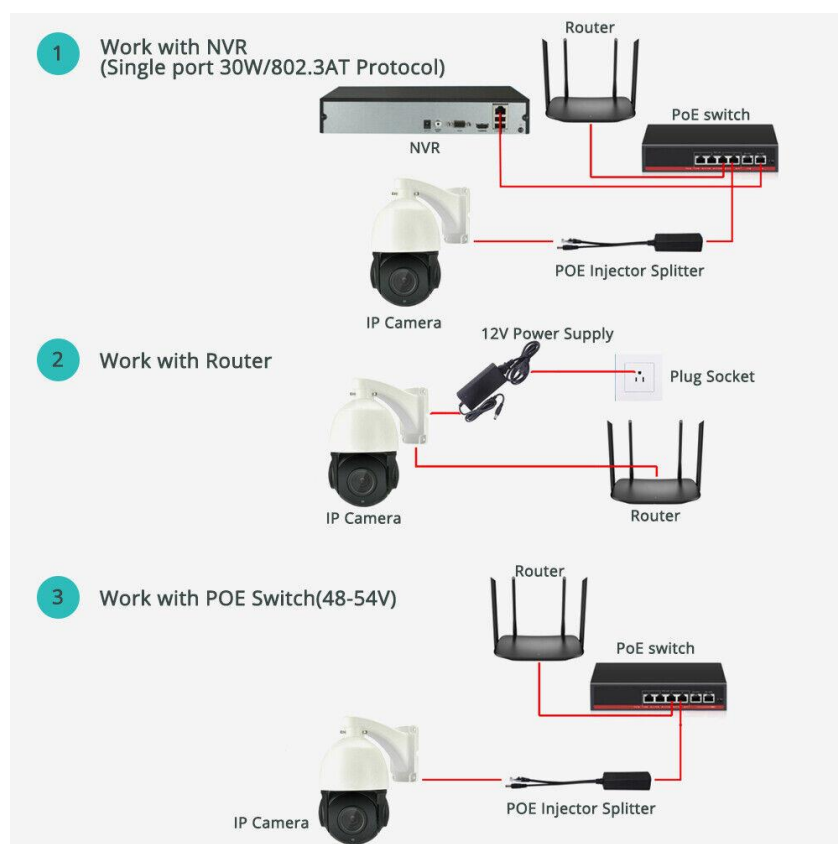


Figura 9. Sistema de seguridad con poe switch, poe nvr y sin nvr

I.4.9 Programas para el control de Cámaras

La visualización de las cámaras de seguridad se las puede realizar mediante la red lan o por internet. Para esto se usa el software del cliente “iVMS-4200”

Según (hikvision, s.f.) El software gratuito iVMS-4200 es compatible con la mayoría del hardware de Hikvision. Equipa a los usuarios con video en vivo desde la transmisión de la cámara, control de acceso, intercomunicador de video, alarmas y almacenamiento de datos.

- Abundantes módulos: video, control de acceso, asistencia, intercomunicador, alarma, mapa electrónico y más.
- Experiencia de usuario y diseño visual amigables: interfaz de usuario plana y liviana, y diseño basado en componentes.
- Múltiples idiomas: 33 idiomas, incluidos inglés, chino simplificado, árabe, etc.

Este mismo software se puede configurar para añadir dispositivos, preferencias, etc. Incluso se puede configurar para verlo por internet, esto mediante el registro y con la contraseña y usuario determinado. Cabe mencionar que no solo incluye la vista a tiempo real si no también la administración de las grabaciones.

De la misma manera se puede usar incluso Hik-connect el cual es una aplicación para celulares.

I.5 Matriz del marco Lógico (MML)

Nivel	Resumen Narrativo del Proyecto	Indicador	Medios de Verificación	Supuestos
Fin	Incorporar tecnologías para apoyo en la administración académica de la facultad de ciencias integradas de la UAJMS de la ciudad de Bermejo. Contribuir con un manual que brinde soporte a los empleados que emplean el sistema de cámaras de seguridad.	A los dos años de haber implementado el proyecto la comunidad universitaria expresa satisfacción acerca del uso de la tecnología como herramienta de mejora en la administración académica-administrativa de la facultad de ciencias integradas.	Encuestas que expresen satisfacción o conformidad de los estudiantes y docentes.	Aceptación por parte de los involucrados hacia el diseño.
Propósito	Mejorar la seguridad infraestructural y personal mediante el diseño una red de cámaras de seguridad para el módulo 2 de la facultad de	Al finalizar el proyecto el 88% de los puntos críticos hallados en el edificio de ciencias integradas se verán cubiertos por el sistema y por lo tanto de seguridad. Véase en anexos A.	Carta del decano que exprese su conformidad con el grado del proyecto. Véase en anexos C.	La implementación del sistema de video vigilancia

	ciencias integradas de la UAJMS en la ciudad de Bermejo.			
Componentes	C.1 Diseñar y simular un sistema de video vigilancia con el software Ip Video System Design Tool para el módulo 2 de la facultad de ciencias integradas de la UAJMS en la ciudad de Bermejo.	Al concluir el proyecto se obtendría un sistema que cubre el 100% de los requerimientos técnicos bases para todo sistema de video vigilancia: • Ancho de banda. • Espacio en disco. • Tiempo de grabación. Véase en anexos A.	Carta del docente de la materia que exprese su conformidad respecto al grado del proyecto. Véase en anexos C.	Colaboración por parte de las autoridades facultativas.

	C.2 Manual de procedimientos para el uso de cámaras de seguridad y vigilancia	Al finalizar el proyecto se cuenta con un manual de procedimientos para el uso de cámaras de seguridad y vigilancia. De acuerdo a la: • Constitución Política del Estado. • Ley No. 264 Sistema Nacional de Seguridad Ciudadana “Para una vida segura”.	Se cuenta con un manual impreso que contiene los roles y procedimientos que se deben de cumplir en el sistema de seguridad de acuerdo a las normas de la constitución política del estado.	El manual propuesto es validado por el encargado de las TIC de la UAJMS de Bermejo.
--	--	---	---	--

Actividades	Componente 1: Diseñar y simular un sistema de video vigilancia con el software Ip Video System Design Tool para el módulo 2 de la facultad de ciencias integradas de la UAJMS en la ciudad de Bermejo. Las actividades a realizar en este componente son las señalizadas por la metodología top-down. Fase 1: Análisis de los requerimientos. Fase 2: Desarrollar diseño lógico. Fase 3: Desarrollar diseño físico. Fase 4: Aprobar, optimizar y documentar diseño Componente 2: Manual de procedimientos para el uso de cámaras de seguridad y vigilancia	Materiales	32323,4		Reporte de almacenamiento disponible, ancho de banda a ocupar y tiempo de grabación a estimar. Véase en anexos B. Registros del proyecto una vez finalizado. Proformas de cada uno de los equipos. Véase en anexos b. Cronograma planteado. Revisiones realizadas por parte del docente de la materia.	Margen económico. Existencia de los equipos en el mercado local. Plazos de entrega.
		Mano de obra	9,300			
		Consultados	1,800			
		Total	43.423,4 Bs.			

	• Investigar leyes y normas que regulen el uso correcto de las cámaras de seguridad. • Determinar roles y responsabilidades dentro del sistema de video vigilancia. • Determinar las actividades y procedimientos que cumplirá cada rol mediante diagramas de procesos.			
--	---	--	--	--

Tabla 5. Matriz de marco lógico

CAPÍTULO II

COMPONENTES

Capítulo 2: Componentes

I.6 Componente I: Diseñar y simular un sistema de video vigilancia con el software Ip Video System Design Tool para el módulo 2 de la facultad de ciencias integradas de la UAJMS en la ciudad de Bermejo

I.6.1 Resumen de la metodología para el diseño de red

La metodología top-down divide los problemas para así obtener subproblemas más manejables y sencillos de solventar. De este modo se conectan los subproblemas y solucionamos el problema principal. Esta metodología de desarrollo consta de 6 fases, en este caso se desarrollará hasta la fase 4 por el motivo de que no se realizará la implementación:

- **Fase 1: Análisis de los requerimientos.**
 - Analizar metas del negocio.
 - Analizar metas técnicas.
 - Analizar red existente.
 - Analizar tráfico existente
- **Fase 2: Desarrollar diseño lógico.**
 - Diseñar topología de red.
 - Diseñar modelos de direccionamiento y hostnames.
 - Seleccionar protocolos para Switching y Routing.
 - Desarrollar estrategias de seguridad.
 - Desarrollar estrategias de administración de red.
- **Fase 3: Desarrollar diseño físico.**
 - Seleccionar tecnologías y dispositivos para redes de campus.
 - Seleccionar tecnologías y dispositivos para redes empresariales.
- **Fase 4: Aprobar, optimizar y documentar diseño.**
 - Probar el diseño de red.
 - Optimizar el diseño de red.
 - Documentar el diseño.

- **Fase 5: Implementar y probar la red.**
 - Realizar cronograma de implementación.
 - Implementación del diseño de red (final).
 - Realizar pila de pruebas.
- **Fase 6: Monitorear y optimizar la red.**
 - Operación de la red en producción.
 - Monitoreo de la red.
 - Optimización de la red.

I.6.2 Ingeniería de requerimientos

I.6.2.1 Requerimientos funcionales

Se llevó a cabo un estudio de redes con los siguientes requerimientos del proyecto:

- Cubrimiento total del bloque por las cámaras de seguridad, sin dejar ningún punto ciego.
- Rango de cámaras y calidad de imagen satisfactorias y rentables.
- Cámaras que cumplan la función de visión nocturna.
- Ubicación de obstáculos y estructura de las edificaciones para tener en cuenta.
- Ubicación de los switches y controladoras.
- Dimensionamiento de la red.
- Ubicación requerida de las salas de equipos y monitoreo además de las cámaras.

Monitoreo rentable y factible.

I.6.2.2 Requerimientos no funcionales

- Debe de estar protegido contra el acceso no autorizado.
- El sistema debe ser capaz de escalar según la necesidad.
- El sistema de cámaras debe cumplir con todas las leyes y reglamentos aplicables.
- La disponibilidad del monitoreo debe ser total a todo momento.
- El sistema debe ser fácil de realizar mantenimiento y actualizar.
- El sistema que gestiona el monitoreo debe poder ejecutarse en diferentes plataformas con cambios mínimos.

- El sistema de monitoreo debe ser fácil de usar y comprender.

I.6.3 Desarrollo del componente de acuerdo a la metodología utilizada

I.6.3.1 Fase 1: Análisis de los requerimientos

I.6.3.1.1 Análisis de metas del negocio

Para entender los requerimientos es importante conocer a fondo la institución en la cual se trabajará.

II.1.3.1.1.1 Misión

Formar profesionales competentes e integrales, que asimilen y transfieran, avance científico – tecnológico de acuerdo a las exigencias del entorno, con criterios de equidad, responsabilidad social universitaria, diversidad cultural y el respeto al medio ambiente. (uajms, s.f.)

II.1.3.1.1.2 Visión

La UAJMS es una reconocida institución pública y autónoma que desarrolla la formación competente e integral de la persona, liderando la educación superior, de acuerdo a las exigencias del medio social, enfatizando el enfoque pedagógico centrado en el aprendizaje a través de procesos presenciales, a distancia, convencionales, virtuales, de pre y postgrado, con actividades de investigación, extensión e interacción social con entidades similares del país y el exterior en un marco de la responsabilidad social universitaria. (uajms, s.f.)

II.1.3.1.1.3 Estructura organizacional

Según (uajms, 2023) la estructura organizativa y académica de la UAJMS consta de tres niveles:

1) Nivel institucional y/o estratégico, que tiene a su cargo la proyección general de la actividad académica universitaria y el relacionamiento institucional con las instancias generales de la administración pública y la sociedad civil organizada; dentro de las cuales están las máximas autoridades universitarias:

- Honorable Consejo Universitario
- Rector

- Vicerrector

2) Nivel intermedio o ejecutivo, que responde al nivel de secretarías, Facultades y

Departamentos Administrativos y Académicos, que tienen a su cargo la proyección integrada de un conjunto específico de áreas de conocimientos y su relacionamiento con sectores determinados de la sociedad y responden a:

- Secretaría General
- Secretaría de Desarrollo Institucional
- Secretaría Académica
- Secretaría de Gestión Administrativa y Financiera
- Secretaría de Educación Continua
- Facultades de la UAJMS
- Departamentos Administrativos y Académicos.

3) Nivel Operativo o de ejecución, es decir Departamentos, Institutos de Investigación y

Unidades en general, tiene a su cargo la proyección de un área de conocimiento específica y su relacionamiento con necesidades y demandas sociales determinadas.

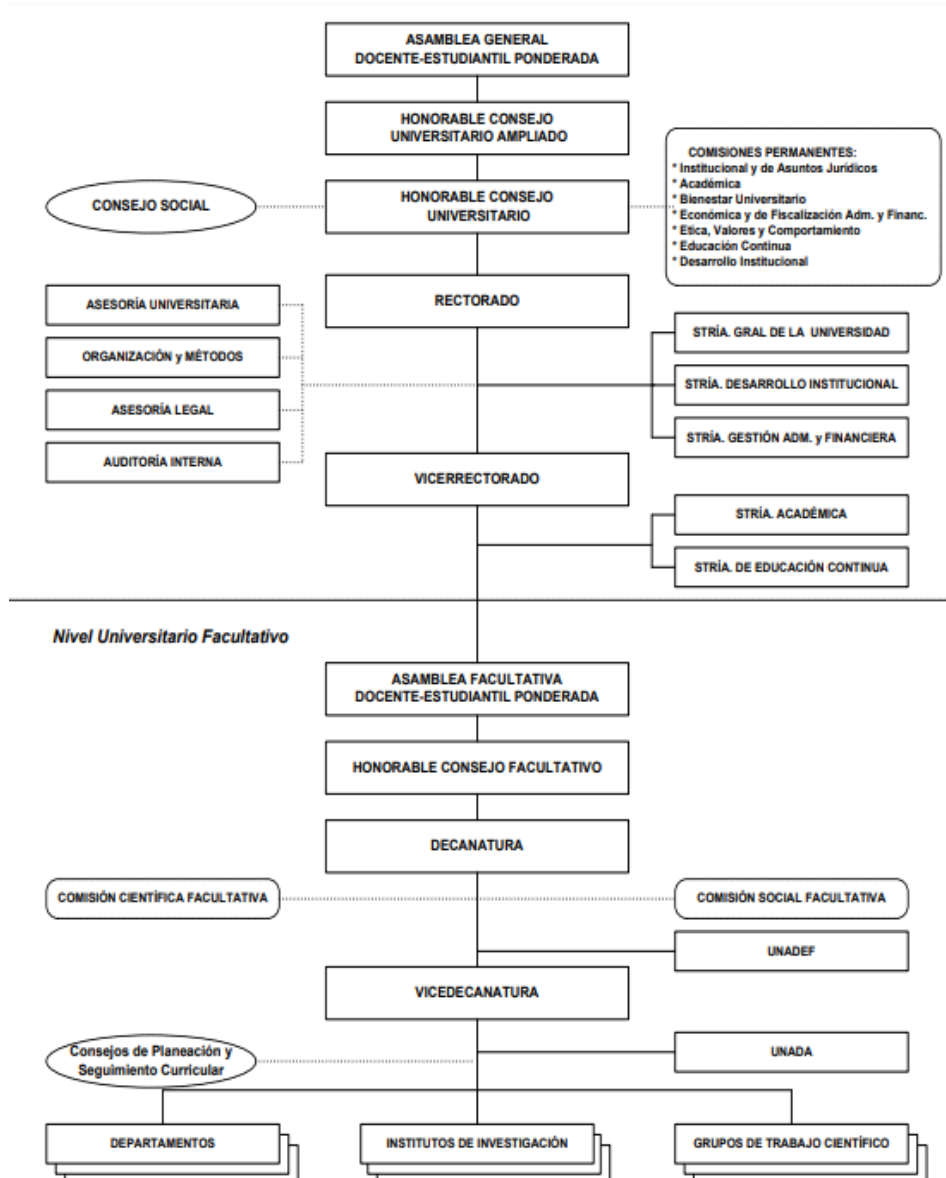


Figura 10. Diagrama estructura orgánica uajms

I.6.3.1.2 Análisis de metas técnicas

Este diseño tiene persigue como metas principales los siguientes puntos: Proveer de seguridad al bloque mediante cámaras ip para salvaguardar los equipos, infraestructura y personal.

- Disponer de un ancho de banda optimo y estable.
- Optimizar gastos en cuanto a materiales y equipos
- Tener una red con administración centralizada.

- Lograr de este bloque un lugar más seguro y por lo tanto mejor visto.
- Realizar una red prolija y óptima.
- Lograr seguridad lógica en la red de video vigilancia.

Existen algunos requerimientos técnicos que es necesario cumplir, estos son: mantenibilidad, escalabilidad, calidad de servicio, seguridad y administración.

- **Mantenibilidad:** La red debe de ser fácil de mantener y actualizar.
- **Escalabilidad:** El diseño de la red debe de ser adaptable a cambios, estos cambios pueden ser como expansión de la red, adición de nuevos dispositivos, etc.
- **Calidad de Servicios:** La red diseñada tiene que posibilitar priorizar los servicios y aplicaciones.
- **Seguridad:** El diseño debe de cubrir la seguridad tanto física como lógica.
- **Administración:** En base al diseño de la red se obtiene una administración centralizada.

I.6.3.1.3 Análisis de la red existente

Descripción: Este bloque consta de tres plantas al ser relativamente nuevo no existe una red ya establecida, por lo tanto, tampoco equipos ni algún tipo de tráfico de datos.

Estas plantas tienen espacios bastantes amplios como pueden pasillos, distribuidor, auditorio, etc.

Planos: a continuación, se tiene los planos del bloque, este bloque cuenta con 3 plantas.

II.1.3.1.3.1 Análisis físico de la infraestructura existente

A. Planta baja

La planta baja de este bloque cuenta con los siguientes ambientes:

- | | |
|--------------------|----------------------------|
| • 9 aulas | • UNADEF |
| • 2 baños | • UNADA |
| • Deposito | • Departamento de jefatura |
| • Biblioteca | • Secretaria |
| • Sala de archivos | • Centro de estudiantes |



55

B. Primer piso

El primer piso de este bloque cuenta con los siguientes ambientes:

- 6 aulas
- 2 laboratorios de gabinete
- Laboratorio de computación
- Sala de control
- Baño
- Sala de estar
- Ambiente anexo
- Sala de archivos
- Cocina
- Sala de reuniones
- Sala de docentes

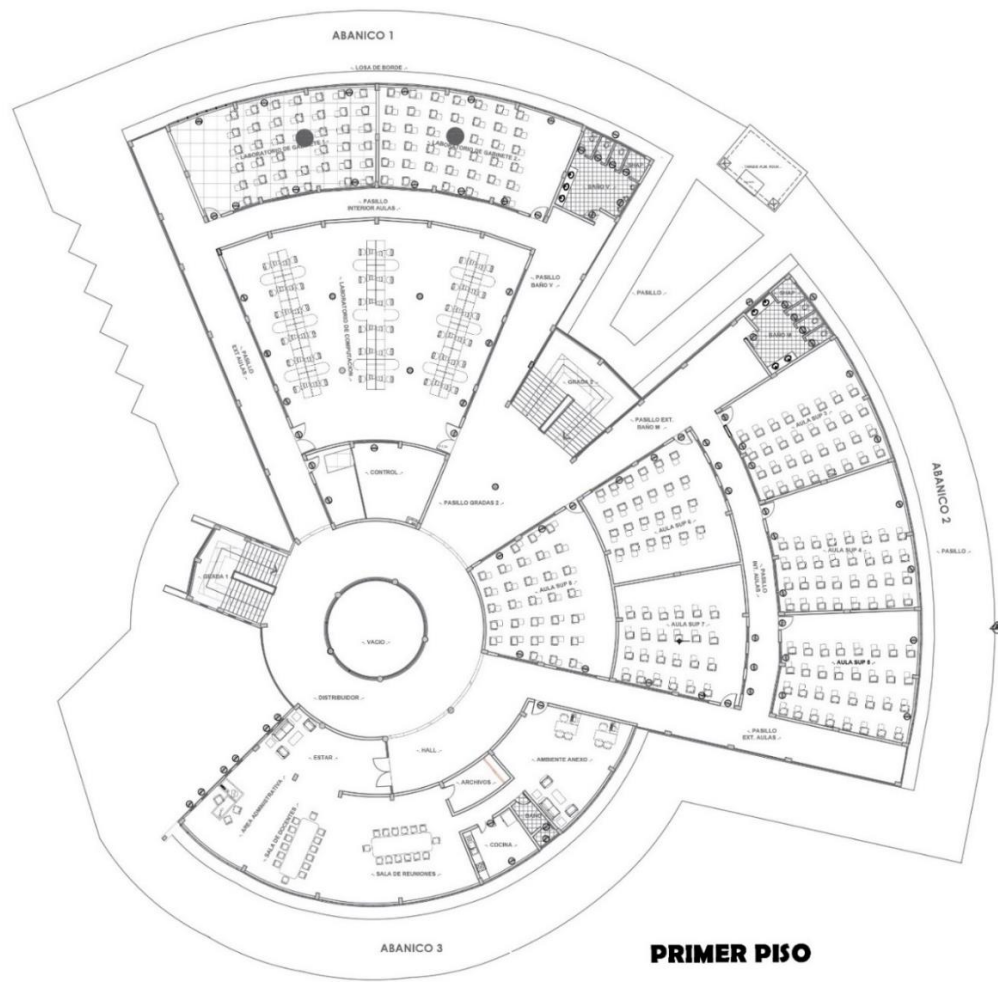


Figura 12. Planos primer piso

C. Segundo piso

El segundo piso de este bloque cuenta con los siguientes ambientes:

- 5 aulas
- 2 baños
- Auditorio
- Sala de equipos
- Sala de reunión
- Sala de investigación
- Sala de decano
- Sala de vicedecano

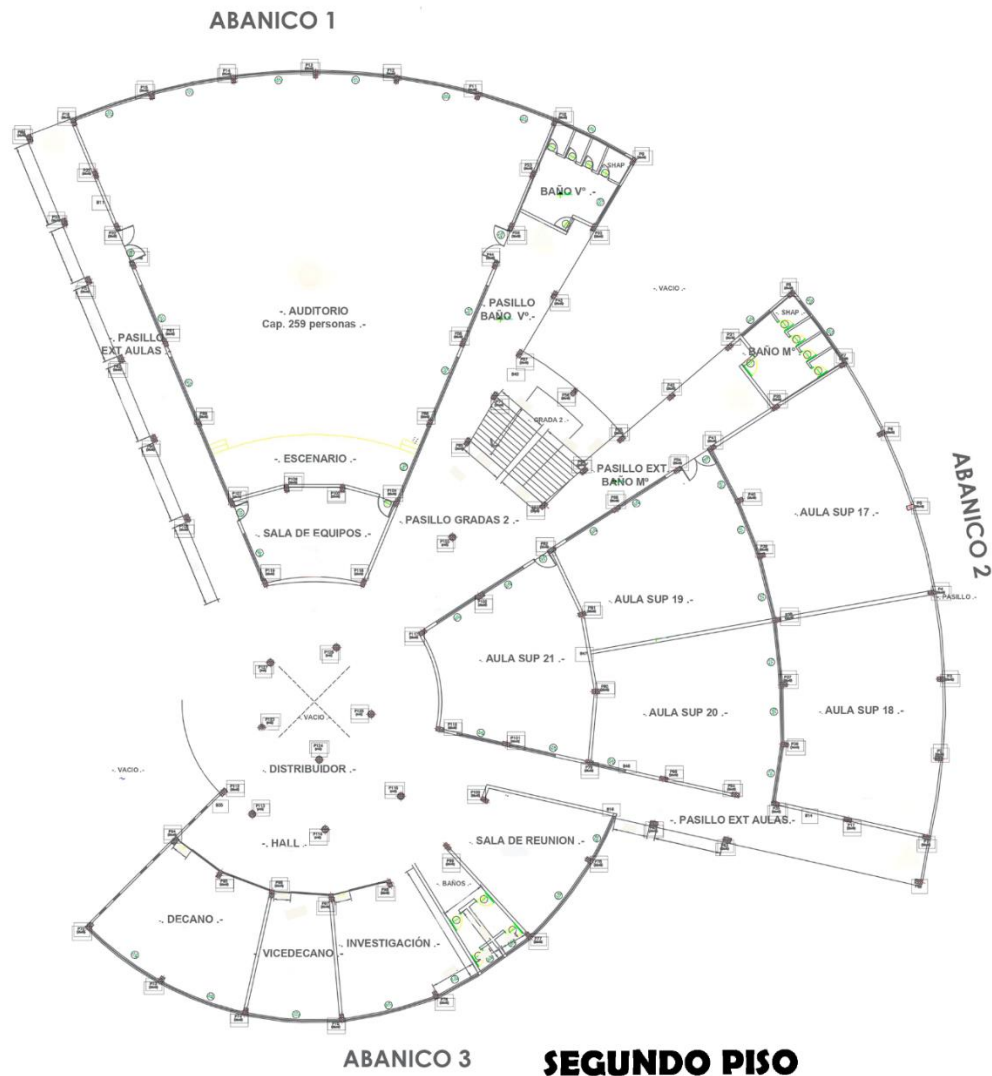


Figura 13. Planos segundo piso

I.6.3.2 Fase 2: Desarrollar diseño lógico

I.6.3.2.1 Ubicación de las cámaras de seguridad

Para lograr determinar los lugares más adecuados para ubicar las cámaras se deben de tener en cuenta las siguientes características.

- **Angulo de visión:** Para obtener un buen ángulo de visión dependerá principalmente de la ubicación de la cámara hacia el objeto a enfocar y a que distancia se halla de este. La calidad de imagen dependerá de esos factores.
- **Altura:** En general altura mínima sugerida para una cámara de seguridad es de 1.90 metros, pero aun así esta queda vulnerable, por ese motivo de que las personas altas puedan tocarla la altura sugerida es de 2.80 metros.
- **Visibilidad:** Es fundamental colocar la cámara de video-vigilancia en espacios vacíos donde no se vean obstruidos la imagen por cualquier motivo.
- **Iluminación:** Es importante evitar las contraluces, luz frontal y minimizar los reflejos al colocar una cámara.

Espacios interiores: En estos ambientes se deben instalar principalmente en las esquinas, ahí es donde pueden tener un mayor ángulo de visión. Es critico ubicarlas en posiciones donde puedan cubrir las entradas como puertas y ventanas.

Espacios al aire libre: En exteriores es importante cubrir los principales puntos de acceso. Las cámaras de exteriores deben de ser visibles para ejercer un efecto disuasorio. Además, deben de ser cámaras resistentes al clima o condiciones que se puedan llegar a dar como lluvia y polvo.

En base a estas características analizaron los planos y se identificaron los puntos críticos donde es crucial el cubrimiento de las cámaras y los puntos estratégicos para donde ubicarlas.

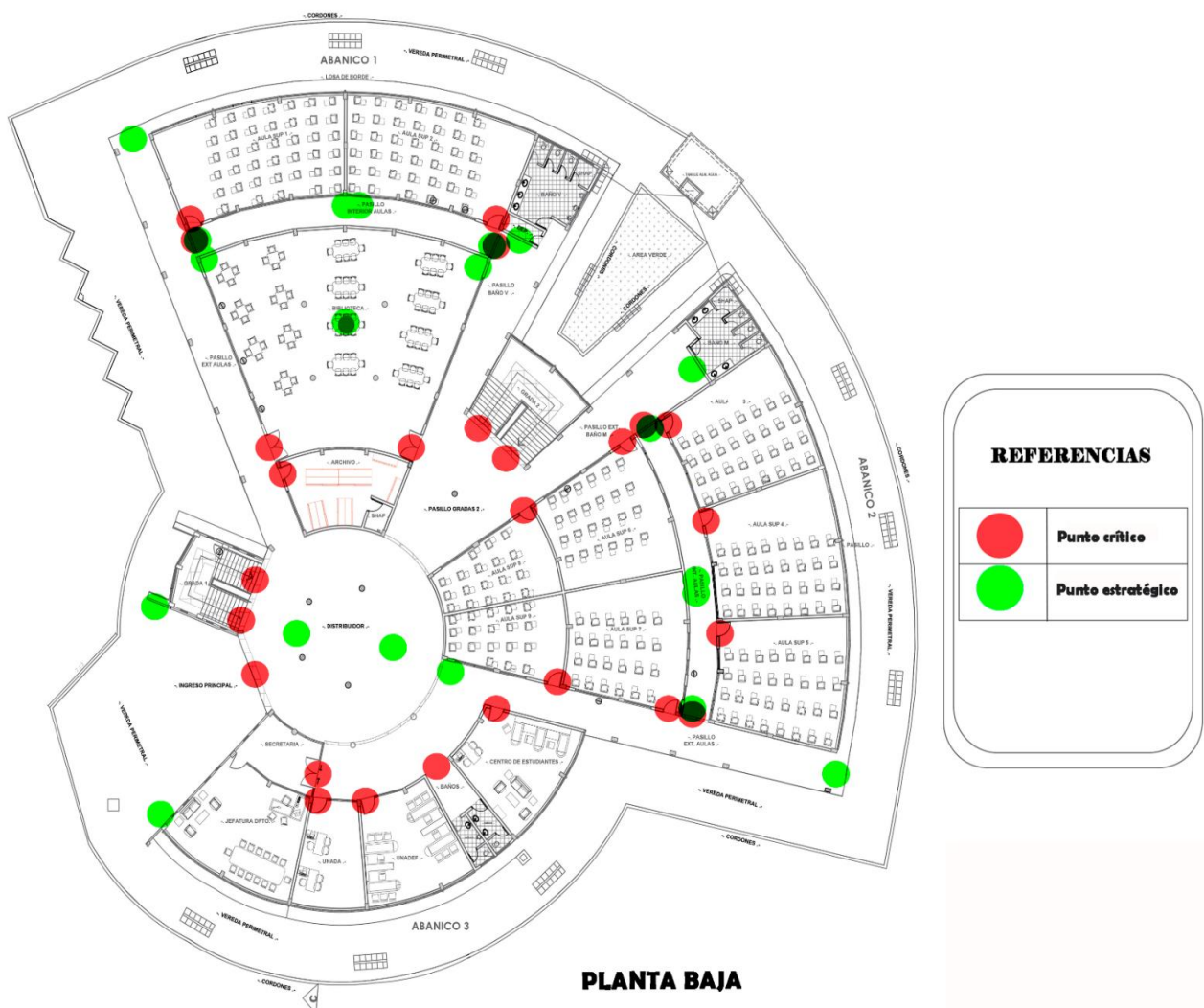


Figura 14. Planta baja puntos críticos y estratégicos

Planta baja	Cantidad de puntos
Puntos críticos	26
Puntos estratégicos	20

Tabla 6. Puntos críticos y estratégicos planta baja

En la planta baja hay un total de 26 puntos críticos y 20 puntos estratégicos.

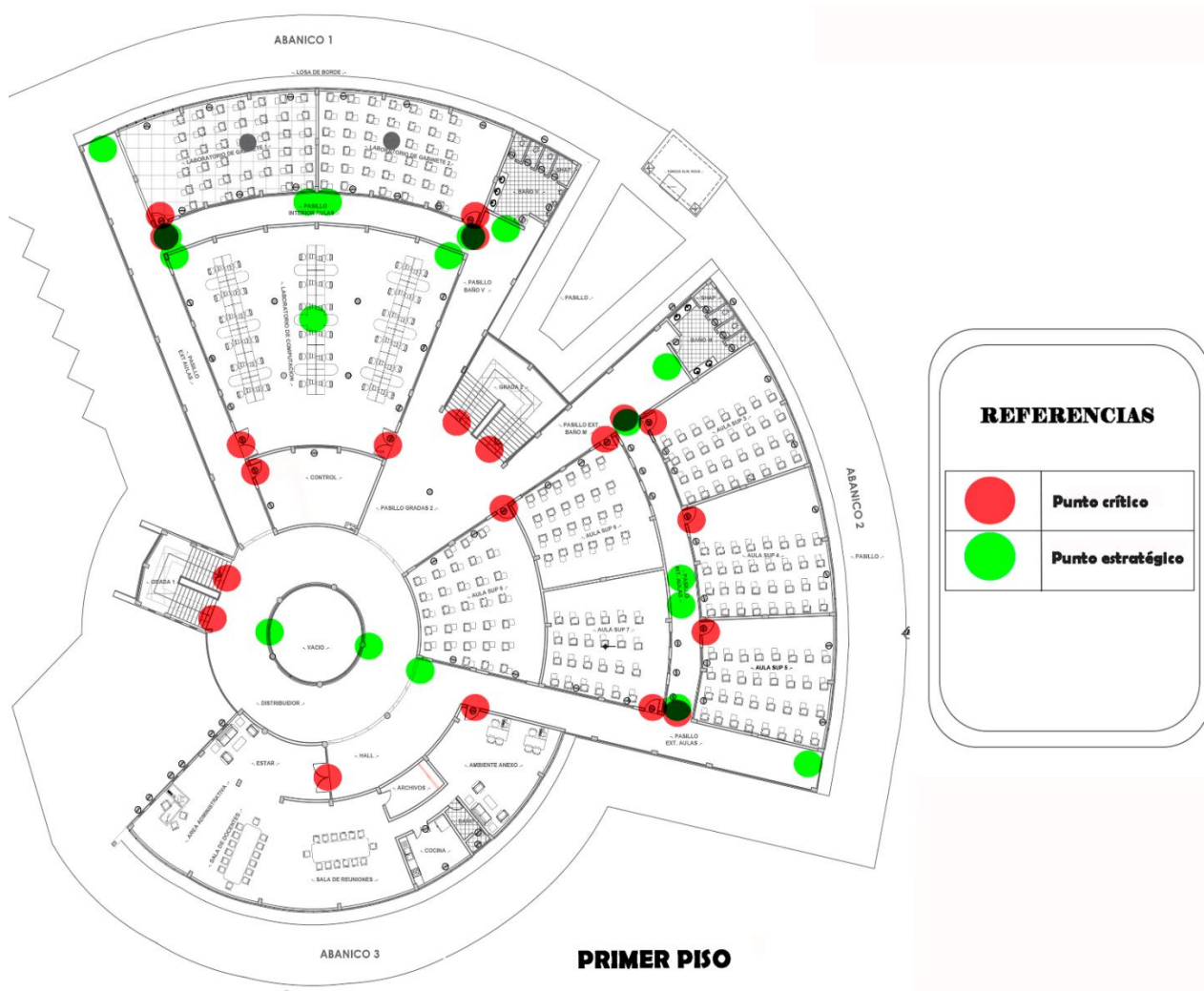


Figura 15. Primera planta puntos críticos y estratégicos

Primera planta	Cantidad de puntos
Puntos críticos	21
Puntos estratégicos	18

Tabla 7. Puntos críticos y estratégicos primera planta

En la primera planta hay un total de 21 puntos críticos y 18 puntos estratégicos.

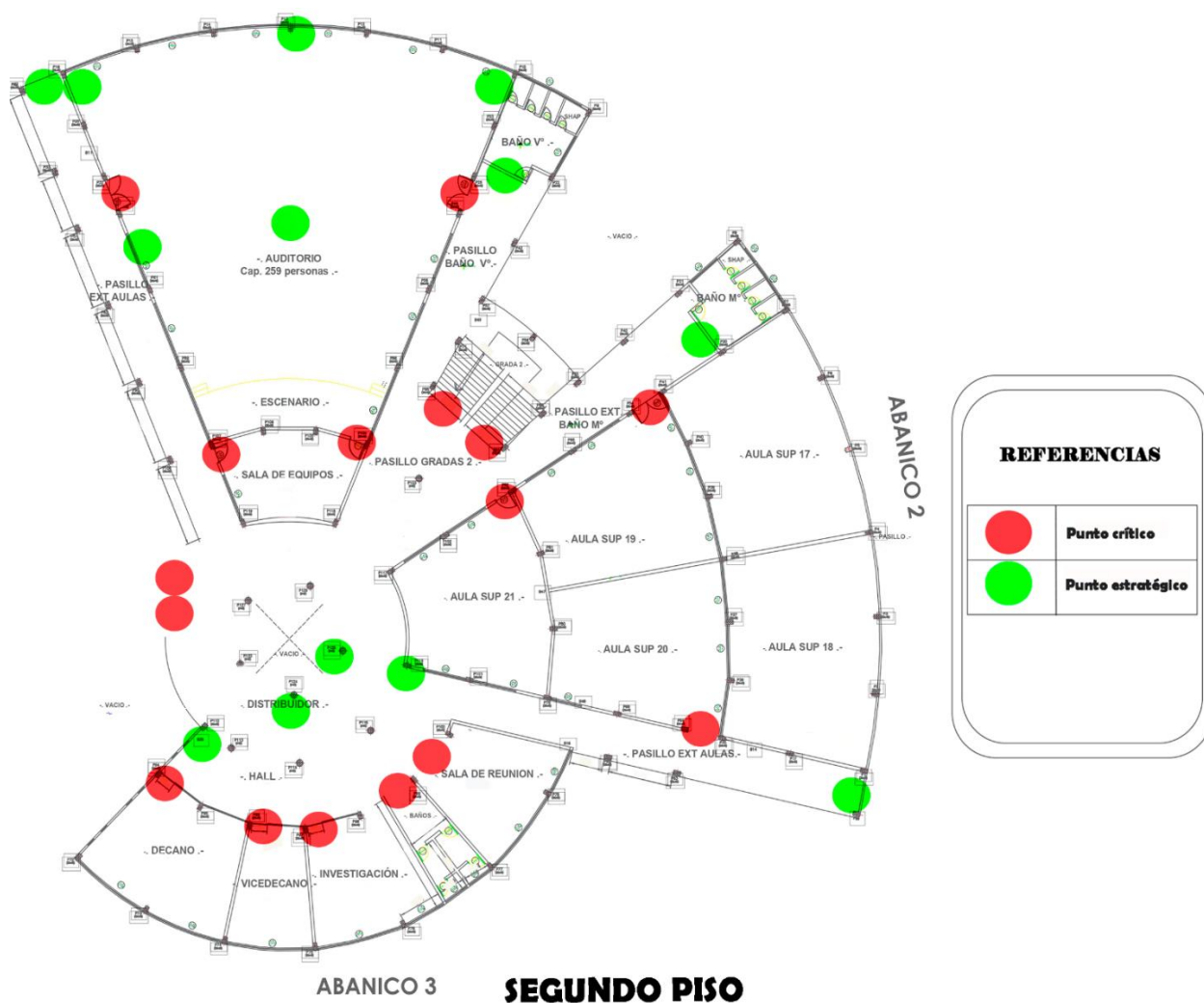


Figura 16. Segunda planta puntos críticos y estratégicos.

Segunda planta	Cantidad de puntos
Puntos críticos	16
Puntos estratégicos	13

Tabla 8. Puntos críticos y estratégicos segunda planta

En la planta baja hay un total de 16 puntos críticos y 13 puntos estratégicos.

En total habría 63 puntos críticos y 51 estratégicos donde ubicar las cámaras de seguridad.

I.6.3.2.2 Diseñar topología de red.

Esta red cubrirá 3 plantas en total, todas con espacios amplios y puntos ciegos, Se ubicarán cámaras de seguridad para interior, exterior y ojos de pez. Las necesarias para cubrir eficientemente el bloque completo.

Teniendo en cuenta los costos, infraestructura y la escalabilidad la mejor opción que se optó por un sistema CCTV ip, esto a través de cámaras ip y cableado utp cat 6a.

Para guiarnos respecto a los equipos se tiene la siguiente figura de referencias.

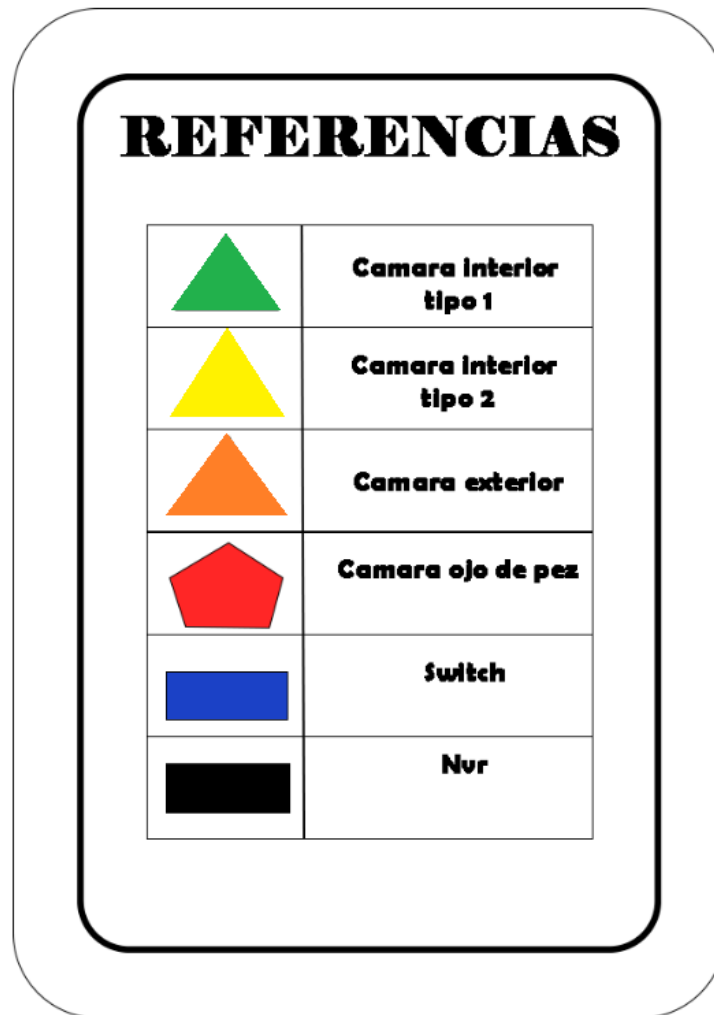
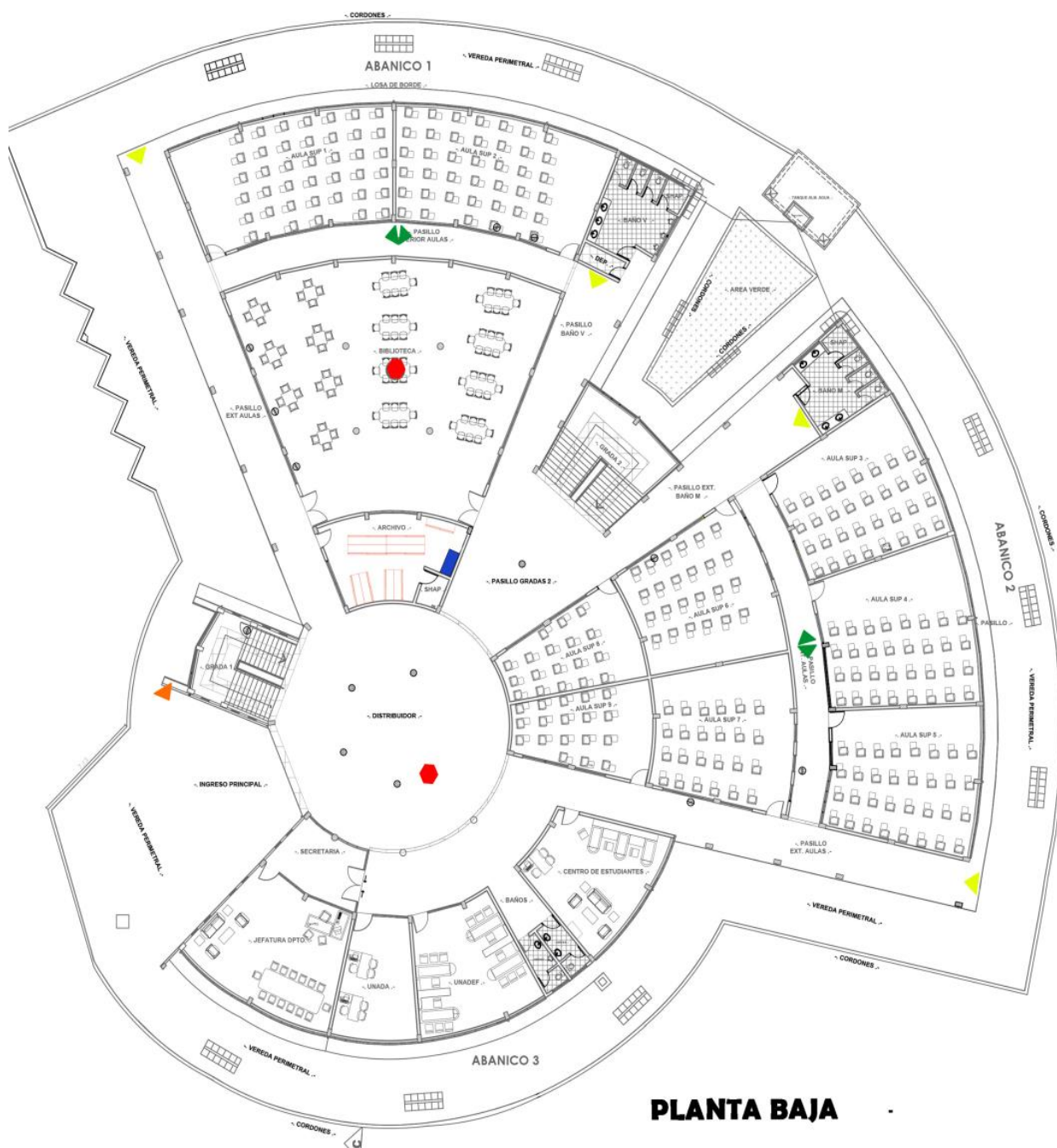


Figura 17. Referencias de las cámaras y equipos

II.1.3.2.2.1 Desarrollo de red planta baja

En la planta baja se realizó este diseño en base a los siguientes indicadores:

- Los pasillos entre aulas al ser cortos se optaron por cámaras de interior tipo 1 de 2 mp, estas tienen menor rango en cuanto a la densidad de los pixeles los cuales a más de 16m aprox se van perdiendo, pero como la distancia máxima estimada a cubrir es de 12m lo cual la calidad se mantendría intacta y se podría reconocer hasta rostros tranquilamente. Además de ser una opción bastante factible según las necesidades y la relación calidad-precio.
- En cuanto a los pasillos largos que van entre 21-32 m aprox. Se optaron por cámaras de interior tipo 2, las cuales pueden soportar más rango que las de tipo 1 por lo tanto su densidad de pixeles no se pierde y la calidad de visualización y grabación queda intacta.
- En la biblioteca y distribuidor se optó por dos cámaras ojo de pez de 360° ya que se prevén que estos sectores estén bastante concurridos y en estos ambientes la necesidad de no dejar puntos ciegos es crucial.
- En la entrada se definió una cámara exterior para vigilar lo que es la entrada y su patio.



PLANTA BAJA

Figura 18. Diseño planta baja cámaras referenciadas

De esta forma quedarían ubicadas las cámaras teniendo en cuentas los puntos estratégicos.

II.1.3.2.2 Desarrollo de red primer piso

En el primer piso se realizó este diseño en base a los siguientes indicadores:

- Del mismo modo que en la planta baja se optó por cámaras de interior tipo 1 para cubrir distancias hasta de 12 m.
- En los pasillos largos se mantienen las cámaras de interior tipo 2.
- En el distribuidor se optó por dos cámaras ojo de pez de 360° en el distribuidor ya que se prevén que este sector esté bastante concurrido y otro en el laboratorio por la seguridad de los equipos y control de acceso a cuarto de equipos.

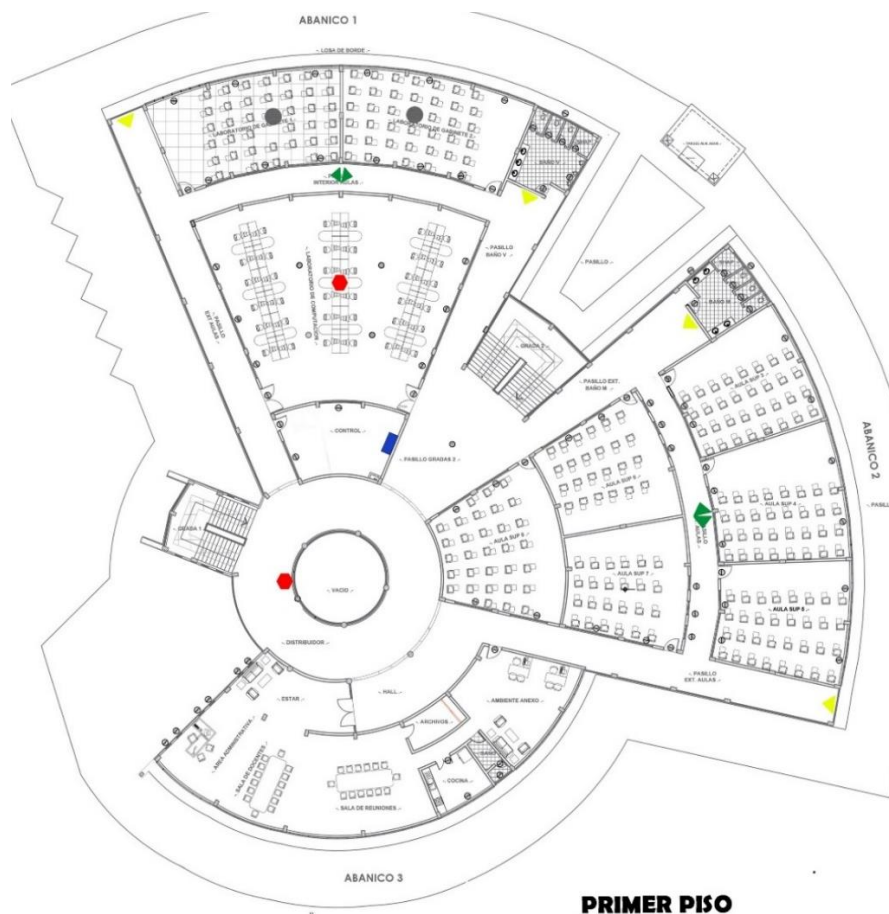
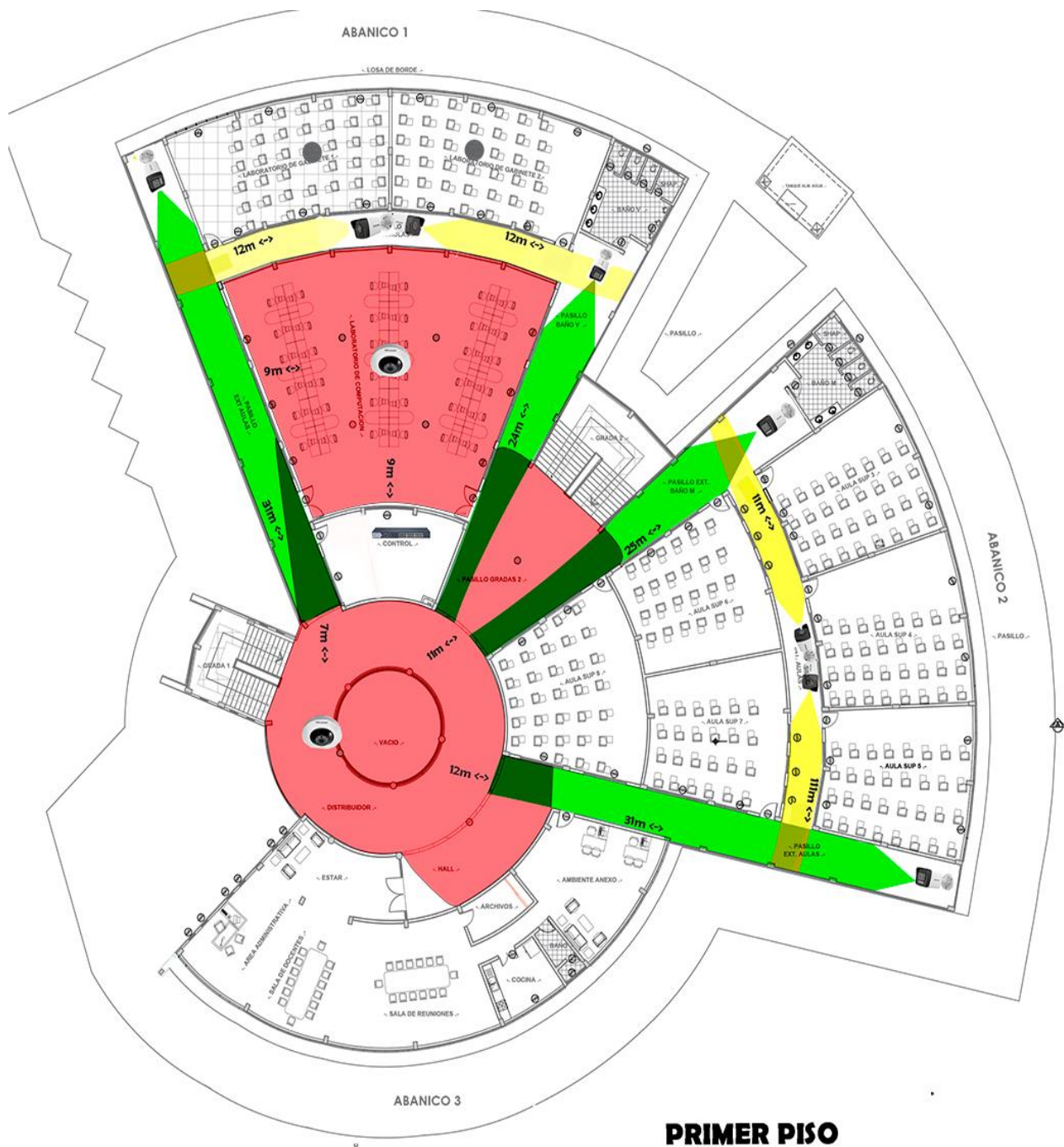


Figura 20. Diseño primer piso cámaras referenciadas

De esta forma quedarían ubicadas las cámaras teniendo en cuentas los puntos estratégicos.



PRIMER PISO

Figura 21. Diseño primer piso cobertura de cámaras y equipos

Se definió las posiciones de las cámaras como también las zonas que cubrirán en base a sus relaciones entre sus ángulos y distancias.

II.1.3.2.2.3 Desarrollo de red segundo piso

En el segundo piso se realizó este diseño en base a los siguientes indicadores:

- En esta planta solo existen pasillos largos por lo tanto se optó por las cámaras de interior tipo 2.
- En el auditorio se optó la cámara ojo de pez que cubre 360° por el motivo de que este ambiente es un sector abierto y grande, así mismo para el distribuidor.
- En el cuarto de monitoreo se halla el nvr y de este se distribuirán a los equipos de monitoreo para hacer seguimiento a las cámaras de vigilancia.

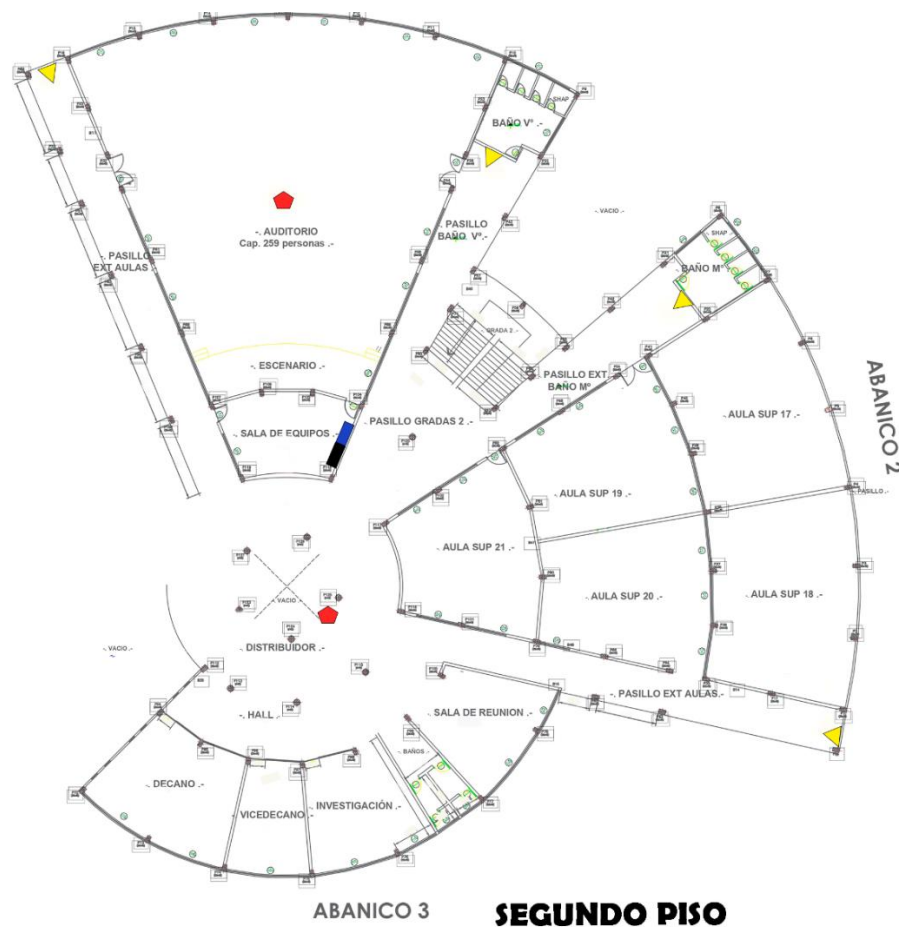


Figura 22. Diseño segundo piso cámaras referenciadas

De esta forma quedarían ubicadas las cámaras teniendo en cuentas los puntos estratégicos.

I.6.3.2.3 Desarrollo lógico

Se desarrolló la red según las especificaciones planteadas logrando así determinar los siguientes puntos:

- Todas las cámaras ip de la planta baja (11 en total) se conectarán directamente a un switch 24 puertos, estos puertos de sobran fueron estimados según las necesidades de la planta y el crecimiento de la red a futuro.
- Las cámaras ip del primer piso (10 en total) se conectarán a un switch 24 puertos también estimando la proyección de la red.
- Las cámaras ip del segundo piso (6 en total) se conectarán a un switch 24 puertos también estimando la proyección de la red.
- Se realizará un backbone tipo distribuido donde los switches del planta baja y segundo piso se conectarán a un switch administrable de 24 puertos del primer piso.
- Se centralizará la red y obtendrá una topología tipo estrella, lo cual facilitará la gestión y el control de la red.
- Siempre se ve optimo hacer la planta baja o la primera planta como el cuarto de equipos donde sería el centro del backbone, por motivos de conexión óptica con otros bloques o incluso la central, otro motivo es el sistema de puesta a tierra. Lo cual en términos de optimización y eficiencia en cuanto a materiales y distancias para cumplir con las reglas de cableado estructurado es lo más factible, por lo tanto:
 - ✓ Se propone definir el cuarto de equipos de la primera planta donde se halla el cuarto de control.
 - ✓ Se propone establecer el centro de monitoreo en la segunda planta donde se halla la sala de equipos actualmente.

I.6.3.2.4 Descripción del diseño

La segunda planta tendrá un nvr y un switch cada de 24 puertos donde en los mismos se conectarán las cámaras ip mediante los puertos PoE. La planta baja igual consta de este switch administrable el total las cámaras de ambas plantas serian 17. 6 de la segunda planta y 11 de la baja.

Estos dos switches de la planta baja y de la segunda planta estarán conectadas directamente a un switch administrable de 24 puertos en la sala de equipos que se halla en la primera planta donde este mismo mediante puertos PoE tendrá conexiones como a las cámaras ip (10 en total), también al mismo tiempo al servidor o router que provea servicios de internet. El nvr estará ubicado en la sala de control en el segundo piso este mismo puede obtener acceso a internet siempre y cuando el router obtenga un proveedor de servicio de internet, dando por sentado a que la red será encriptada, privada y segura.

De este modo la red se centralizará en la primera planta.

I.6.3.2.5 Esquema del diseño lógico generalizado

En base a lo establecido se desarrolló el siguiente diseño lógico.

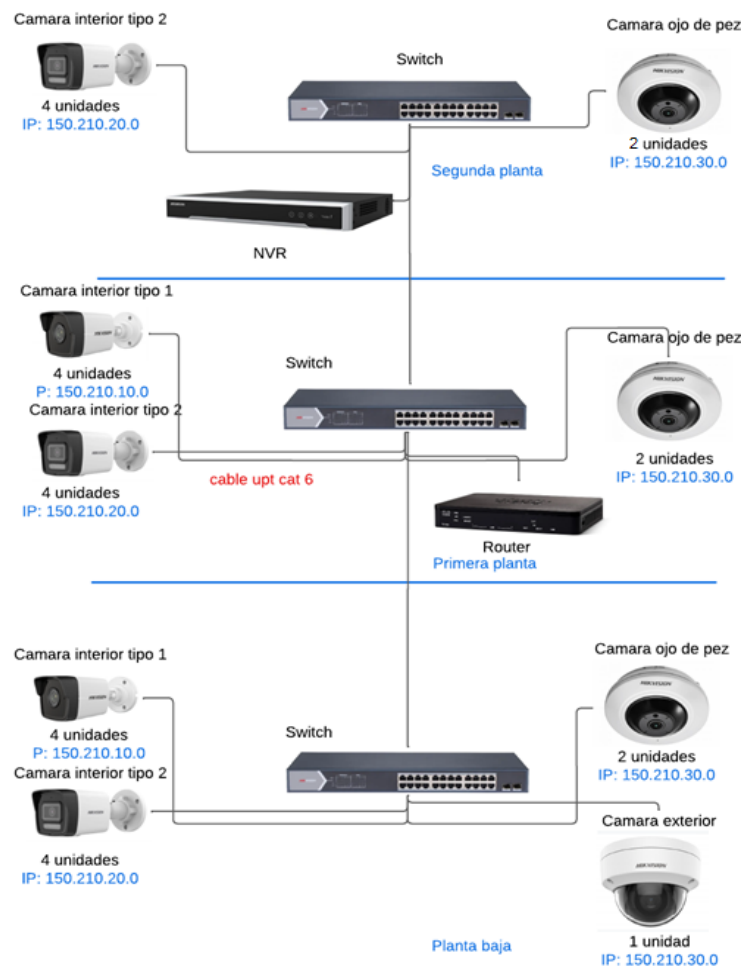


Figura 24. Diseño lógico del sistema de seguridad

Por otra parte, se puede definir los puertos a usarse como también los que se reservarían teniendo en cuenta la escalabilidad del diseño el cual debe de ser adaptable a cambios, estos cambios pueden ser como expansión de la red, adición de nuevos dispositivos, etc.

N°	Unidad o sector	Equipo	Puertos totales	Puertos ocupados	Puertos reservados
1	Planta baja	Switch 1	24	11	13
2	Primera planta	Switch 2	24	10	14
3	Segunda planta	Switch 3	24	6	18
Total			72	27	45

Tabla 9. Puertos reservados switch

Unidad o sector	Equipo	Puertos totales	Puertos ocupados	Puertos reservados
Segunda planta	Nvr	32	27	5

Tabla 10. Puertos reservados nvr

Se pueden observar los puertos reservados tanto como para cámaras como para equipos de cómputo, esto estimando la cantidad de puertos a usarse en un futuro.

I.6.3.2.6 Diseñar modelos de direccionamiento y hostnames

Las cámaras hikvision vienen con una ip por defecto el cual es esta 192.168.1.64, esta dirección no es ideal, porque al tratar de una institución con una red mediana con opciones de escalabilidad es conveniente usar una ip de clase b, esta sería la ip 150.210.0.0.

Al ser una cantidad de cámaras manejables se usará la configuración de ip estáticas en las cámaras ip, para prever que estén todas en la misma red.

Estas cámaras se dividieron en subredes, estos segmentos se definirán según el sector que cubren y la cantidad de las mismas.

A continuación, se desarrollaron tablas donde por sector se define el direccionamiento que tendría cada dispositivo con su determinada puerta de enlace. Cabe aclarar que cada guion entre medio significa la sucesión en un rango.

N°	Unidad o sector	Equipo	Dirección IP	Mascara de subred	Puerta de enlace	Hostnames	Cantidad
1	Pasillo corto	Cámara interior tipo 1	150.210.10.2 - 150.210.10.9	255.255.192.0	150.210.10.1	IPCamera01 - IPCamera08	8

Tabla 11. Direccionamiento de equipos en pasillos cortos

N°	Unidad o sector	Equipo	Dirección IP	Mascara de subred	Puerta de enlace	Hostnames	Cantidad
2	Pasillo largo	Cámara interior tipo 2	150.210.20.10 - 150.210.20.21	255.255.192.0	150.210.20.1	IPCamera09 - IPCamera20	12

Tabla 12. Direccionamiento de equipos en pasillos largo

N°	Unidad o sector	Equipo	Dirección IP	Mascara de subred	Puerta de enlace	Hostnames	Cantidad
3	Patio exterior	Cámara exterior	150.210.30.2 2	255.255.192.0	150.210.30.1	IPCamera21	1

Distribuidor , auditorio y biblioteca	Cámar a ojo de pez	150.210.30.2 3 - 150.210.30.2 8			IPCamera 22 - IPCamera 27	6
---	--------------------------	---	--	--	---------------------------------------	---

Tabla 13. Direccionamiento de equipos en terraza, patio de entrada y distribuidores

I.6.3.2.7 Desarrollar estrategias de seguridad.

En cuanto a la seguridad se aplicó segmentación en nuestra red, esta misma permitirá brindar más control sobre el tráfico de red, optimiza el rendimiento de la red y mejora la situación de seguridad.

Esta es una forma factible de impedir que los usuarios no autorizados accedan a activos valiosos.

En otros aspectos de seguridad Hik-connect mediante la tecnología P2P y el cifrado de enlace completo TLS (protocolo criptográfico) ambas permiten el acceso seguro y remoto a los dispositivos de esta plataforma. Esto garantiza la seguridad de transmisión en la red de los sistemas internos.

Otro aspecto a mencionar en cuanto a la seguridad es la encriptación de la transmisión que esto se puede activar para cada cámara ip mediante el software ivms-4200.

Además de que muchos de los dispositivos hikvision cuenta con el protocolo https, este es el caso de nuestra grabadora de red. En este mismo se puede habilitar la navegación por https, esto hará que todas las comunicaciones entre su navegador y el sitio web estén encriptadas.

Tipo de seguridad	Seguridad física	Seguridad lógica
	Colocación estratégica de equipos	Segmentación vlan
	Monitoreo a tiempo real y grabación las 24 hrs.	Protocolo https, tecnología P2P y el cifrado de enlace completo TLS
	Cubrimiento de puntos críticos	Encriptación de transmisión

Tabla 14. Seguridad física y lógica

I.6.3.2.8 Desarrollar estrategias de administración de red

En cuanto a la administración al ser una red centralizada esta se facilita, en cuanto a las grabaciones serán administradas por el software del grabador (nvr) estas se guardarán por cada mes.

Este software del nvr nos permite gestionar aspectos fundamentales como:

Software de administración	Parámetros que gestiona
iVMS-4200	Tipo de compresión.
	Calidad de grabación.
	Horarios de grabación.
	Alertas por parte de las cámaras.
	Gestión de direcciones ip.
	Gestiona el almacenamiento.
	Prioridades de grabación.
	Modo de grabación.

Tabla 15. Software de administración

I.6.3.3 Fase 3: Desarrollar diseño físico

En esta fase mostraremos lo equipos que serán usados para el diseño físico de la red, pero para esto es importante igual realizar una comparación entre las marcas más grandes que existen en el mercado en cuanto a los equipos a usar como cámaras de seguridad, NVR, switch, etc. Y la comparación de lo que ofrece cada marca.

I.6.3.3.1 Comparación de equipos entre marcas de seguridad

AXIS

Axis, la multinacional sueca lleva más de 35 años en el sector de las comunicaciones y de los equipos de video-vigilancia y seguridad.

También está en la cresta de la ola en cuanto desarrollo y siempre está haciendo nuevas invenciones junto con otras empresas, como por ejemplo lo que escribí hace 2 años sobre

xPredator, unas cámaras térmicas con inteligencia artificial, diseñadas para detectar robos de productos en supermercados. Aunque podemos encontrar equipos pequeños, de uso normal para pequeños y medianos negocios, la realidad es que están especializados en grandes instalaciones y sistemas muy profesionales, como podrían ser campos de fútbol, bancos o aeropuertos.

La calidad de sus cámaras de vigilancia es excelente y muy duradero. Sin embargo, el precio es muy elevado (la calidad se paga). (blogseguridad, 2020)

DAHUA

Dahua es una de las marcas que tienen mejor relación calidad precio.

Invierten mucho dinero en I+D, estando siempre realizando e inventando nuevos dispositivos y aplicaciones para desarrollo de nuevos productos.

Recientemente ha recibido un premio en la 2020 CES Tech Awards, en la categoría de Smart Home con su dispositivo Imou Ranger IQ, una cámara IP diseñada para proteger viviendas y pequeños negocios. No es una cámara cualquiera, sino que está dotada de inteligencia artificial que le permite diferenciar humanos de animales, reconocer las caras, cuando son conocidos, familiares, amigos o intrusos y notificar cuando sea necesario. Tiene alarma integrada y rotación 360° por lo que no se te escapará ni una sola esquina de tu habitación. Incluso tiene una visera que tapará la cámara físicamente cuando estemos en casa para mantener la privacidad.

Respecto las cámaras de vigilancia IP o digitales que se instalan en locales con un DVR o NVR son de muy buena calidad y fiabilidad. He instalado muchas de estas, más que las Hikvision, y son de mis favoritas. El punto bueno es desde luego el precio, que puede ser un 30% más económico que Hikvision. Esto no significa que sea de peor calidad: es de una calidad impresionante, tanto sus cámaras, la calidad de la imagen y la durabilidad de los grabadores. Realmente no tiene nada que envidiar al gigante número 1. (blogseguridad, 2020)

HIKVISION

Hikvision siempre ha sido creador de tecnología puntera en sus dispositivos de seguridad.

En estos últimos años ha recibido varios premios relacionados con el reconocimiento térmico en sus cámaras, tal y como presumen ellos mismo desde su propio blog. En los certámenes de ESX Innovation Awards 2019 (USA), Detektor International Award (EMEA) o Security & Fire

Excellence Awards 2019 ha recibido premios a la alta precisión, resistencia, fiabilidad e innovación en sus cámaras térmicas, en cuando a la detección de incendios y fiabilidad de alarmas.

Respecto a las cámaras de video-vigilancia destaca la fiabilidad y calidad, así como la durabilidad. Actualmente su catálogo es muy amplio, y podemos elegir desde cámaras domo HD (720P) hasta lo más actual, como podría ser cualquier cámara a 4K reales, sea por IP o cable tradicional (digital).

Los sistemas que están preparados para una fácil instalación o que son auto-instalables funcionan a la perfección y, a pesar de su sencillez, son muy completos. Probablemente sean las mejores cámaras actuales, en base a la calidad. Incluso el sistema de alarma de hikvision es muy completo y sencillo. (blogseguridad, 2020)

Viendo la practicidad, variedad, calidad y conociendo el mercado que ofrece, se optó por elegir cámaras de esta marca.

También se compararon los nvr.

AXIS

Con una grabadora de vídeo en red Axis tendrá en sus manos una solución en alta definición, fiable y fácil de instalar, que se adapta perfectamente a la amplia gama de productos de red Axis. Los grabadores vienen con todo el software necesario ya cargado, lo que incluye licencias del software de gestión de vídeo. En Axis, todas las consultas se gestionan a través de un único canal, por lo que puede tener la tranquilidad de que cualquier problema se resolverá de forma rápida y eficiente. Contamos con más de 100 técnicos de soporte técnico altamente experimentados en todo el mundo, preparados para ayudarle cuando y donde lo necesite. (sitejal, s.f.)

DAHUA

Los NVR Dahua son grabadores profesionales de cámaras IP con la mejor relación calidad precio, además de las cámaras IP del mismo fabricante, Dahua y X-Security, son compatibles con todas las cámaras IP Onvif. Disponemos de NVRs para cámaras IP de todas las resoluciones, con conexión Ethernet o Wifi, con puertos PoE, con entrada de alarmas, salidas de vídeo VGA y HDMI hasta 4K, que admiten de 1 hasta 4 discos duros. Acceso remoto por Internet con un ordenador, un móvil o una Tablet, IOS o Android. (evoseguridad, s.f.)

Dahua es una marca líder de mercado en cuanto a la video-vigilancia, a continuación, según (integrarcctv, s.f.) se mostrarán algunos puntos a considerar para elegir sus equipos nvr:

- Gracias al estándar HDCVI, soporta transmisión de múltiples señales sobre el mismo cable coaxial, Estos serían: Potencia, datos, audio y video.
- Todos los DVR/NVR de Dahua permiten combinar diferentes modos de grabación tanto en la misma franja horaria como en horarios diferentes.
- La función P2P (Peer to Peer o red de pares) te permite acceder a un DVR o NVR Dahua de manera remota sin tener que incurrir en complicadas configuraciones o reenvíos de puertos en tu router o el de tu red local.

HIKVISION

Las cámaras de calidad superior merecen una NVR de máxima calidad. Las grabadoras de video en red integradas de Hikvision ofrecen las ventajas de administrar el ancho de banda y el almacenamiento con la última tecnología de compresión H.265+ Los NVR todo en uno cuentan con potentes capacidades, que soportan una resolución de hasta 32 MP para la grabación. La salida de ultra alta definición de hasta 4K es ahora compatible con todos los modelos de NVR, desde el nivel básico hasta el profesional. Para la seguridad de los datos, las grabadoras de video en red de Hikvision ofrecen funciones RAID, reposición en caliente N+1 y ANR, asegurando una grabación de video estable y confiable. Con las unidades de Aprendizaje Profundo, la grabación de video de Hikvision se vuelve más potente y más inteligente que nunca. (hikvision, 2021)

Conociendo más la marca y los productos que este ofrece además de la variedad y calidad se optó por elegir NVR de esta marca.

I.6.3.3.2 Tecnologías y equipos a implementar

Hoy en día al tener tantas opciones se seleccionaron los equipos a usar como también la descripción del por qué:

Para el diseño de esta red se usará cable utp cat 6 a que tiene una velocidad de transmisión de hasta 10 Gbps y un ancho de banda de 500 MHz. Además de ser 100 % cobre, además está trenzado para brindar aislamiento adicional para reducir la diafonía. Cabe mencionar que es compatible con el cable cat5e y cat6.

Se usará este tipo de cable ethernet tanto como para el cableado horizontal como para el vertical.

II.1.3.3.2.1 Cámaras

Cámara interior tipo 1

Se eligió la cámara bala **DS-2CD1023G0E-I** por el motivo principal de ser una buena opción en cuanto calidad precio, esta cuenta con alimentación PoE y con iluminación infrarroja que pueden llegar a cubrir hasta 30 metros. Con una calidad de 2 mp (1920×1080) suficientes para brindar una calidad de imagen totalmente satisfactoria a los 12 metros de distancia y contiene compresión de video H.265+.

Cámara interior tipo 2

Se eligió la cámara bala **DS-2CD1043G2-LIU** al ser un tipo de cámara que cuenta con alimentación PoE además de tener iluminación infrarroja que llega a cubrir hasta 30 metros. Con una calidad de 4 mp (2560 X 1440) a diferencia de la de 2 mp esta cámara tiene que cubrir más espacio por lo tanto más megapíxeles son necesarios para no perder calidad, además contiene compresión de video inteligente de H.265+.

Cámara exterior

Se eligió la cámara domo **2CD1123G0E-I** porque es resistente al agua y al polvo y resistente al vandalismo, características necesarias para ubicarla en exterior. También cuenta con alimentación PoE y cumple satisfactoriamente la relación calidad precio, cubre el espacio asignado satisfactoriamente con una distancia focal de 2,8 mm obtiene un campo de visión horizontal 112,1° y campo de visión vertical 60,0°. Con una calidad de 2 mp (1920 X 1080) los suficientes para el área que deseamos cubrir, además contiene compresión de video inteligente de H.265+.

Cámara ojo de pez

Se eligió la cámara ojo de pez **DS-2CD2955FWD-IS** principalmente por el espacio que cubre como su nombre lo indica es ojo de pez y cubre un ángulo de 360°. Este mismo cuenta también con alimentación PoE y luz infrarroja de hasta 30m. Con una calidad de 5 mp (2560 X 1920) los suficientes para el área que deseamos cubrir, además contiene ir hasta 8 metros y una compresión de video inteligente de H.265+.

II.1.3.3.2 Equipos de grabación y switch

Se eligió el switch **DS-3E1526P-SI** este es administrable por lo tanto permite priorizar el tráfico y los recursos para que el rendimiento de una aplicación o servicio sea optimo, monitorea el estado de la red, mandar alarmas de red, poe hasta 25 metros para encender las camaras.

Se optó por el NVR de hikvision **DS-7732NI-M4(STD)** el cual cuenta con 4 espacios de almacenamiento que soportan hasta 14 Tb cada uno, alimentación PoE, soporta resoluciones hasta 8k y un ancho de banda de Ancho de banda de 320 Mbps entrada / 400 Mbps salidas. Estas características cubren totalmente las necesidades del sistema.

II.1.3.3.2.3 Cableado

Se decidió por cable utp cat 6 al usar PoE el de sus 4 pares trenzados de cobre en este cable es indispensable para disipar el calor óptimamente, además puede transmitir ethernet de 10 gigabits a distancias de 100 metros. Aparte es más económico este tipo de cable a comparación con el cable coaxial que además no soporta PoE.

A continuación, se determinó unas tablas con los equipos a usar y sus características:

EQUIPO	CARACTERISTICAS TECNICAS
Cámara interior tipo 1	• CMOS de barrido progresivo de 1/2,7" • IP: 2 MP • Compresión: H.264 / H.265 / MJPEG / H.265+
CAMARA IP BULLET FULL HD 2MP 2.8MM DS-2CD1023G0E-I	• Lente: f = 2,8 mm (ángulo de visión 112,1°)



- Grabación: Transmisión principal 1920×1080, 1280×720 - 25 fps, Sub Stream 640×480, 640×360 - 25 fps;
- Funciones: día/noche (ICR) / AGC / 3D DNR / BLC / DWDR / ROI
- Iluminación IR de hasta 30 m
- micrófono incorporado
- Alimentación CC 12 V/PoE.

Cámara interior tipo 2

**CAMARA IP BULLET 4MP 2560 X
1440 LENTE 2.8MM IR40METROS
HYBRID ACUSENSE IP67 DS-
2CD1043G2-LIU**



- Imágenes de alta calidad con resolución de 4 MP
- Apoya la detección de personas y vehículos
- Smart Dual-Light: tecnología avanzada con largo alcance
- Micrófono incorporado para seguridad de audio en tiempo real
- Resistente al agua y al polvo (IP67)
- Tecnología de compresión H.265+ eficiente
- Tipo De Luz Suplementaria: IR, luz blanca
- Gama De Luces Suplementarias: Hasta 30 metros
- Evento Básico: Detección de movimiento (admite activación de alarma por tipos de objetivos específicos (humanos y vehículos)), alarma de manipulación de vídeo, excepción.
- Fuerza 12 VCC $\pm$ 25%, 0,4 A, máx. 5 W, enchufe coaxial de Ø5,5 mm, protección contra polaridad inversa, PoE: IEEE 802.3af, Clase 3, máx. 6,5 vat.

Cámara exterior

CAMARA DOMO IP 2MP FULL HD IK10 IR30M 2.8MM DS- 2CD1123G0E-I



- Resolución máxima: 2 Megapíxel (1920 X 1080).
- Iluminación mínima: color 0.01 Lux @ (F2.0, AGC ON).
- Resistente al agua y al polvo (IP67) y resistente al vandalismo (IK10).
- Iluminación mínima: B/N 0 Lux con IR.
- Día / Noche Real (filtro ICR).
- Distancia focal: 2.8 mm (Angulo de visión 112.1°)
- Distancia de infrarrojo: 30 mts Smart IR.
- Funciones normales: dWDR / D3 DNR / BLC.
- Compresión: H.265+ / H.265 / H.264+ / H.264.
- Compatible con la plataforma de Hik-Connect.
- Alimentación: 12 Vcc / PoE 802.3 af / 5 W

Cámara ojo de pez

**CAMARA DOMO IP 5MP 2560 X 1920
180° FISHEYE IR 8 MTS AUDIO DS-
2CD2955FWD-IS**



- Imágenes de alta calidad con resolución de 5 MP
- Excelente rendimiento con poca luz.
- Tecnología de compresión H.265+ eficiente para ahorrar ancho de banda y almacenamiento
- Imágenes claras incluso contra una fuerte luz de fondo gracias a la tecnología WDR real de 120 dB.
- Admite 14 modos de visualización
- FOV: FOV horizontal 180 °, FOV vertical 180°
- Flujos de vídeo duales
- DC12V y PoE (802.3af)
- Reducción digital de ruido
- Admite almacenamiento integrado, hasta 128 GB
- Alcance IR de hasta 8M
- Audio/Alarma

SWITCH

24 Port Gigabit Smart POEwitch DS-3E1526P-SI



- 24 puertos PoE 802.3af/at RJ45 de 10/100/ 1000 Mbps.
- 2 puertos SFP para fibra óptica de 1Gb.
- Gestión de topología de Red.
- Envío de alarmas de Red.
- PoE extendido de hasta 250 m para encender cámaras.
- Compatible con plataforma de administración Hik-PartnerPro, HikCentral e iVMS4200.
- Presupuesto de energía PoE 370 W.
- Soporta QoS para proporcionar un ancho de banda más estable y menor latencia para tráfico de Red.
- Soporta VLANs Para dividir la Red de manera virtual para mejorar la seguridad/ comunicación de la Red.

NVR

NVR HIKVISION DS-7732NI-M4



- Grabador NVR para cámaras IP
- Grabador NVR para cámaras IP 32 CH Ancho de banda entrante soportado 320 Mbps
- Resolución máxima 32 Mpx
- Compresión H.265+/H.265/H.264+/H.264
- Salida HDMI 8K, HDMI 4K y VGA
- Alarmas
- Espacio para 4 HDD

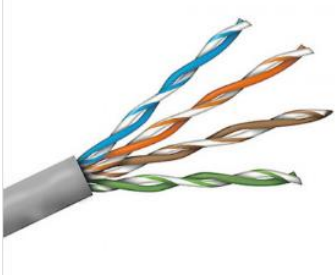
CABLE UTP CAT 6 	• Tipo de aislamiento: polietileno. • Tipo de cubierta: PVC negro con propiedades retardante a la llama y resistente a la intemperie. • Separador de polietileno para asegurar alto desempeño contra diafonía. • Para conexiones y aplicaciones IP.
Seagate Exos 7E8 6TB 512e SATA 256MB caché 3.5 pulgadas disco duro empresarial (ST6000NM0115) 	• Capacidad formateada de almacenamiento de datos de 6 TB (6 Terabytes) • Velocidad de transferencia de datos hacia/desde medios 6,0 Gb/s • Búfer de caché de 256 MB • Tiempo de búsqueda promedio 8,9 ms • Velocidad de rotación 7200 RPM • Interfaz SATA 6.0Gb/s DIMENSIONES • (Alto x Ancho x Fondo) Unidad 4 pulgadas x 5,8 pulgadas x 1 pulgada • Unidad de peso 1,3 libras • Requisitos del sistema PC

Tabla 16. Equipos a usar y sus características

II.1.3.3.2.4 Calidad de servicios en equipos

Esta red debe de ser diseñada teniendo en cuenta la necesidad de brindar disponibilidad en cuanto a los servicios y la capacidad de poder priorizar unos sobre otros.

Equipos	QoS	Prioridad de servicios	Audio	IR	Alarma
Nvr	Si	Si			
Switch	Si	Si			
Cámara interior tipo 1			Si	Si	No
Cámara interior tipo 2			Si	Si	No
Cámara ojo de pez			Si	Si	Si
Cámara exterior			No	Si	No

Tabla 17. Calidad de servicios

El nvr y switch cuentan con gestión de servicios los cuales permiten gestionar los mismos, estos serían las cámaras que tienen audio, IR y alarma.

I.6.3.4 Fase 4: Aprobar, optimizar y documentar diseño

I.6.3.4.1 Configuración e instalación de cámaras de seguridad

Para la instalación del sistema de seguridad se determinaron los siguientes equipos:

Un nvr de 32 puertos que soporta altas resolución hasta de 8k, estos tendrán dos discos de 6 tb los cuales almacenarán las grabaciones. Se usarán tres switches de 24 puertos los cuales serán administrables. En cuanto a las cámaras de interior serian un total de 8 cámaras de interior tipo 1, 12 cámaras de interior tipo 2, 1 cámara exterior y 5 cámaras ojo de pez. Se usarán equipos PoE el mismo alimentado por el cable utp categoría 6.

Se necesitará de un pc para la configuración y activación de las cámaras ip, esto se puede realizar por medio de un navegador web, software del nvr o por medio de la herramienta SADP. A continuación, se muestra una imagen de la interfaz de la herramienta SADP.

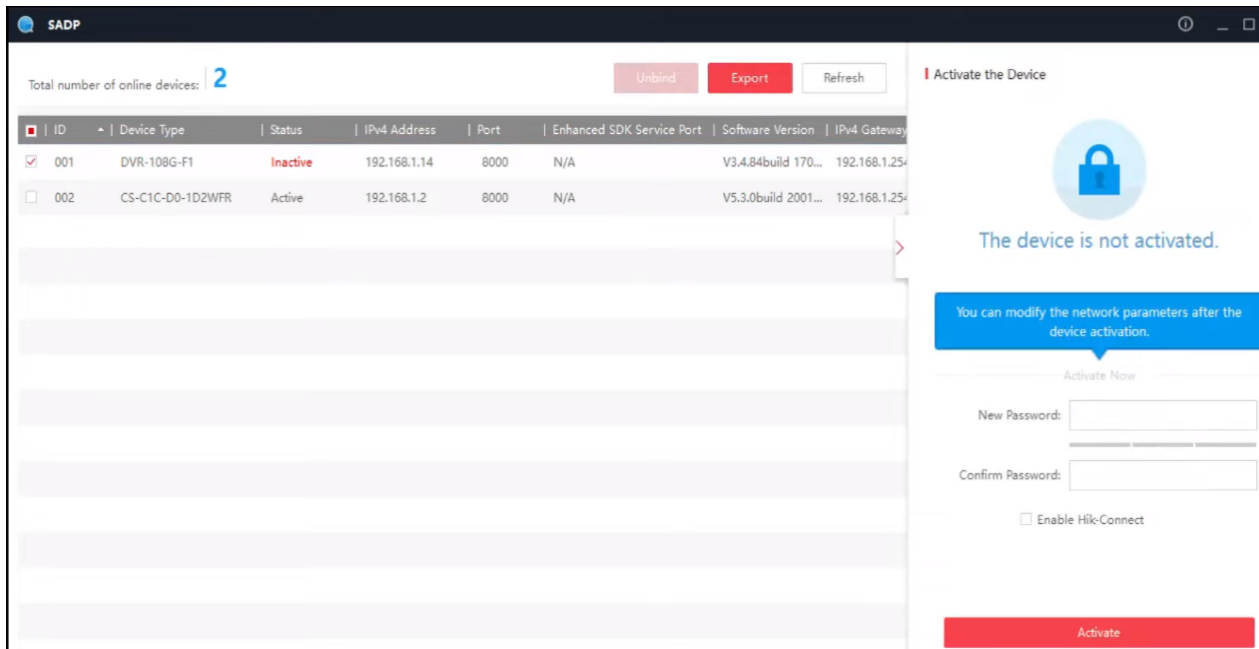


Figura 25. Software sadp

En el caso de la segunda es el software en el cual se maneja el grabador (nvr o dvr) el mismo se descarga e instala según la versión que indica la documentación del equipo.

Este mismo software detectara cualquier dispositivo hikvision que se encuentre en la red local, ya sea cámara ip, un dvr o un nvr. Sin importar la ip que tenga por defecto, de esta manera se puede activar la cámara, cambiar la dirección ip, habilitar el modo dhcp, entre otros.

Ahora en cuanto a la configuración en general se puede hacer desde un navegador web o desde el software del nvr el cual sería el **IVMS-4200**. Se muestra la interfaz para logearse en la siguiente imagen.

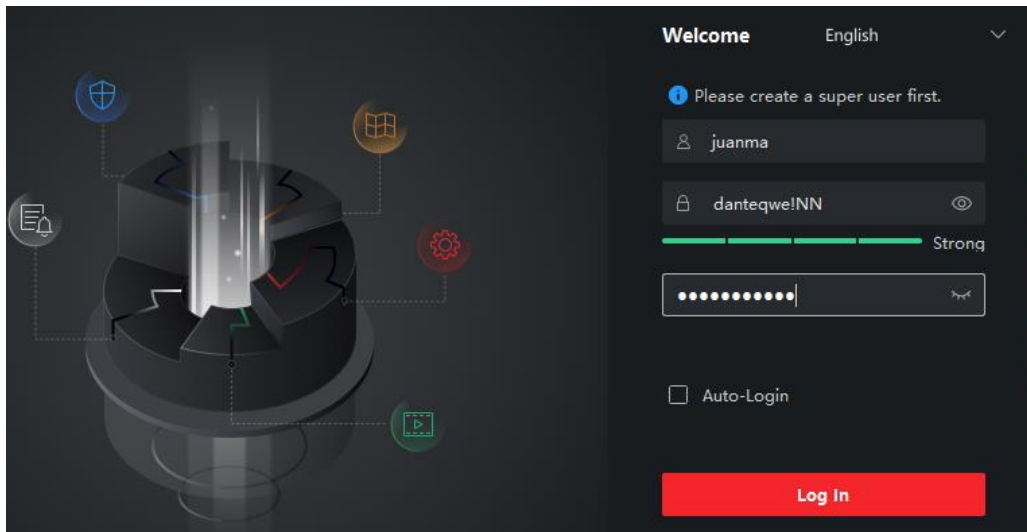


Figura 26. Interfaz de inicio de sesión

Ya dentro del software ponemos la ip del nvr, añadimos el usuario y contraseña y esto nos llevara a la página de hikvision donde nos mostrara la interfaz del nvr, en el mismo se descarga los plugins. Mediante este interfaz podremos realizar acciones como configurar la puerta de enlace, la dirección ip, mascara de subred, añadir cámaras ip mediante su ip estática ya asignada por el software SADP todo esto por el motivo de que las cámaras estén en una misma red que el grabador. La interfaz del software se muestra en la siguiente imagen.

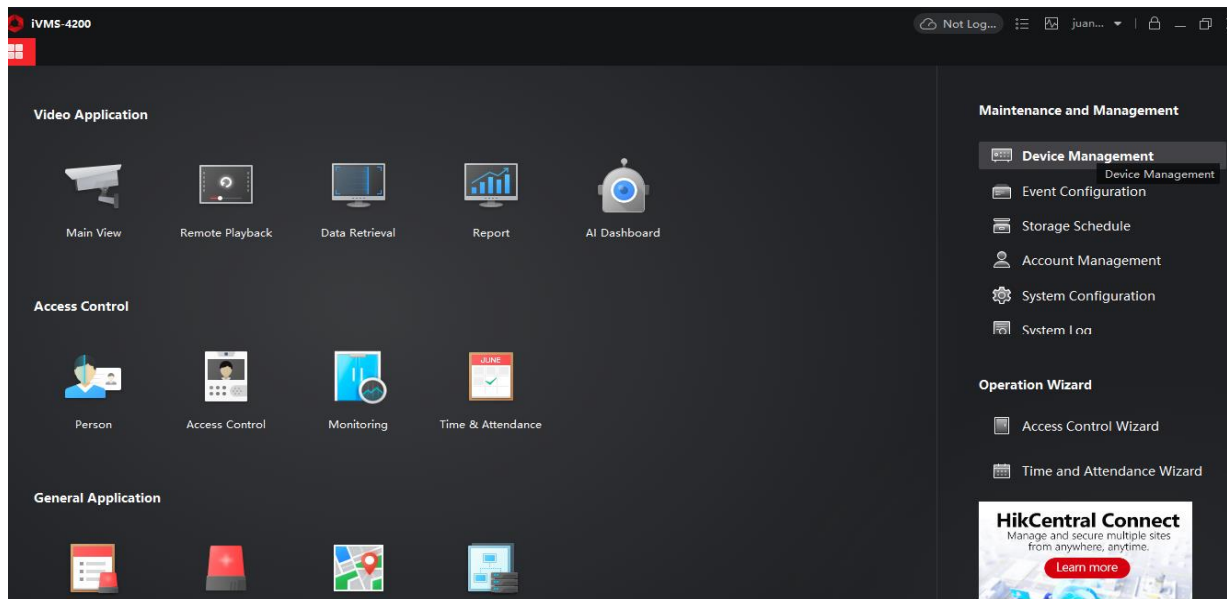


Figura 27. Interfaz del menú del software

I.6.3.4.1.1 Añadir cámara ip y configuración de grupos

Primeramente, nos vamos al apartado de device management luego a add y ahí nos saltara el siguiente menú.

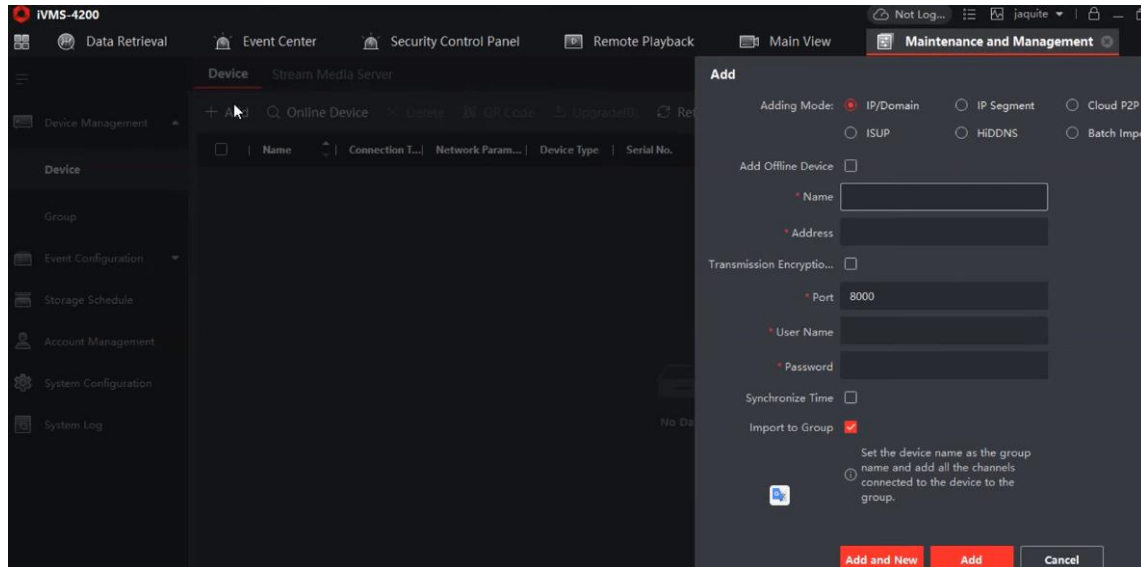


Figura 28. Adición de cámara ip

Y aquí podremos añadir el nombre, dirección ip, nombre del usuario y su respectiva contraseña. Además, hay dos casillas una de ellas es sincronizar el tiempo de la cámara respecto al ordenador y la otra es import to group lo cual crea automáticamente una carpeta donde estará la cámara. En este caso la cantidad de cámaras es considerable por lo cual conviene crear carpetas personalizadas.

Se crearán 3 carpetas donde las cámaras estarán divididas por piso, para esto se selecciona add group, se añade el nombre de la carpeta y se importan las cámaras que ya han sido añadidas.

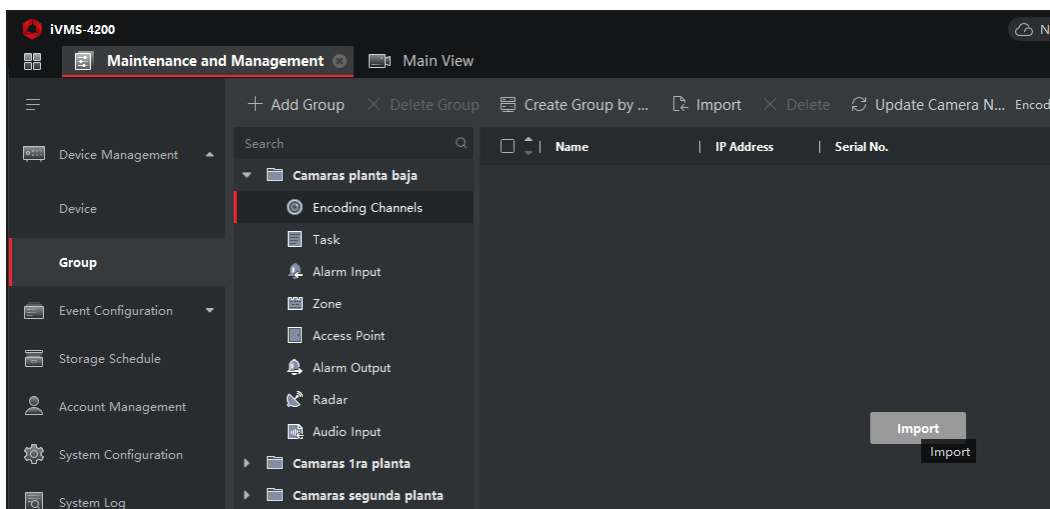


Figura 29. Visualización de carpetas

Se vería de la siguiente forma.

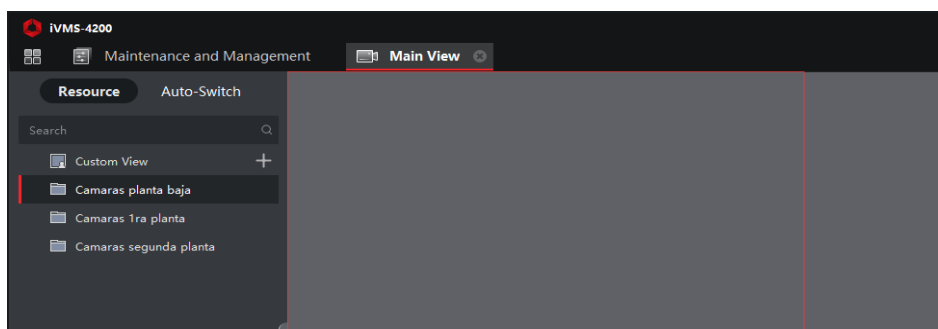


Figura 30. Visualización de carpetas creadas

Para configurar el almacenamiento se va a configuración remota de ahí a general en storage en este espacio nos mostrara los discos que tenemos disponibles. Estos discos se añadirán mediante lo identifiquen el pc.

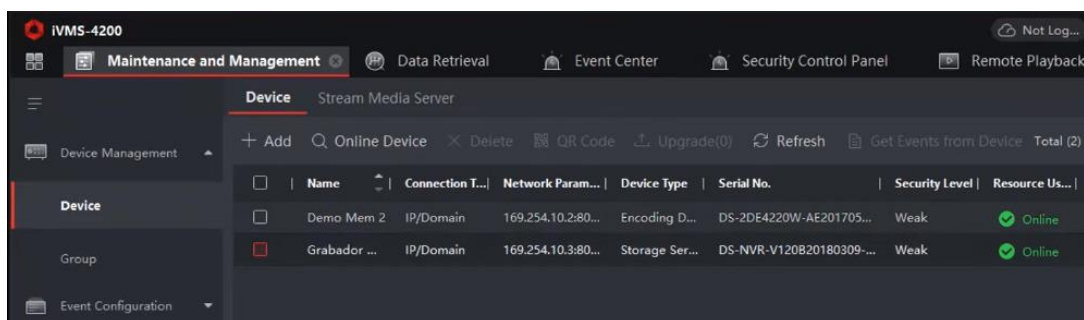


Figura 31. Gestión de storage 1

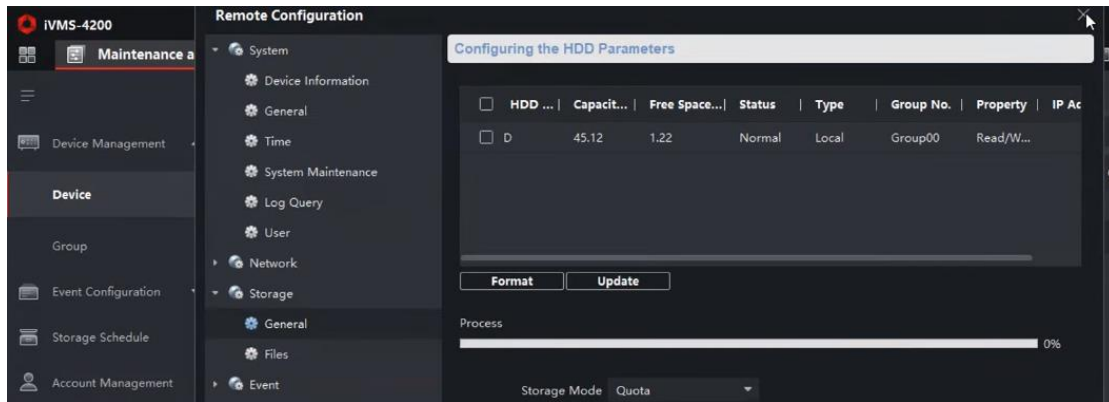


Figura 32. Gestión de storage 2

I.6.3.4.2 Testeo y resultados de las cámaras de seguridad

Para testear la funcionalidad, límites y alcances con las cámaras de seguridad se optó por emplear el software **IP Video System Design Tool** donde se realizó un testeo con cada tipo de cámara:

- Cámara interior tipo 1.
- Cámara interior tipo 2.
- Cámara exterior.
- Cámara ojo de pez.

Cada una de estas cámaras contara con parámetros a llenar, estos serían:

PARAMETROS	DESCRIPCION
Altura de instalación	Altura que se halla instalada la cámara (metros).
Formato CC/CMOS	Es el formato del sensor de imagen (pulgadas).
Resolución	Resolución de cámara.
Distancia focal	Longitud focal del objetivo de la cámara. (distancia entre el centro óptico de la lente y el sensor de la cámara).
Distancia hasta el objeto (máxima)	La distancia en la que está el sujeto de prueba.
Altura del objeto	Es la altura del sujeto de prueba.
Ancho CDV	Es el ancho de campo de visión.

Tabla 18. Descripción de parámetros

II.1.2.4.2.1 Testeo cámara interior tipo 1

Se identifico nuestra cámara en la base de datos del software, esto según el fabricante y modelo.

FABRICANTE	MODELO
Hikvision	DS-2CD1023G0E-I

Tabla 19. Fabricante y modelo cámara interior tipo 1

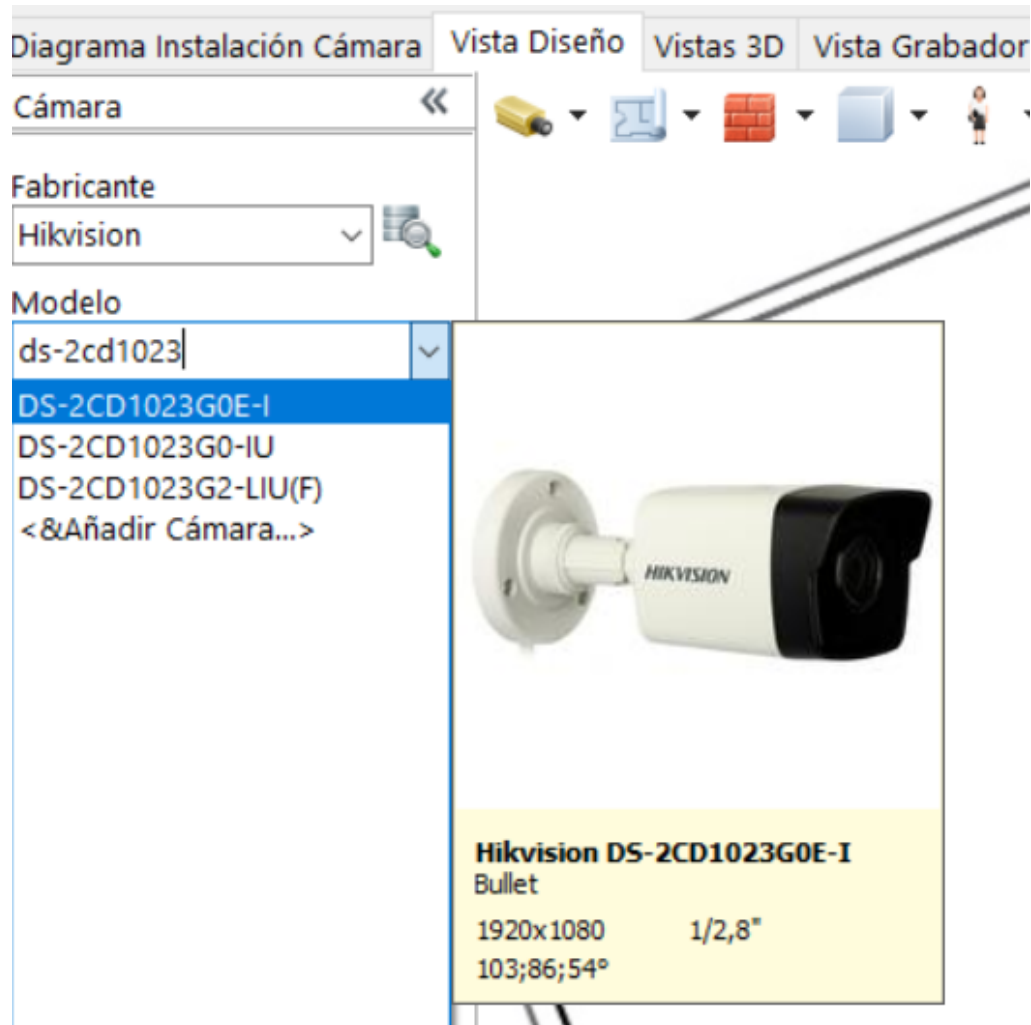


Figura 33. Identificación de cámara interior tipo 1

Para realizar el testeo de la cámara de seguridad se tomaron en cuenta los siguientes parámetros.

PARAMETROS	VALORES
Altura de instalación	2,8 (m) (recomendada)
Formato CC/CMOS	1/2,8 (optima)
Resolución	1920x1080
Distancia focal	2.8 (mm)
Distancia hasta el objeto (máxima)	12 (m)
Altura del objeto	1,7 (m)
Ancho CDV	8,5 (m)

Tabla 20. Parámetros cámara interior tipo 1

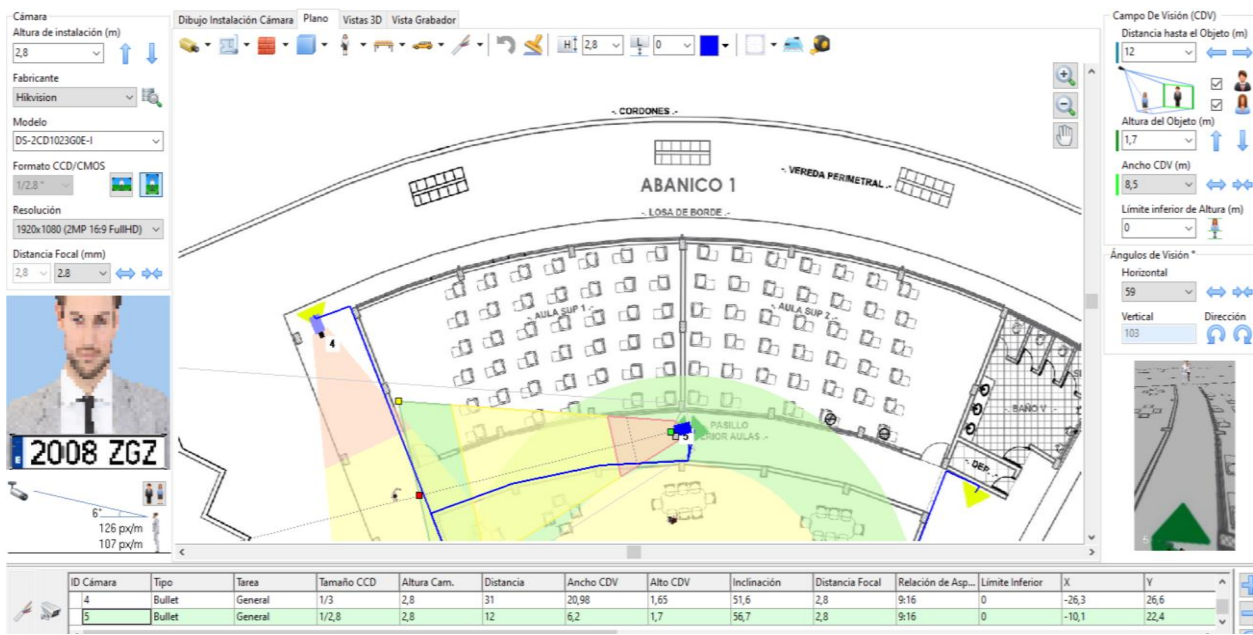


Figura 34. Parámetros cámara interior tipo 1

Una vez añadidos los parámetros el software nos soltara los siguientes resultados.

Cámara 5

Hikvision: DS-2CD1023G0E-I



Resolución: 1080x1920
Tamaño CCD: 1/2,8 ; 9:16
Distancia Focal: 2,8
Altura Cam.: 2,8 m
Inclinación: 56,7°
Ángulos de Visión °: 59°; 103°
Distancia: 12 m
Ancho CDV: 8,5 m
Píxeles en el Objeto: 107 px/m
Zona muerta: -0,36 m (Ancho: 0,82 m)

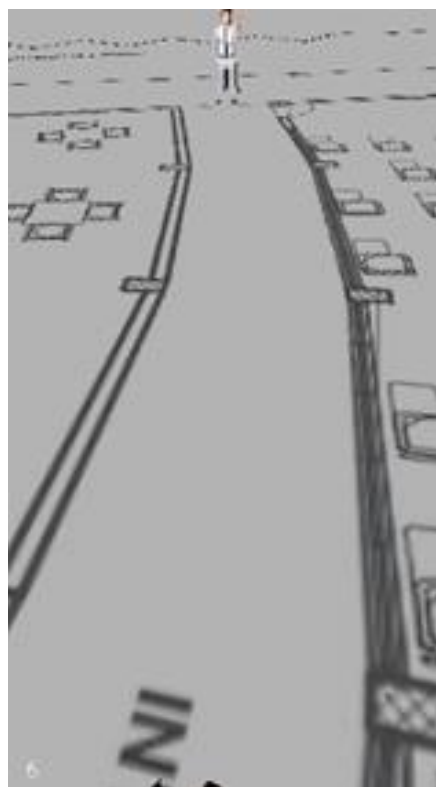


Figura 35. Resultado testeo 1 cámara interior tipo 1

Este nos muestra las características de nuestra cámara, así como también sus parámetros y la simulación de la vista del objetivo a distancia real y como se vería su rostro acercando la grabación.

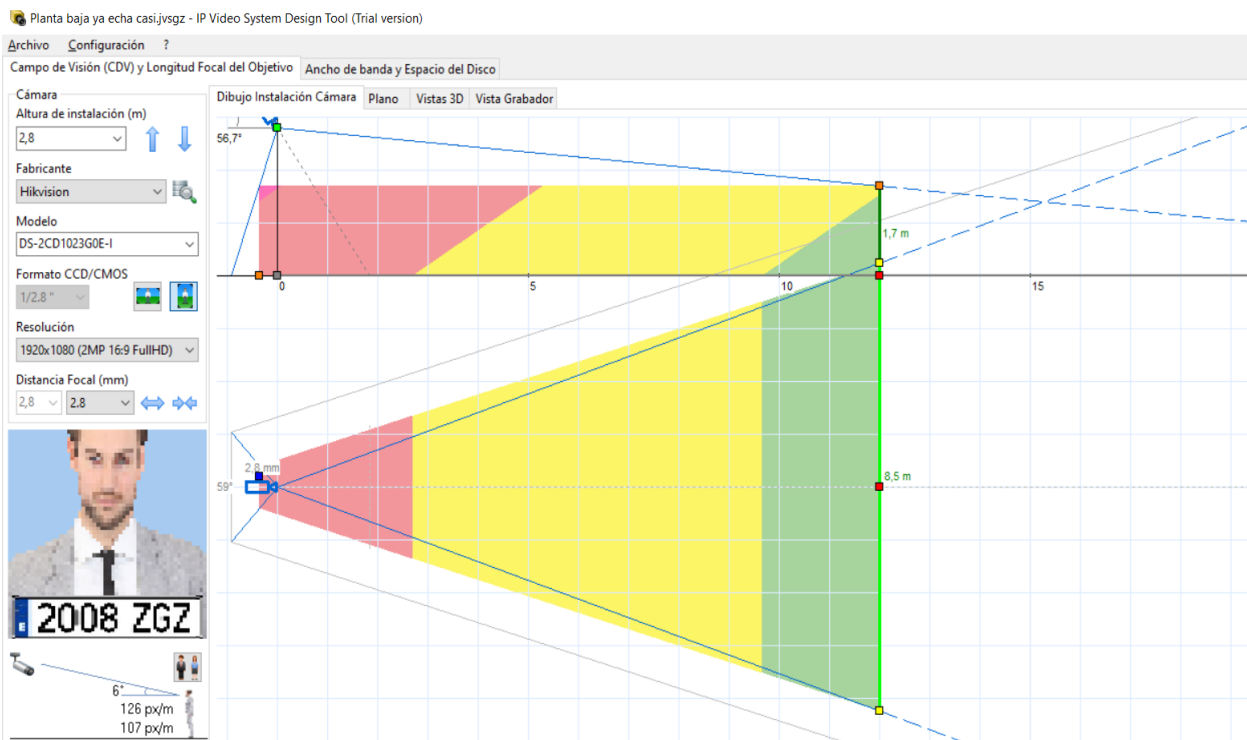


Figura 36. Resultado testeo 2 cámara interior tipo 1

En este segundo testeo es una gráfica que indica el ángulo de inclinación de la cámara como así también la distancia focal y el ángulo de visión horizontal que se obtendría.

II.1.2.4.2.2 Testeo cámara interior tipo 2

Se identifico nuestra cámara en la base de datos del software, esto según el fabricante y modelo.

FABRICANTE	MODELO
Hikvision	DS-2CD1043G2-LIU

Tabla 21. Fabricante y modelo cámara interior tipo 2

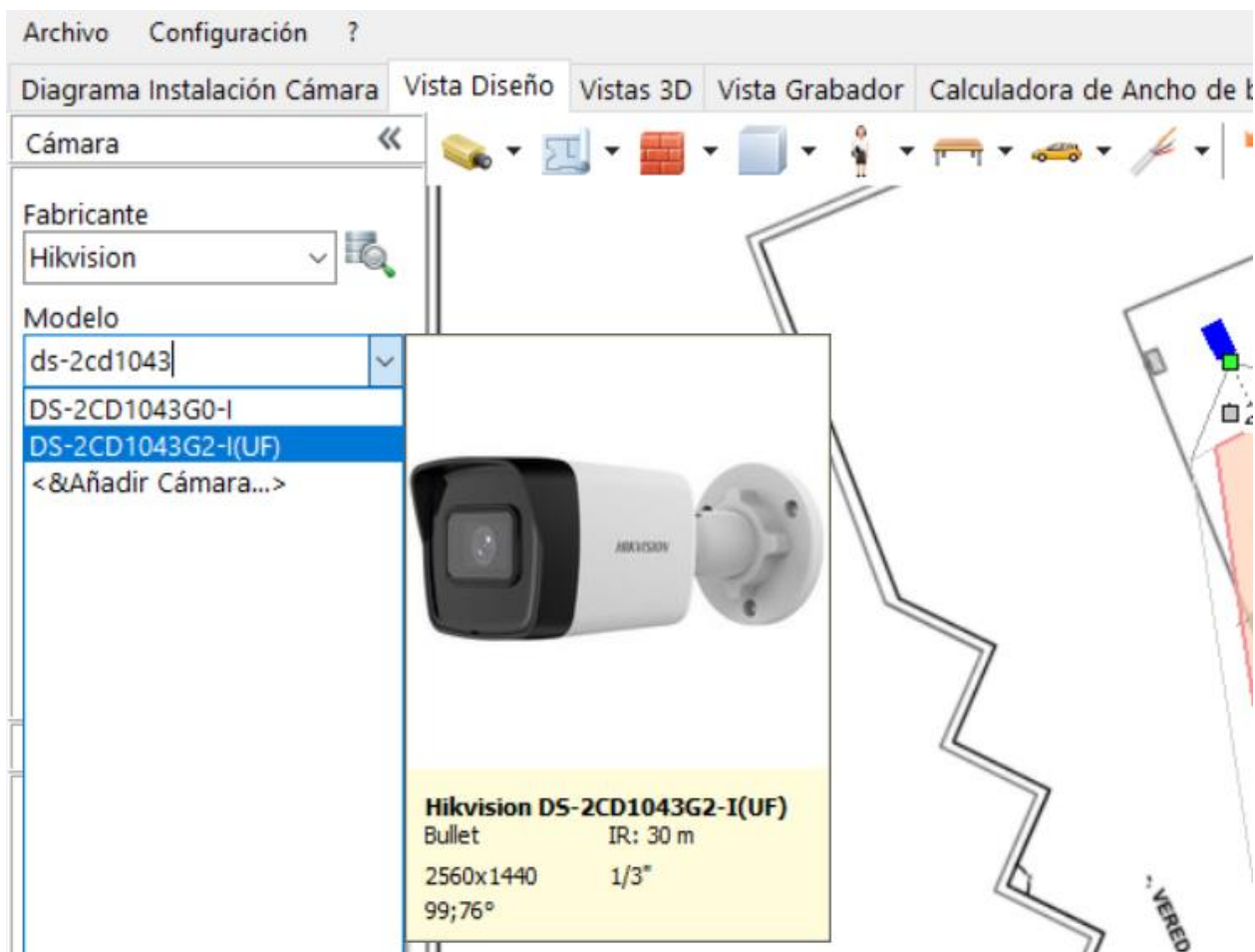


Figura 37. Identificación de cámara interior tipo 2

Para realizar el testeo de la cámara de seguridad se tomaron en cuenta los siguientes parámetros.

PARAMETROS	VALORES
Altura de instalación	2,8 (m) (recomendada)
Formato CC/CMOS	1/3 (optima)
Resolución	2560x1440
Distancia focal	4 (mm)
Distancia hasta el objeto (máxima)	31 (m)
Altura del objeto	1,7 (m)
Ancho CDV	18,3 (m)

Tabla 22. Parámetros cámara interior tipo 2

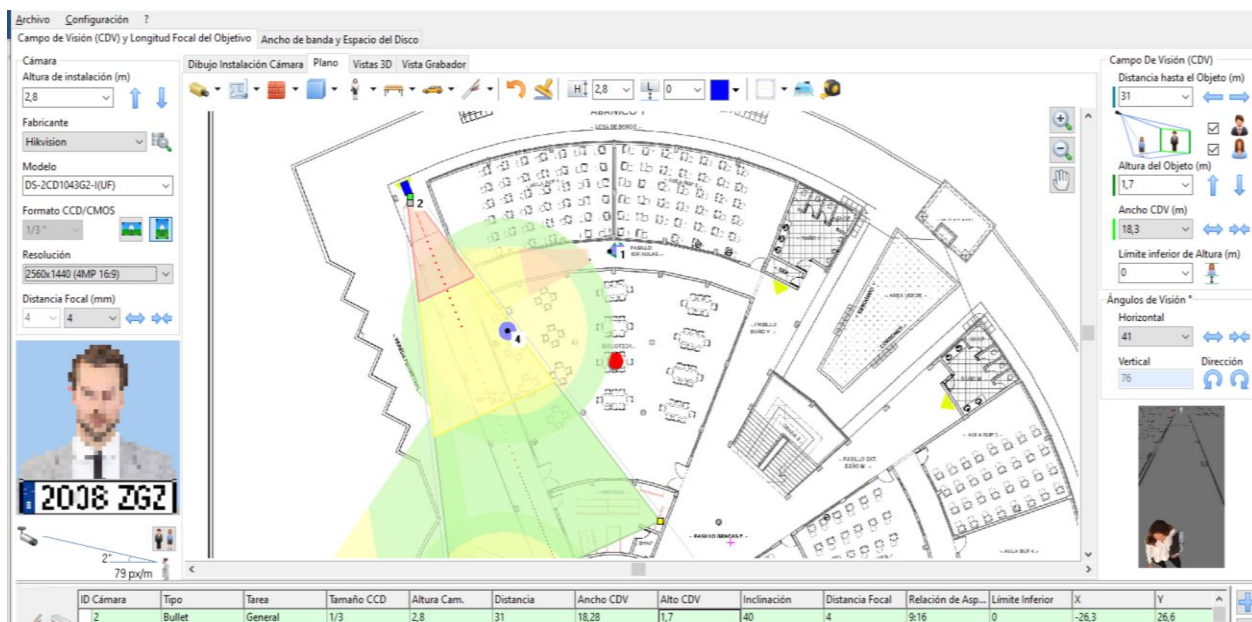
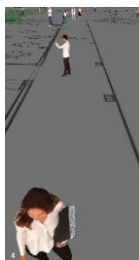


Figura 38. Parámetros cámara interior tipo 2

Una vez añadidos los parámetros el software nos soltara los siguientes resultados.

Cámara 4

4MP Fixed Bullet Network Camera



www.jvsg.com

Resolución: 1440x2560
 Tamaño CCD: 1/3 ; 9:16
 Distancia Focal: 4
 Altura Cam.: 2,8 m
 Inclinación: 40,1°
 Ángulos de Visión °: 41°; 76°
 Distancia: 31 m Ancho CDV: 18,3 m
 Píxeles en el Objeto: 75 px/m
 Zona muerta: 0,59 m (Ancho: 0,89 m)





Figura 39. Resultado testeo 1 cámara interior tipo 2

Este nos muestra las características de nuestra cámara, así como también sus parámetros y la simulación de la vista del objetivo a distancia real y como se vería su rostro acercando la grabación.



Figura 40. Resultado testeo 2 cámara interior tipo 2

En este segundo testeo es una gráfica que indica el ángulo de inclinación de la cámara como así también la distancia focal y el ángulo de visión horizontal que se obtendría.

II.1.2.4.2.3 Testeo cámara exterior

Se identifico nuestra cámara en la base de datos del software, esto según el fabricante y modelo.

FABRICANTE	MODELO
Hikvision	DS-2CD1123G0E-I

Tabla 23. Fabricante y modelo cámara exterior

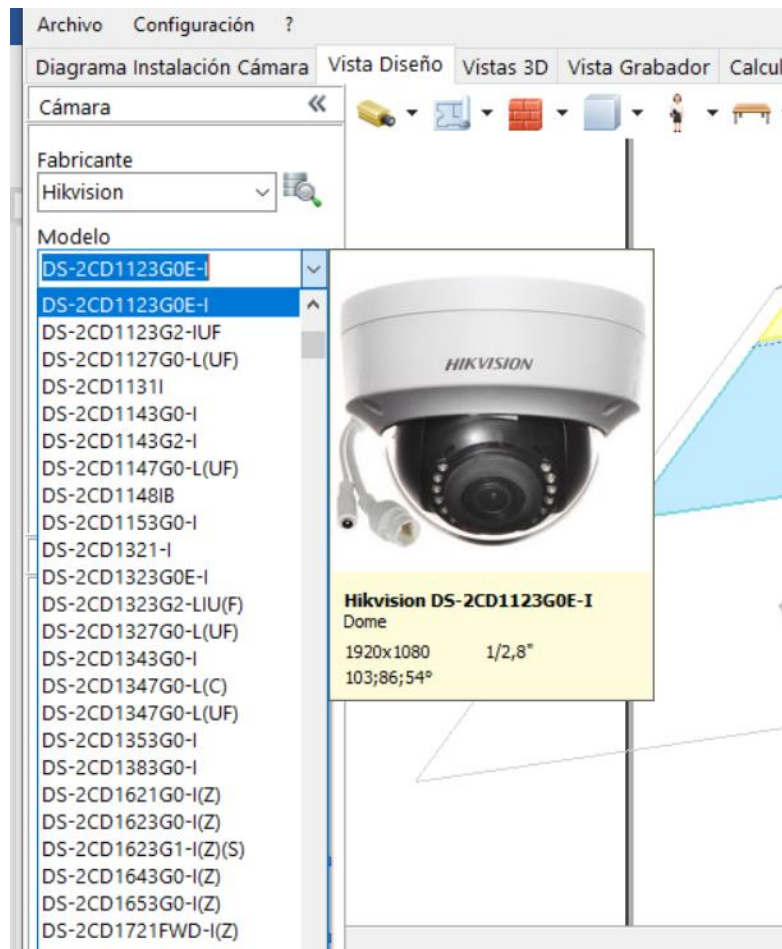


Figura 41. Identificación de cámara exterior

Para realizar el testeo de la cámara de seguridad se tomaron en cuenta los siguientes parámetros.

PARAMETROS	VALORES
Altura de instalación	4 (m) (recomendada)
Formato CC/CMOS	1/2,8 (optima)
Resolución	1920x1080
Distancia focal	2,8 (mm)
Distancia hasta el objeto (máxima)	14 (m)
Altura del objeto	1,7 (m)
Ancho CDV	30,6 (m)

Tabla 24. Parámetros cámara exterior

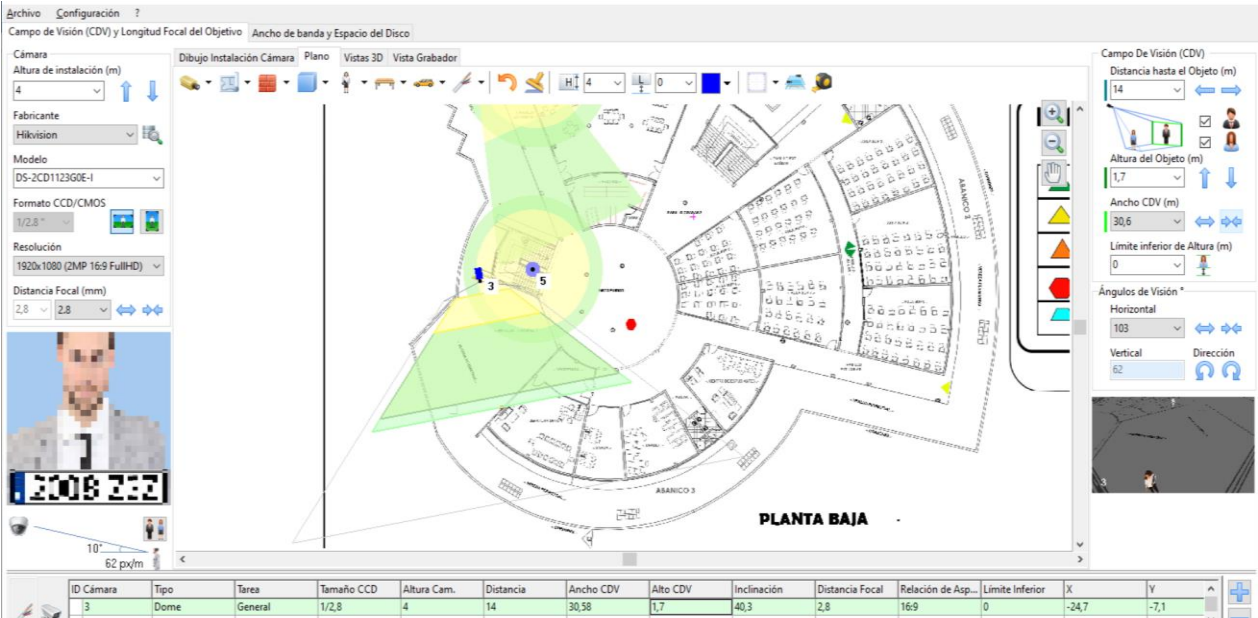


Figura 42. Parámetros cámara exterior

Una vez añadidos los parámetros el software nos soltara los siguientes resultados.

Cámara 3

Hikvision: DS-2CD1123G0E-I



Resolución: 1920x1080
Tamaño CCD: 1/2,8 ; 16:9
Distancia Focal: 2,8
Altura Cam.: 4 m
Inclinación: 40,3°
Ángulos de Visión °: 103°; 62°
Distancia: 14 m
Ancho CDV: 30,6 m
Píxeles en el Objeto: 58 px/m
Zona muerta: 1,35 m (Ancho: 6,33 m)

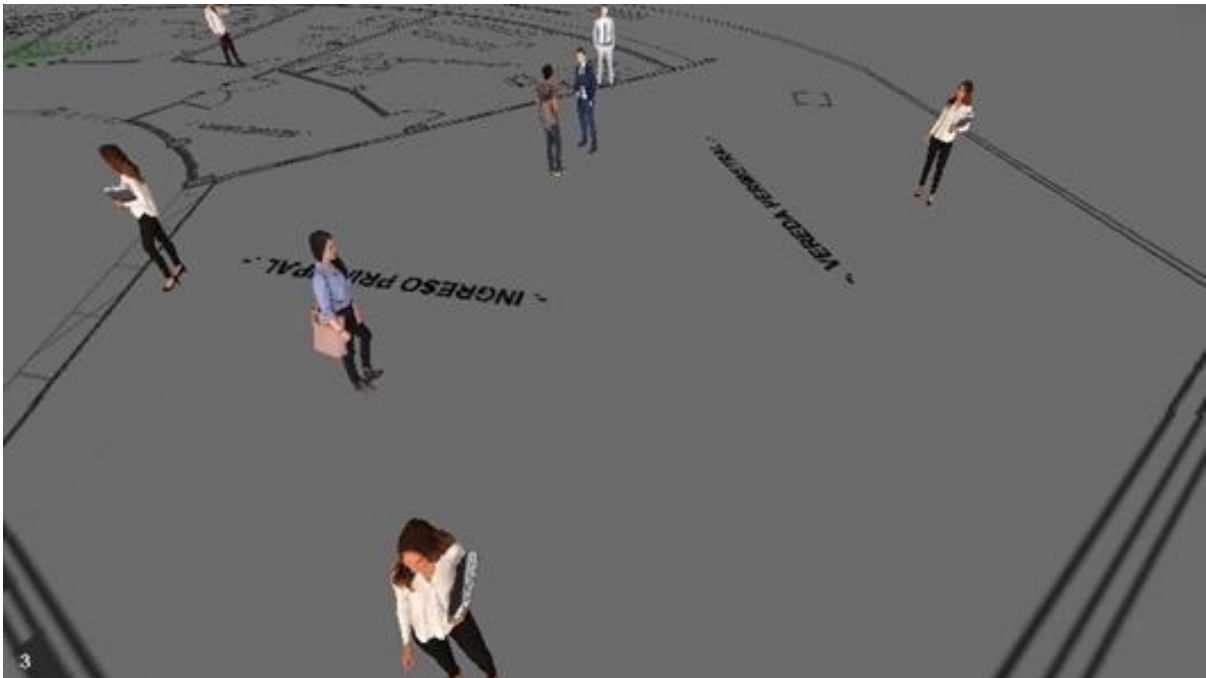


Figura 43. Resultado testeo 1 cámara exterior

Este nos muestra las características de nuestra cámara, así como también sus parámetros y la simulación de la vista del objetivo a distancia real y como se vería su rostro acercando la grabación.

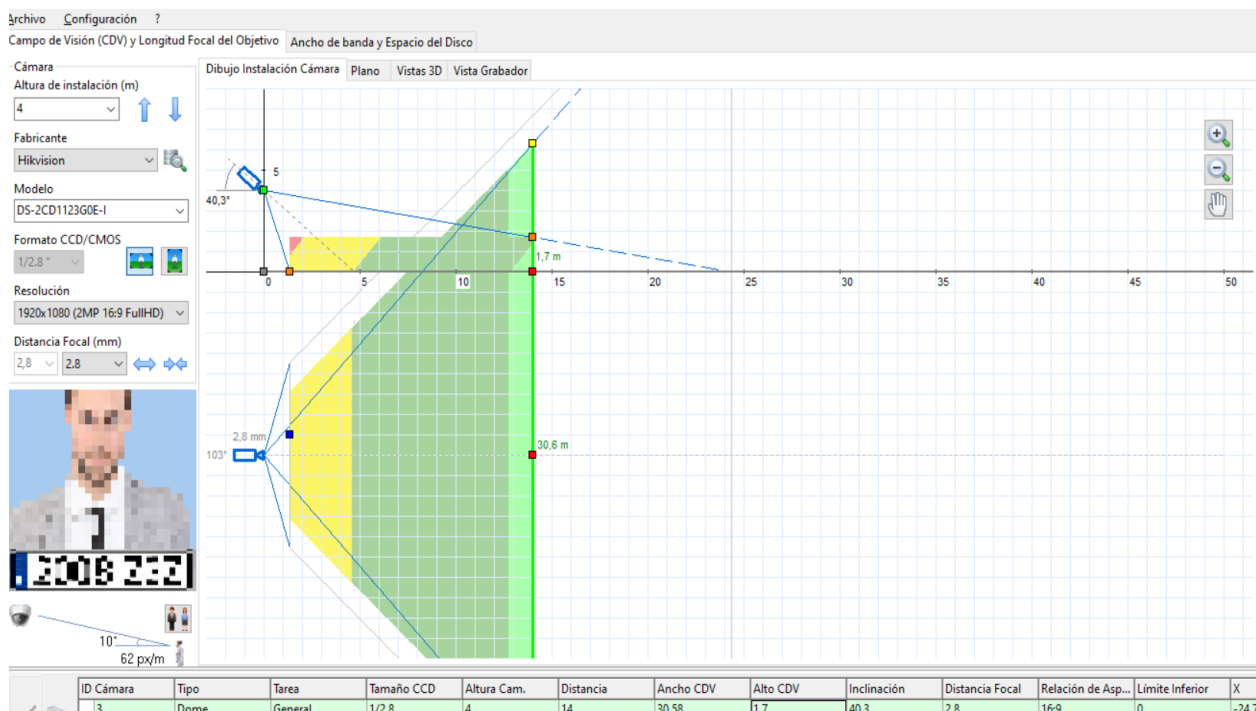


Figura 44. Resultado testeo 2 cámara exterior

En este segundo testeo es una gráfica que indica el ángulo de inclinación de la cámara como así también la distancia focal y el ángulo de visión horizontal que se obtendría.

II.1.2.4.2.4 Testeo cámara ojo de pez

Se identifico nuestra cámara en la base de datos del software, esto según el fabricante y modelo.

FABRICANTE	MODELO
Hikvision	DS-2CD2955FWD-IS

Tabla 25. Fabricante y modelo cámara ojo de pez

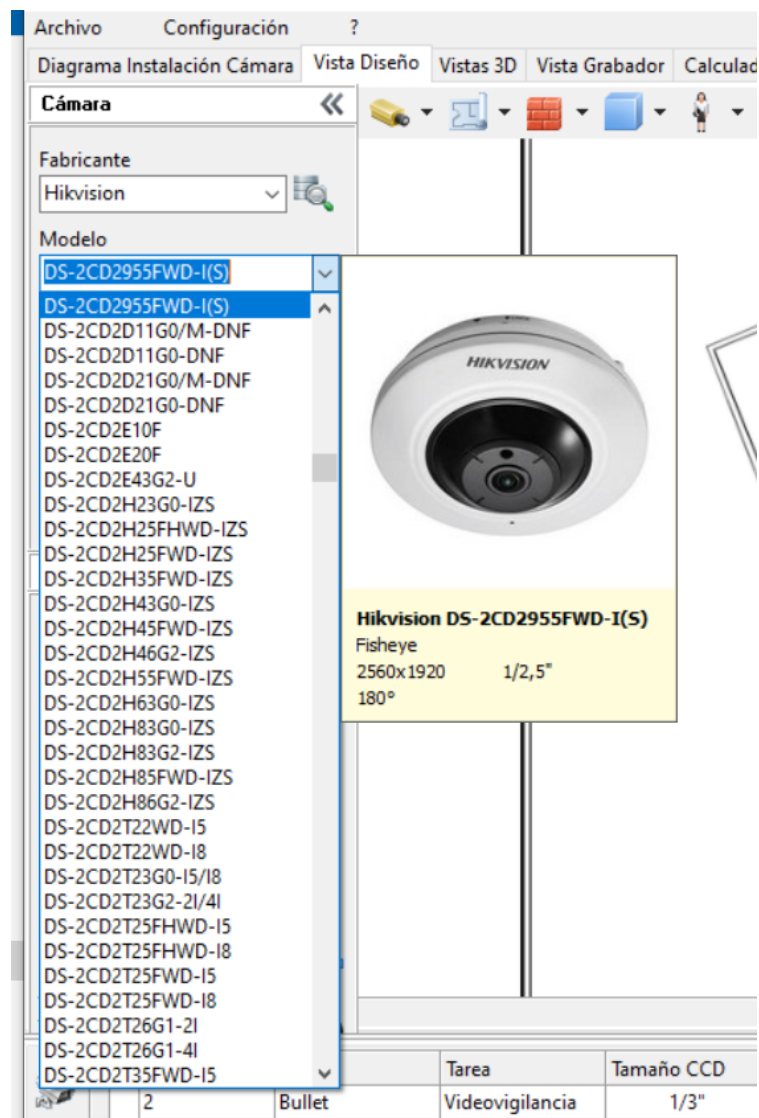


Figura 45. Identificación de cámara ojo de pez

Para realizar el testeo de la cámara de seguridad se tomaron en cuenta los siguientes parámetros.

PARAMETROS	VALORES
Altura de instalación	3 (m) (recomendada)
Formato CC/CMOS	1/2,5 (optima)
Resolución	2560x1920
Distancia focal	1,05 (mm)

Distancia hasta el objeto (máxima)	10 (m)
Altura del objeto	1,7 (m)

Tabla 26. Parámetros cámara ojo de pez

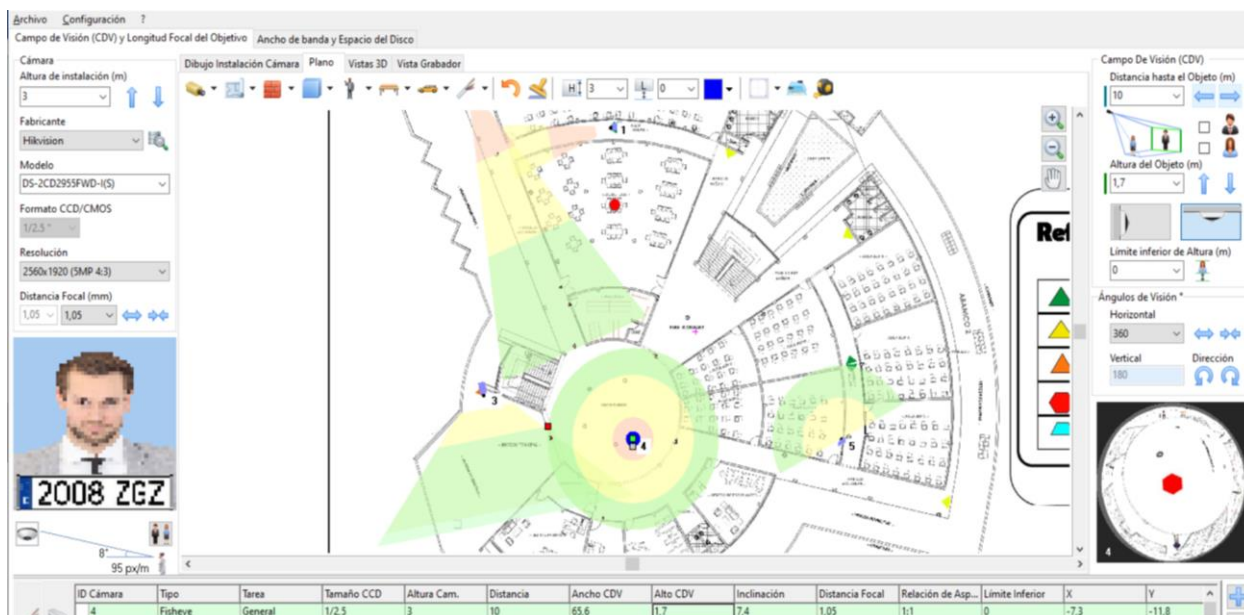
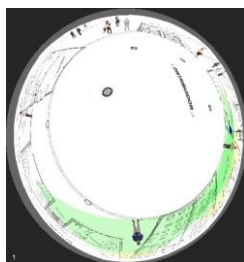


Figura 46. Parámetros cámara ojo de pez

Una vez añadidos los parámetros el software nos soltara los siguientes resultados.

Cámara 1

Hikvision: DS-2CD2955FWD-I(S)



Resolución: 2560x1920
 Tamaño CCD: 1/2,5 ; 1:1
 Distancia Focal: 1,05
 Altura Cam.: 3 m
 Inclinación: 4,8°
 Ángulos de Visión °: 360°; 180°
 Distancia: 11 m
 Ancho CDV: 17,9 m
 Píxeles en el Objeto: 84 px/m
 Zona muerta: 0 m (Ancho: 0 m)



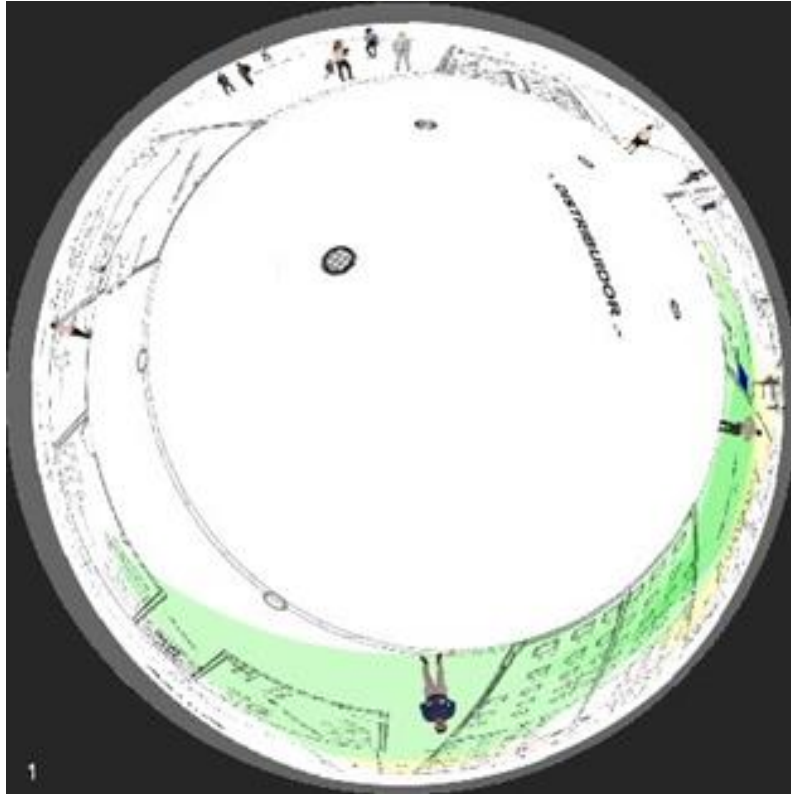


Figura 47. Resultado testeo 1 cámara ojo de pez

Este nos muestra las características de nuestra cámara, así como también sus parámetros y la simulación de la vista del objetivo a distancia real y como se vería su rostro acercando la grabación.

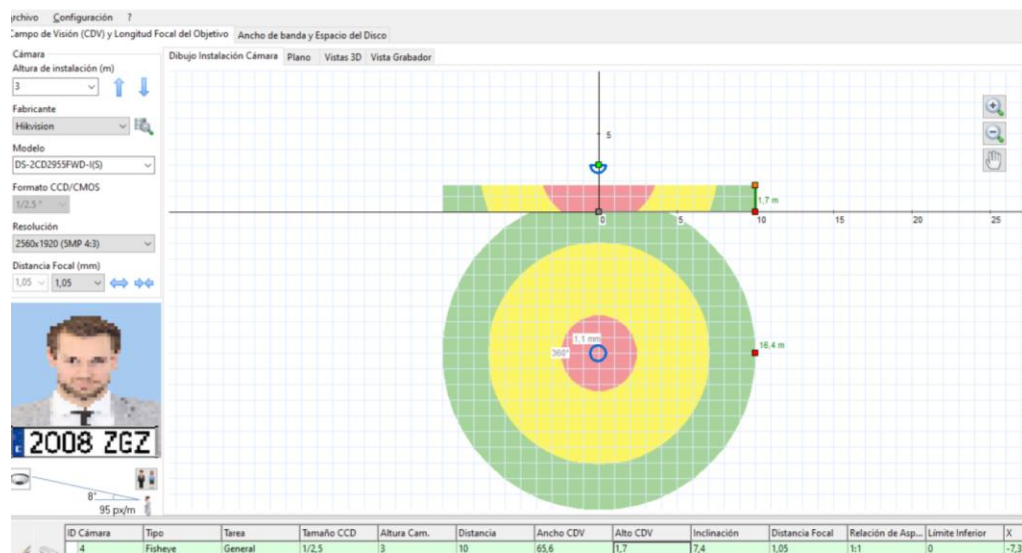


Figura 48. Resultado testeo 2 cámara ojo de pez

En este segundo testeo es una gráfica que indica el ángulo de inclinación de la cámara como así también la distancia focal y el ángulo de visión horizontal que se obtendría.

A continuación, se observa la vista general simulada del grabador nvr.

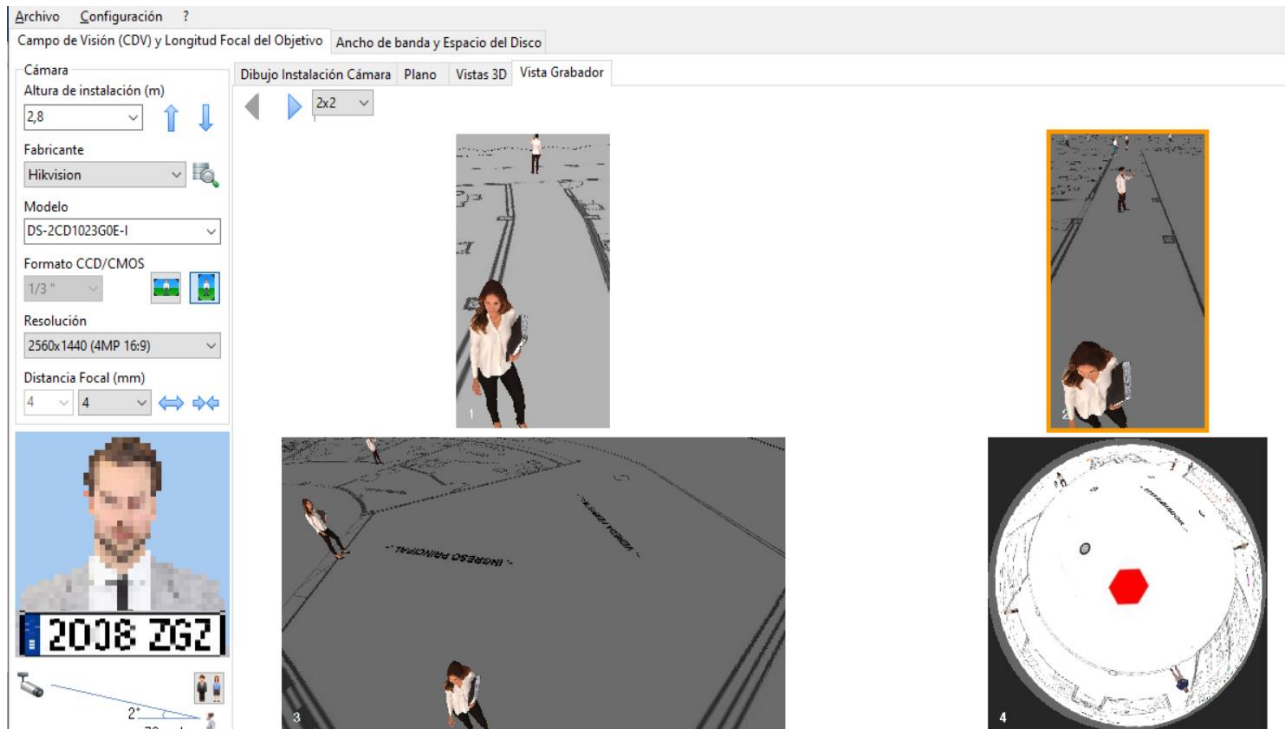


Figura 49. Vista del grabador

I.6.3.4.3 Diseño final y cableado

Se usó el software Ip Video System Design Tool, simulando el sistema de videovigilancia con sus equipos, así como también el cableado a usar.

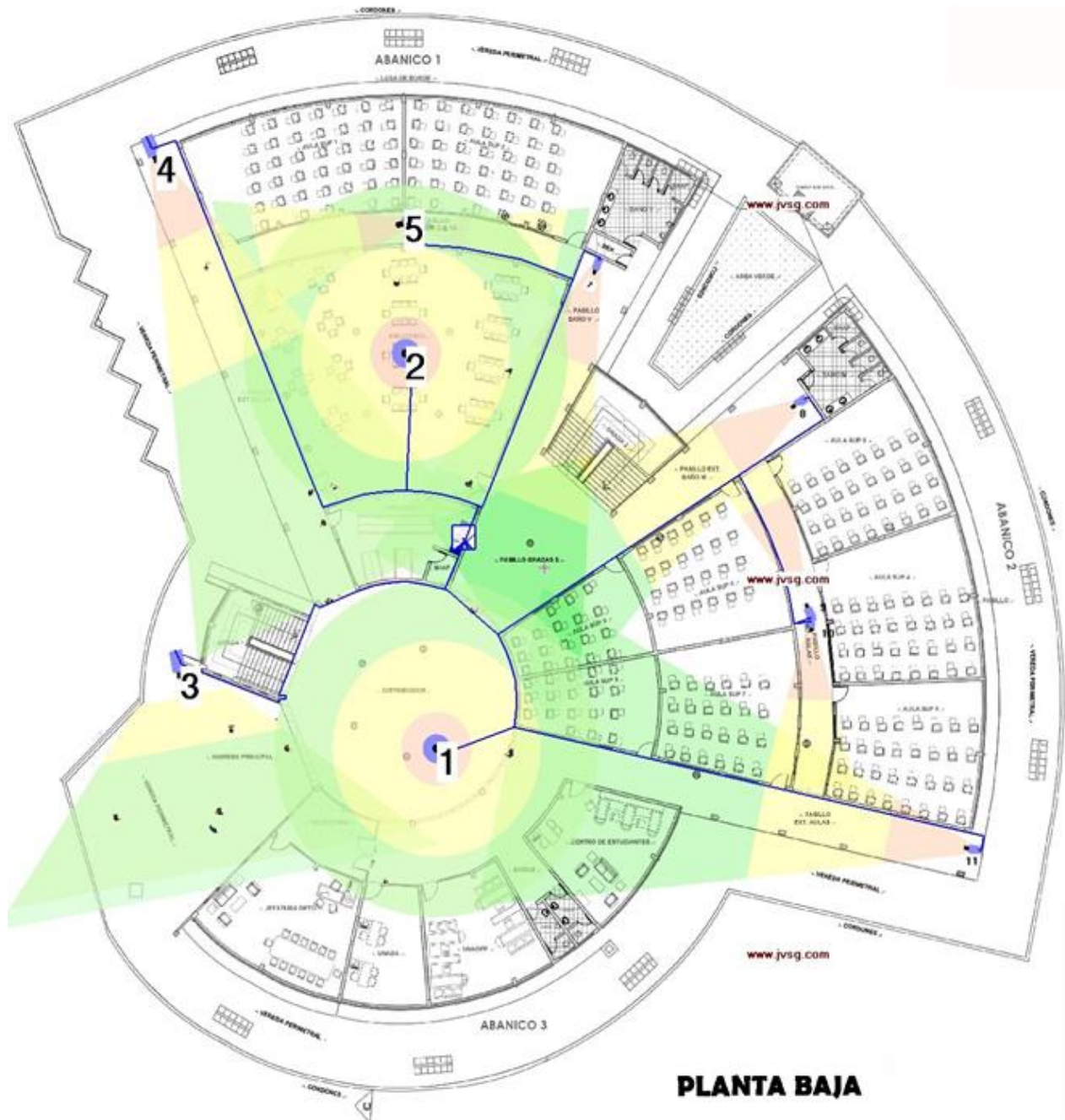


Figura 50. Diseño final de cableado y cámaras planta baja

Este software también tiene una herramienta que permite diagramar el cableado además de realizar sus conexiones y nos brinda la distancia recorrida de cada uno en horizontal.

Lista de cables

ID Cable	Tipo	Desde	Hasta	Longitud, m
1	Par trenzado	1	Switch de red 1	20,12
2	Par trenzado	2	Switch de red 1	16,63
3	Par trenzado	3	Switch de red 1	28,7
4	Par trenzado	4	Switch de red 1	41,92
5	Par trenzado	5	Switch de red 1	31,88
6	Par trenzado	6	Switch de red 1	31,78
7	Par trenzado	7	Switch de red 1	22,44
8	Par trenzado	8	Switch de red 1	36,65
9	Par trenzado	9	Switch de red 1	39,45
10	Par trenzado	10	Switch de red 1	39,39
11	Par trenzado	11	Switch de red 1	48,48

TOTAL:

Tipo de cable	Longitud, m
Par trenzado	357,44

Figura 51. Listado de cableado planta baja

El total de cableado horizontal usado para la planta baja es de 357,44 m

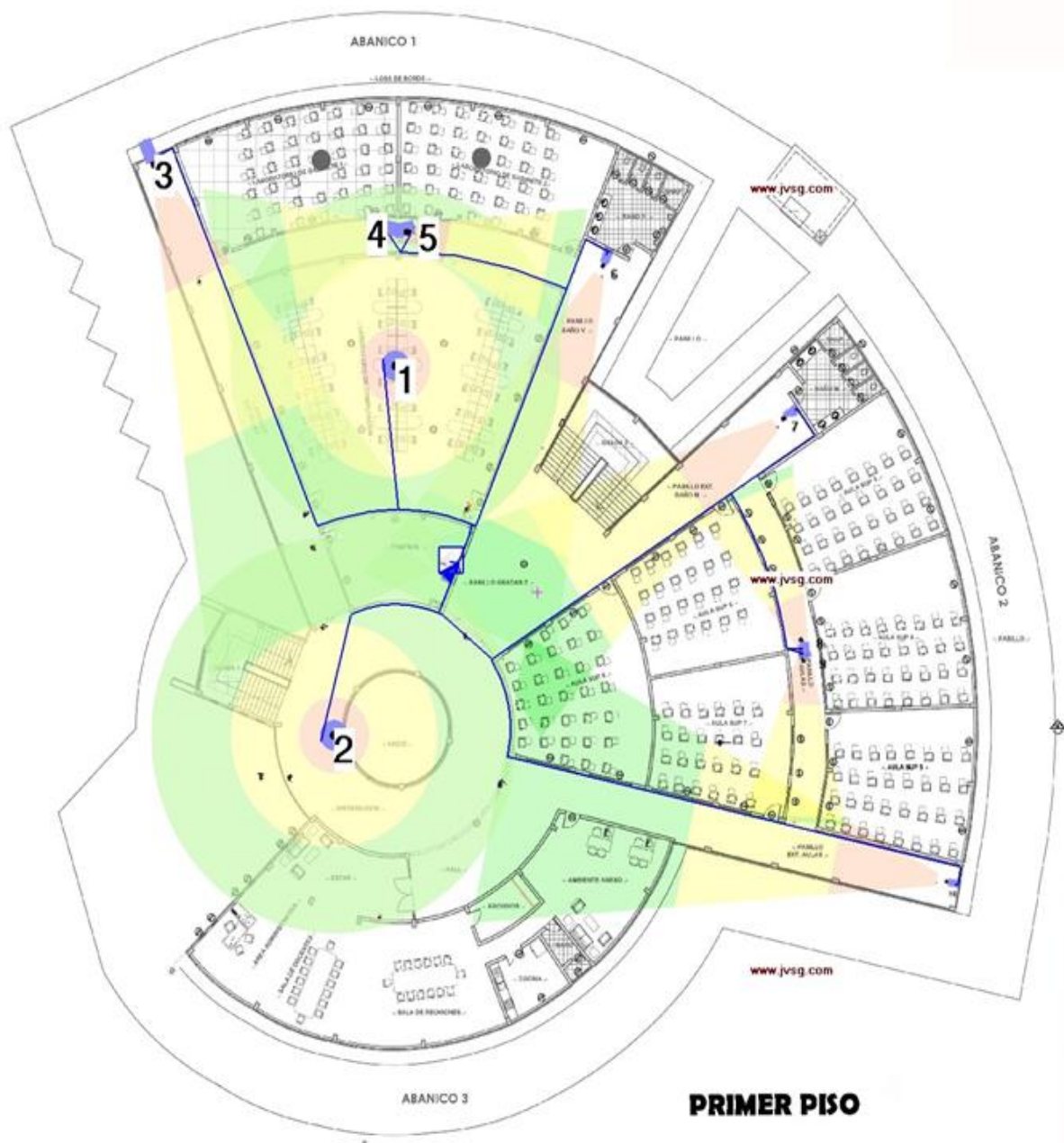


Figura 52. Diseño final de cableado y cámaras primera planta

Lista de cables

ID Cable	Tipo	Desde	Hasta	Longitud, m
1	Par trenzado	1	Switch de red 2	17,45
2	Par trenzado	2	Switch de red 2	17,82
3	Par trenzado	3	Switch de red 2	41,93
4	Par trenzado	4	Switch de red 2	32,8
5	Par trenzado	5	Switch de red 2	32,71
6	Par trenzado	6	Switch de red 2	25,06
7	Par trenzado	7	Switch de red 2	37,07
8	Par trenzado	8	Switch de red 2	39,74
9	Par trenzado	9	Switch de red 2	39,83
10	Par trenzado	10	Switch de red 2	48,22

TOTAL:

Tipo de cable	Longitud, m
Par trenzado	332,63

Figura 53. Listado de cableado primera planta

El total de cableado horizontal usado para la primera planta es de 332,63 m.

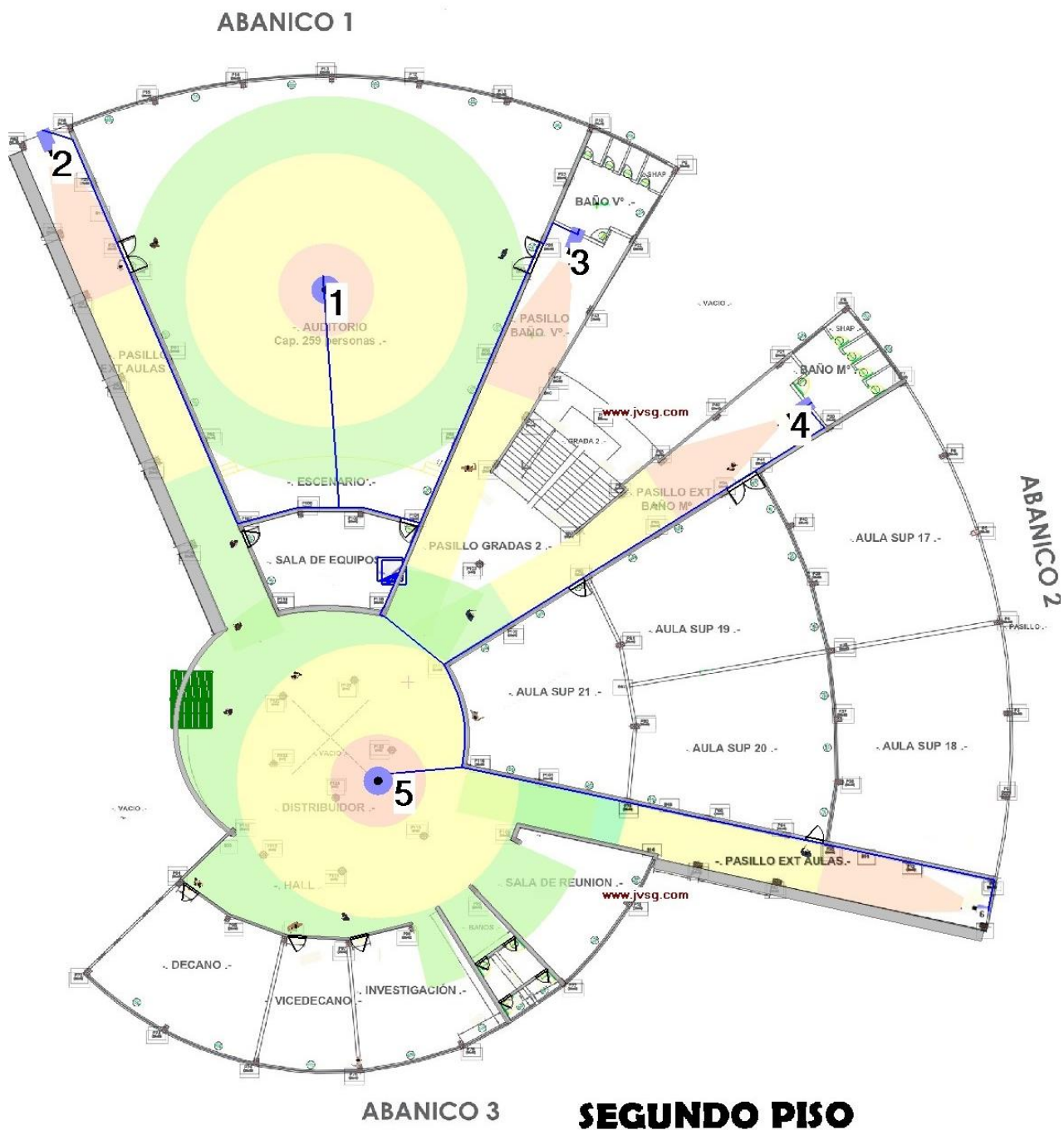


Figura 54. Diseño final de cableado y cámaras segunda planta

Lista de cables

ID Cable	Tipo	Desde	Hasta	Longitud, m
1	Par trenzado	1	Switch de red 3	18,61
2	Par trenzado	2	Switch de red 3	35,3
3	Par trenzado	3	Switch de red 3	22,71
4	Par trenzado	4	Switch de red 3	32,04
5	Par trenzado	5	Switch de red 3	16,77
6	Par trenzado	6	Switch de red 3	41,42
7	Par trenzado	Switch de red 3	Grabador de Video 1	0,25

TOTAL:

Tipo de cable	Longitud, m
Par trenzado	167,1

Figura 55. Listado de cableado segunda planta

El total de cableado horizontal usado para la segunda planta es de 167,1 m.

Por lo tanto, el cableado total sería:

Plantas	Cableado a usar
Planta baja	357,44 m
Primera planta	332,63 m.
Segunda planta	167,1 m.
Total	857,17 m.

Tabla 27. Cableado horizontal total

En cuanto al cableado vertical la altura de cada planta es de 4 m y de cada entrepiso es de 0,5 m, de este modo:

Plantas	Altura	Cableado a usar
3	4	12 m
Entrepiso		
2	0,2	0,4 m
Total		12,4 m

Tabla 28. Cableado vertical total

El cableado en vertical sería de 12,4 m, eso nos daría un total de 869,57 m.

I.6.3.4.4 Diagrama de despliegue y componentes

El sistema se despliega de la siguiente manera.

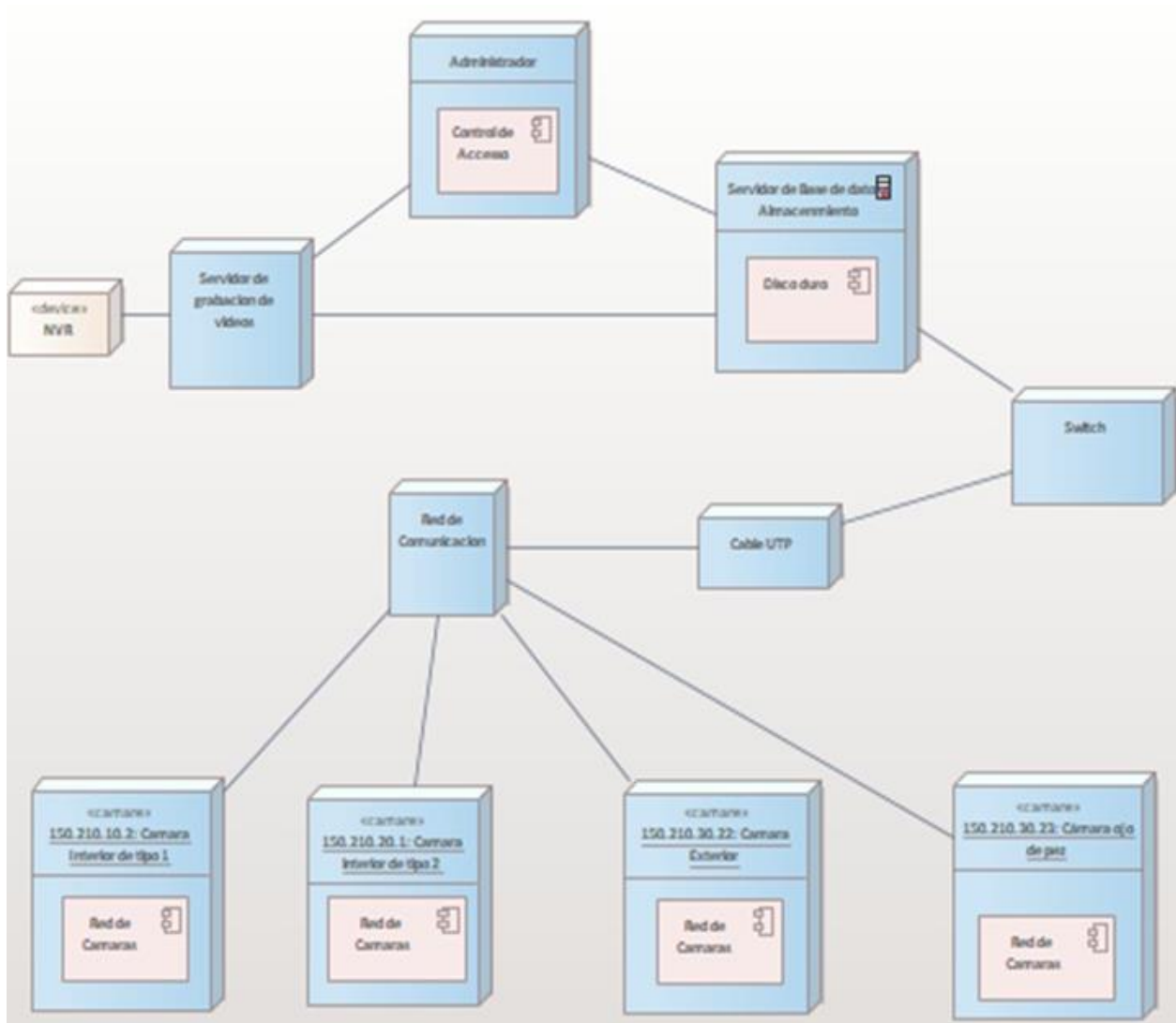


Figura 56. Diagrama de despliegue

El "Administrador" tiene acceso al sistema de cámaras de seguridad para supervisar y controlar las operaciones.

El "Servidor de Grabación de Video" gestiona la grabación y almacenamiento de video.

El "NVR (Network Video Recorder)" es un dispositivo dedicado para grabar y almacenar video de las cámaras.

El "Switch" facilita la conexión y comunicación entre todos los dispositivos de la red, incluyendo las cámaras, el servidor de grabación de video y el servidor de base de datos y almacenamiento.

El "Cable UTP Cat6" se utiliza para conectar los diferentes dispositivos de la red.

El "Seagate Exos 7E8 6TB" es el disco duro empresarial utilizado para almacenar los datos grabados por las cámaras.

En base al proyecto y los equipos optados se concluye el siguiente diagrama de componentes.

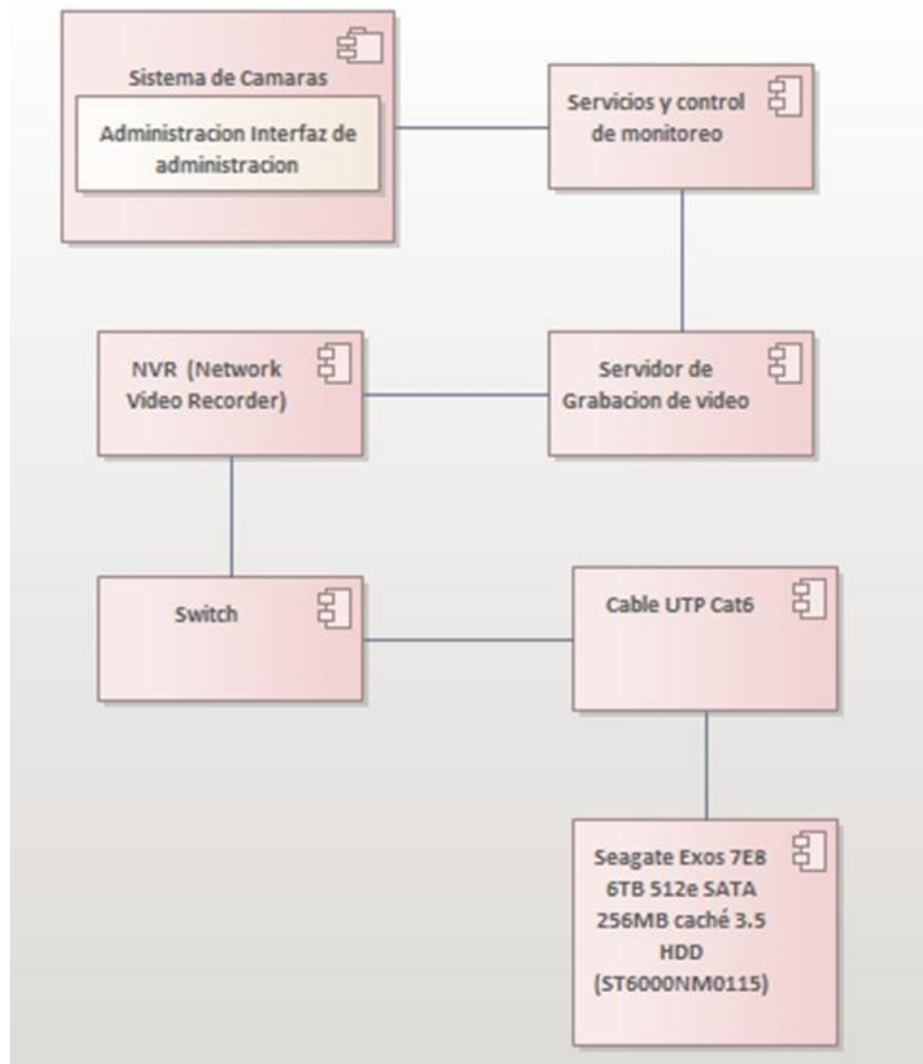


Figura 57. Diagrama de componentes

El "Sistema de Cámaras" es el componente principal que engloba todos los elementos del sistema de seguridad.

El "Administrador" interactúa con el sistema a través de la "Interfaz de Administración".

Los "Servicios de Control y Monitoreo" gestionan el funcionamiento y la supervisión de las cámaras.

El "Servidor de Grabación de Video" almacena las grabaciones de las cámaras.

El "NVR (Network Video Recorder)" es el dispositivo encargado de grabar y almacenar el video de las cámaras de red.

El "Switch" facilita la conexión de todos los dispositivos de red.

El "Cable UTP Cat6" se utiliza para la conexión de red entre los diferentes componentes.

El "Seagate Exos 7E8 6TB" es el disco duro empresarial utilizado para almacenar los datos grabados por las cámaras.

I.6.3.4.5 Cálculo de almacenamiento y ancho de banda

Para realizar el cálculo de almacenamiento y ancho de banda en total que ocuparan de las cámaras se usara la herramienta **Storage and Network Calculator**, el cual es un software propio de hikvision. Este mismo nos permite calcular en días, semanas o meses cuanto podrá grabar el nvr según la cantidad de cámaras, resolución o calidad de las cámaras y disco duro determinado.

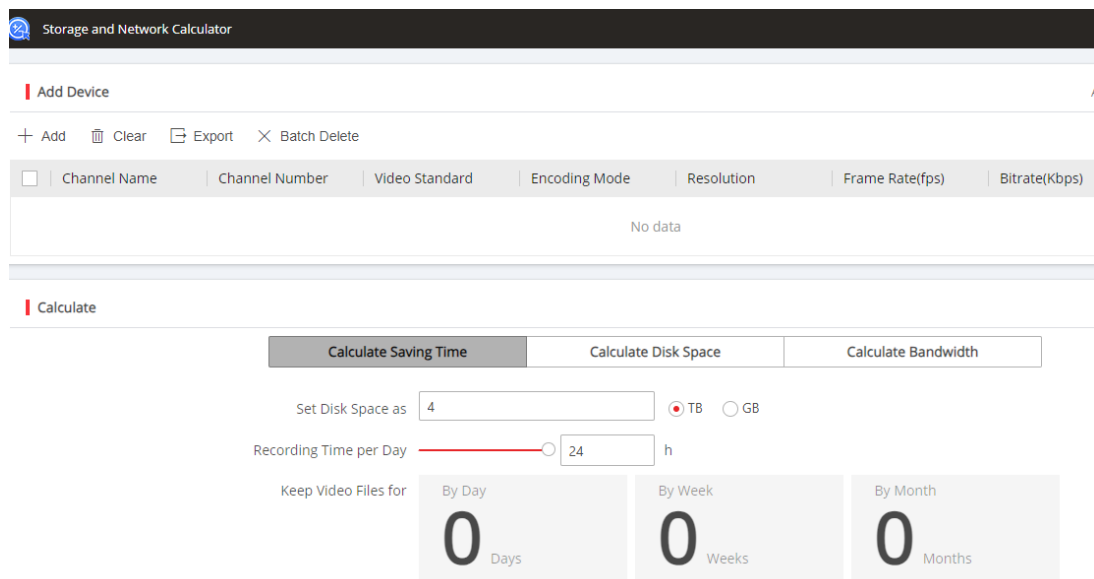


Figura 58. Storage and network calculator

 Add
  Clear
  Export
  Batch Delete

☒	Channel Name	Channel Number	Video Standard	Encoding Mode	Resolution	Frame Rate(fps)	Bitrate(Kbps)
☒	1 Camaras 5mp	6	NTSC	H.265+	5MP(2560×1920)	15	1544
☒	2 Camaras 4mp	12	NTSC	H.265+	4MP(2688×1520)	15	1440
☒	3 Camaras 2mp	9	NTSC	H.265+	1080P(1920×1080)	15	832

Figura 59. Canales de calculadora

Se dividieron los canales en base a los megapíxeles de las cámaras, en total tenemos 6 cámaras de 5 mp, 12 cámaras de 4 mp y 9 cámaras de 2 mp (megapíxeles).

Los calculos se reliazaron según los siguientes parametros:

- El estandar de video.
- La compresion de H.265+.
- Resolucion de cada camara.
- La calidad de fps (delante de 12 es de movimiento continuo y apartir de 30 movimiento natural).
- El bitrate o tasa de datos recomendada.

<

Figura 60. Cálculo de tiempo de guardado

Se determino que mediante dos discos duros de 6 tb, tendríamos un almacenamiento de 12 tb los suficientes como para almacenar 32 dias o 4 semanas o bien 1 mes. Mediante grabacion continua.

The screenshot shows a table with three channels and a calculation section below it.

Channel Name	Channel Number	Video Standard	Encoding Mode	Resolution	Frame Rate(fps)	Bitrate(Kbps)
1 Camaras 5mp	6	NTSC	H.265+	5MP(2560×1920)	15	1544
2 Camaras 4mp	12	NTSC	H.265+	4MP(2688×1520)	15	1440
3 Camaras 2mp	9	NTSC	H.265+	1080P(1920×1080)	15	832

Below the table, there is a 'Calculate' section with three tabs: 'Calculate Saving Time', 'Calculate Disk Space' (selected), and 'Calculate Bandwidth'.

Set Saving Time as: 1 (input field) ☐ Day ☐ Week ☒ Month

Recording Time per Day: 24 (input field) h

Required Disk Space: **11.1** TB

Figura 61. Cálculo de espacio de disco

El calculo para 1 mes de grabacion con los parametros ya mencionados y con grabacion continua (24 horas), nos da un espacio utilizado de 11,1 TB.

The screenshot shows a table with three channels and a calculation section below it.

Channel Name	Channel Number	Video Standard	Encoding Mode	Resolution	Frame Rate(fps)	Bitrate(Kbps)	Operation
1 Camaras 5mp	6	NTSC	H.265+	5MP(2560×1920)	15	1544	
2 Camaras 4mp	12	NTSC	H.265+	4MP(2688×1520)	15	1440	
3 Camaras 2mp	9	NTSC	H.265+	1080P(1920×1080)	15	832	

Below the table, there is a 'Calculate' section with three tabs: 'Calculate Saving Time', 'Calculate Disk Space', and 'Calculate Bandwidth' (selected).

Required Bandwidth: **33.30** Mbps

Figura 62. Cálculo de ancho de banda

El ancho de banda necesarios que se requiere para la calidad y compresion señalados anteriormente es de 33,30 Mbps.

CANALES	NUMERO DE CANALES	ESTANDAR DE VIDEO	CODIFICACION DE VIDEO	RESOLUCION	CUADROS POR SEGUNDO(fps)	TASA DE BITS(Kbps)
1 Camaras de 5 mp	6	NTSC	H.265+	5MP(2560x1920)	15	1544
2 Camaras de 4 mp	12	NTSC	H.265+	4MP(2688x1520)	15	1440
3 Camaras de 2 mp	9	NTSC	H.265+	1080P(1920x1080)	15	832

Tabla 29. Canales de calculo

ESPACIO DEL DISCO	TIEMPO DE GRABACION POR DIA	GUARDADO DE ARCHIVOS DE VIDEO (DIA)	GUARDADO DE ARCHIVOS DE VIDEO (SEMANA)	GUARDADO DE ARCHIVOS DE VIDEO (MES)
12 Tb	24 Horas	32 Dias	4 Semanas	1 Mes

Tabla 30. Tiempo de guardado

TIEMPO DE GRABACION	TIEMPO DE GRABACION POR DIA	ESPACIO DE DISCO REQUERIDO
1 Mes	24 Horas	11.1 Tb

Tabla 31. Espacio de disco requerido

TOTAL DE CANALES	TOTAL DE ANCHO DE BANDA
27	33.30 Mbps

Tabla 32. Ancho de banda

I.6.3.4.6 Presupuestos

II.1.3.4.4.1 Presupuesto de equipos

A continuacion se detallaran los costos referenciales de los equipos a implementar en el sistema de vigilancia, se cotizara cada uno de ellos individualmente como tambien el total, todo esto a base de los equipos referenciado en la tabla de equipos a utilizar.

El precio de los equipos se hallan en dolares, por lo cual se usa una conversion para pasar el valor a bolivianos y asi tener los precios unitarios y el total en moneda local.

Todos estos equipos cumplen con los requisitos tecnicos del proyecto y fueron seleccionados por la busqueda entre mejor relacion de calidad/precio.

EQUIPO	CANTIDAD	PRECIO UNITARIO Bs	PRECIO TOTAL Bs
Switch	3	2717,34	8152,02
NVR	1	4341,41	4341,41
Camara interior tipo 1	8	311,02	2488,16
Camara interior tipo 2	12	414,02	4968,24
Camara exterior	1	345,66	345,66
Camara ojo de pez	6	1382,55	8295,30
Disco duro	2	611,96	1264,78
Cableado Cat6	869,57 (m)	3	2608,71
TOTAL			32323,4 Bs

Tabla 33. Presupuesto de equipamiento

II.1.3.4.4.2 Presupuesto de mano de obra

En cuanto al costo de mano de obra se estimo un total de 9.600 bolivianos.

ACTIVIDAD	INSTALACION	PRECIO UNITARIO	CANTIDAD	PRECIO TOTAL
Mano de obra	Por camara	300	27	8,100
	Por nvr y switch	380	3	1,200
TOTAL				9,300

Tabla 34. Presupuesto de mano de obra

I.7 Componente II: Manual de procedimientos para el uso de cámaras de seguridad y vigilancia.

MANUAL DE PROCEDIMIENTOS PARA EL USO DE CAMARAS DE SEGURIDAD Y VIGILANCIA.

CAPÍTULO I ASPECTOS GENERALES

Artículo 1°	Objetivo del procedimiento	124
Artículo 2°	Ámbito de Aplicación	124
Artículo 3°	Responsables de su aplicación	124
Artículo 4°	Base Legal	124
Artículo 5°	Definiciones	124
Artículo 6°	Difusión	125
Artículo 7°	De su modificación	125
Artículo 8°	Responsabilidades	125

CAPÍTULO II SISTEMA DE SEGURIDAD Y VIGILANCIA

Artículo 9°	Del sistema de vigilancia electrónica	126
Artículo 10°	Obligación del monitoreo	126
Artículo 11°	Frecuencia de Operaciones del sistema de seguridad y vigilancia	126

CAPÍTULO III DE LA INSTALACIÓN Y EL FUNCIONAMIENTO

Artículo 12°	Instalación de los equipos de vigilancia	126
Artículo 13°	Responsable de infraestructura	126
Artículo 14°	De la ubicación de las Cámaras	127
Artículo 15°	Monitoreo de las cámaras	127
Artículo 16°	Medidas de seguridad para el acceso a las Grabaciones	127
Artículo 17°	Prohibiciones	127

CAPÍTULO IV
DEL ALMACENAMIENTO Y RECOJO DE LAS GRABACIONES

Artículo 18°	Tiempo de Custodia de las Grabaciones	127
Artículo 19°	Del almacenamiento de las grabaciones.	128
Artículo 20°	Procedimiento para el recojo y custodia de las grabaciones	128
Artículo 21°	Manejo y resguardo de las grabaciones de seguridad	130

CAPÍTULO V
DE LA CUSTODIA Y USO DE LAS GRABACIONES

Artículo 22°	Custodia.	130
Artículo 23°	Del uso de las grabaciones.	130
Artículo 24 °	Procedimientos para el uso de las grabaciones de seguridad y vigilancia.	130

MANUAL DE PROCEDIMIENTOS PARA EL USO DE CÁMARAS DE SEGURIDAD Y VIGILANCIA

CAPÍTULO I ASPECTOS GENERALES

Artículo N° 01 Objetivo del procedimiento

El presente “Manual de Procedimientos para el uso de cámaras de seguridad y vigilancia a las actividades desarrolladas en el módulo dos de la facultad de ciencias integradas de la Universidad Autónoma Juan Misael Saracho de Bermejo tiene el fin de normar, regular e identificar los procedimientos para el debido uso de los equipos y grabaciones como medida de seguridad.

Artículo N° 02 Ámbito de Aplicación

El presente Manual de Procedimientos es de aplicación obligatoria para los trabajadores de esta institución.

Artículo N° 03 Responsables de su aplicación

El área de Seguridad de la Institución se hará cargo a través del encargado de Tic, se encargará de aplicar, controlar y verificar el cumplimiento del presente “Manual de Procedimientos para el uso de las cámaras de seguridad y vigilancia”

Artículo N° 04 Base Legal

El presente Manual de Procedimientos, tiene como base legal las siguientes disposiciones:

- Constitución Política del Estado.
- Ley No. 264 Sistema Nacional de Seguridad Ciudadana “Para una vida segura”, DS N.º 1436, 14 de diciembre de 2012.

Artículo N° 05 Definiciones

Para efectos de mejor entendimiento del presente manual, se tiene las siguientes definiciones;

MAE: Máxima Autoridad Ejecutiva de la Institución en la jerarquía de la organización administrativa en la institución Juan Misael Saracho.

N.V.R.: es un grabador de video en red.

Custodia: acción de vigilar o cuidar de algún bien.

Grabaciones: Es el proceso de capturar datos o imágenes y convertir la información a un formato almacenado en un medio de almacenamiento.

Cámaras de Video: Dispositivos portátiles que sirven para capturar imágenes en secuencia continuada en formato de video.

Monitoreo: Es el proceso sistemático de recolectar, analizar y utilizar información para hacer seguimiento al progreso de un programa en pos de la consecución de sus objetivos, y para guiar las decisiones de gestión.

Artículo N° 06 Difusión

El Área de Asesoría Legal a través del encargado de TIC son los responsables de la difusión del presente manual de procedimientos, en coordinación con el área de Seguridad.

Artículo N° 07 De su modificación

El presente manual de procedimientos podrá ser modificado total o parcialmente, en concordancia con las disposiciones legales en vigencia únicamente con la aprobación del directorio de la institución.

Artículo N° 08 Responsabilidades

La Unidad Administrativa Financiera a través del encargado de TIC serán las directas responsables de la puesta en funcionamiento, mantenimiento y reparación de las cámaras, cables, equipos y accesorios que forman parte del sistema de seguridad y vigilancia además del custodio de las grabaciones de imágenes de seguridad bajo los principios de eficacia, eficiencia, economía, celeridad y transparencia.

El encargado de TIC será el encargado directo de la administración y monitoreo de las cámaras de seguridad, así como también será el directo responsable del acceso a las grabaciones de imágenes.

CAPITULO II SISTEMA DE SEGURIDAD Y VIGILANCIA

Artículo N° 09 Del sistema de seguridad y vigilancia electrónica

Como medida de seguridad y para la protección de los servidores públicos, estudiantes, visitantes y de la propiedad privada bienes muebles e inmuebles de la institución, es que se establece en la administración y en los puestos de control, un sistema de seguridad y vigilancia mediante el uso de cámaras.

Artículo N° 10 Obligación del Monitoreo de Cámaras

El Área de Seguridad tiene la obligación a través de sus agentes de control y/o responsable de monitoreo de cámaras, el de identificar y reportar cualquier novedad o caso fortuito, temporal o accidental e inesperado, ocurrido a las cámaras de seguridad y vigilancia.

Artículo N° 11 Frecuencia de operaciones del sistema de seguridad y vigilancia

El sistema de seguridad y vigilancia operará las veinticuatro (24) horas del día, los 365 días del año, estando sujeto a cualquier desperfecto mecánico imprevisto ya sea por fallas técnicas o por inclemencias del tiempo (fuertes lluvias o tormentas eléctricas).

CAPITULO III DE LA INSTALACIÓN Y EL FUNCIONAMIENTO

Artículo N° 12 Instalación de los equipos de vigilancia

El encargado de TIC dependiente del Área de Dirección de Administración es el encargado de la instalación de las cámaras y los equipos necesarios para el funcionamiento del sistema de seguridad y vigilancia, además se encargará de proveer el mantenimiento necesario para que puedan funcionar de manera efectiva y se puedan mantener en condiciones óptimas.

Artículo N° 13 Responsable de infraestructura

El responsable de infraestructura deberá de elaborar y actualizar en cada periodo de la gestión en base a criterios técnicos y al crecimiento de la infraestructura institucional, un plano de ubicación de las cámaras de seguridad y vigilancia, debiendo proporcionar esta información de manera oportuna al encargado de TIC en coordinación con el responsable de Área de vigilancia.

Artículo N° 14 De la ubicación de las cámaras

Las cámaras de seguridad estarán ubicadas en lugares estratégicos específicamente para la seguridad y vigilancia de las instalaciones y la propiedad pública y privada que realicen actividades dentro de los perímetros del bloque de la institución.

Artículo N° 15 Monitoreo de Cámaras

La Unidad de Fiscalización por intermedio del responsable del área de seguridad se encargaran de controlar, registrar y reportar mediante informes diarios de novedades, los eventos fuera de las condiciones normales que se observe a través de las cámaras de seguridad y vigilancia, estas imágenes se grabaran en formato digital y podrán ser observadas a tiempo real por el encargado de seguimiento y monitoreo de cámaras detallando las actividades que se llevan a cabo en las instalaciones de la institución, así mismo las rondas que realizan los agentes de control operativo, deberán de informar al encargado de TIC si es que alguna cámara de seguridad y vigilancia está en mala posición o si tiene algún percance o desperfecto para su normal funcionamiento.

Artículo N° 16 Medidas de seguridad para el acceso al sistema

El ingreso al sistema de seguridad y vigilancia electrónica estará restringido, bajo un código clave de un usuario y contraseña, teniendo único acceso al mismo el encargado de TIC autorizado por la dirección de administración.

Artículo N° 17 Prohibiciones

Quedan prohibidos los siguientes usos de cámaras de seguridad y vigilancia:

- a) Vigilancia mediante uso de cámaras de seguridad con el propósito de monitorear a los servidores en sus áreas de trabajo, excepto en las oficinas de los puestos de control como medida de seguridad.
- b) Las cámaras de seguridad no se colocarán en las oficinas, cubículos, los baños u otro lugar u oficina que vulnere el derecho a la privacidad de las personas excepto en los puestos de control como medida de seguridad.

CAPÍTULO IV DEL ALMACENAMIENTO DE LAS GRABACIONES

Artículo N° 18 Tiempo de Custodia de las grabaciones

Se establece (1) año para que este en custodia el archivo histórico del sistema informático de la institución, así como la documentación respaldatoria.

Artículo N° 19 Del almacenamiento de las grabaciones

Las grabaciones que resulten del sistema de seguridad y vigilancia se guardarán y mantendrán en la memoria del servidor (NVR) por el lapso de sesenta días (31) días, una vez utilizado todo el espacio en el disco de memoria del NVR, el sistema automáticamente sobrescribirá las grabaciones anteriores por unas nuevas.

Artículo N° 20 Procedimiento para el recojo y custodio de las grabaciones

El encargado de TIC elaborará su cronograma de actividades de manera mensual, donde establecerá el tiempo que le permitan realizar las copias de seguridad de las grabaciones a un disco de memoria externa.

N° 01	DESCRIPCION DEL PROCEDIMIENTO	
Paso	Responsable	Actividad
1	Encargado de TIC	Ingreso al sistema de seguridad y vigilancia mediante un usuario y contraseña
2	Encargado de TIC	Selección de las grabaciones y/o los días que se realizara las copias de seguridad
3	Encargado de TIC	Realiza la copia de seguridad (Backup) en disco de memoria externa
4	Encargado de TIC	Resguarda y custodia las copias de seguridad de las grabaciones en un ambiente seguro
		FIN DEL PROCEDIMIENTO

Tabla 35. Procedimiento para el recojo y custodio de las grabaciones

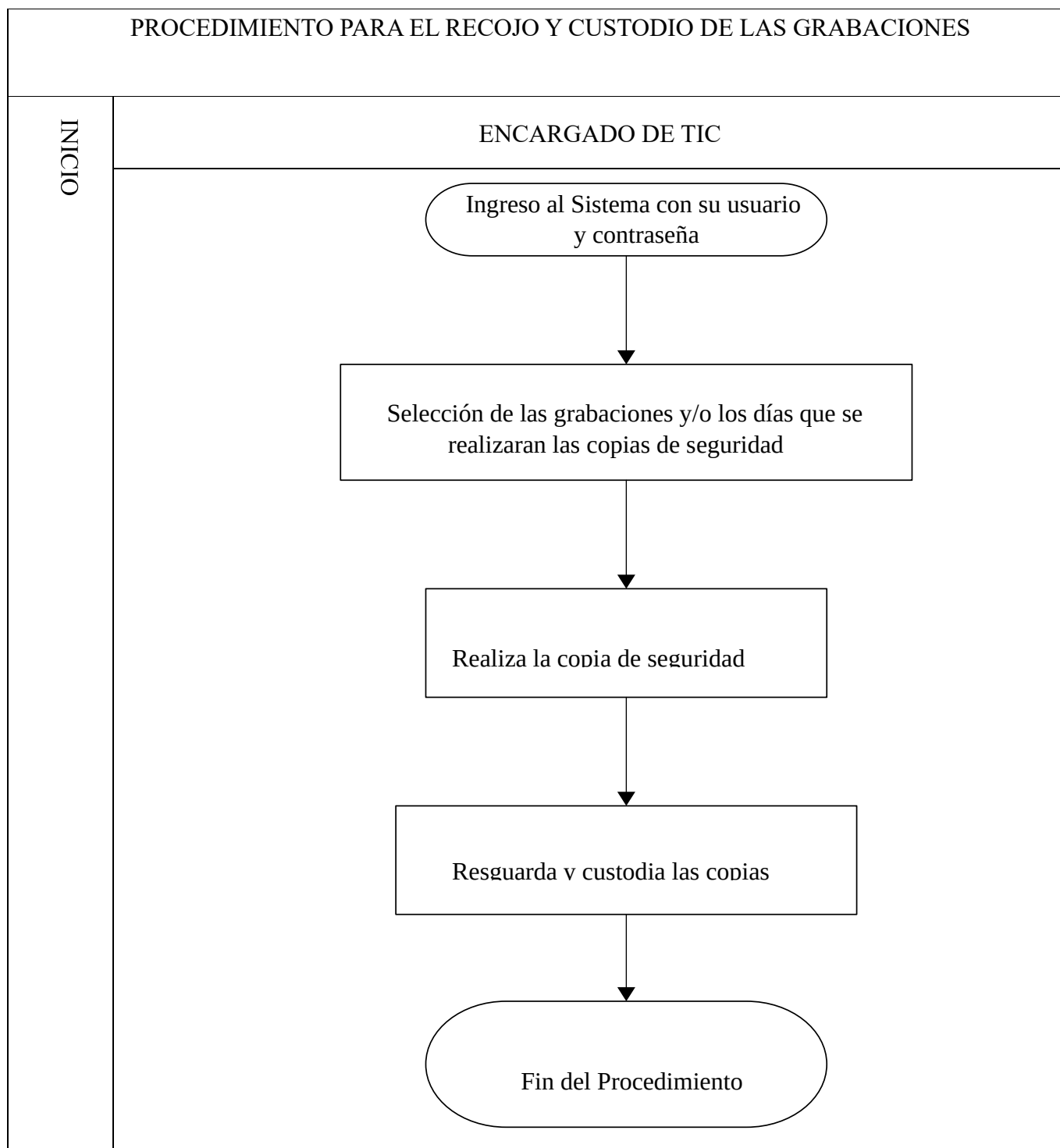


Figura 63. Procedimiento para el recojo y custodio de las grabaciones

Artículo N° 21 Manejo y resguardo de las grabaciones de seguridad

Las memorias externas o discos externos que contienen las copias de las grabaciones de seguridad y vigilancia de la Institución deberán estar debidamente resguardadas en ambientes óptimos para su conservación y utilización bajo llave y de acceso restringido.

CAPÍTULO V DE LA CUSTODIA Y USO DE LAS GRABACIONES

Artículo N° 22 Custodia

La custodia y la disposición de los discos o memorias externas que contengan las copias de seguridad de las grabaciones del sistema de seguridad y vigilancia, estarán a cargo del encargado de las TIC en un ambiente adecuado para su conservación y bajo llave.

Artículo N° 23 Del uso de las grabaciones

Las grabaciones de seguridad y vigilancia estarán resguardadas y el uso de las mismas estará bajo la autorización de la máxima autoridad de la institución, cualquier trabajador, persona natural o jurídica que quiera examinar las grabaciones deberá enviar una solicitud por escrito a la Dirección de la Institución haciendo referencia a las razones por las que se quiere examinar dichas grabaciones, el lugar y las horas aproximadas.

Artículo N° 24 Procedimientos para el uso de las grabaciones de seguridad y vigilancia

Se establece el siguiente procedimiento:

N° 03	DESCRIPCIÓN DEL PROCEDIMIENTO	
Paso	Responsable	Actividad
1	Persona Natural o Jurídica	Solicitud al director de la institución, especificando el motivo para examinar las grabaciones, el lugar y las horas aproximadas
	MAE	Deriva la nota a la dirección de administración.
2	Dirección de administración	Realiza el análisis de la solicitud y deriva al responsable del área de seguridad si corresponde.
3	Responsable de seguridad	Se dirige al encargado de TIC para examinar las grabaciones según solicitud del interesado.

4	Encargado de TIC	Realiza la copia de la grabación conforme al día y hora que solicita y lo pasa al responsable de seguridad.
5	Responsable de Seguridad	Verifica los hechos suscitados y envía un informe a la dirección General.
6	Área Legal	Da respuesta a lo solicitado enviando un informe y una copia de la grabación si así el hecho lo amerita a Dirección General.
		FIN DEL PROCEDIMIENTO

Tabla 36. Procedimientos para el uso de las grabaciones de seguridad y vigilancia

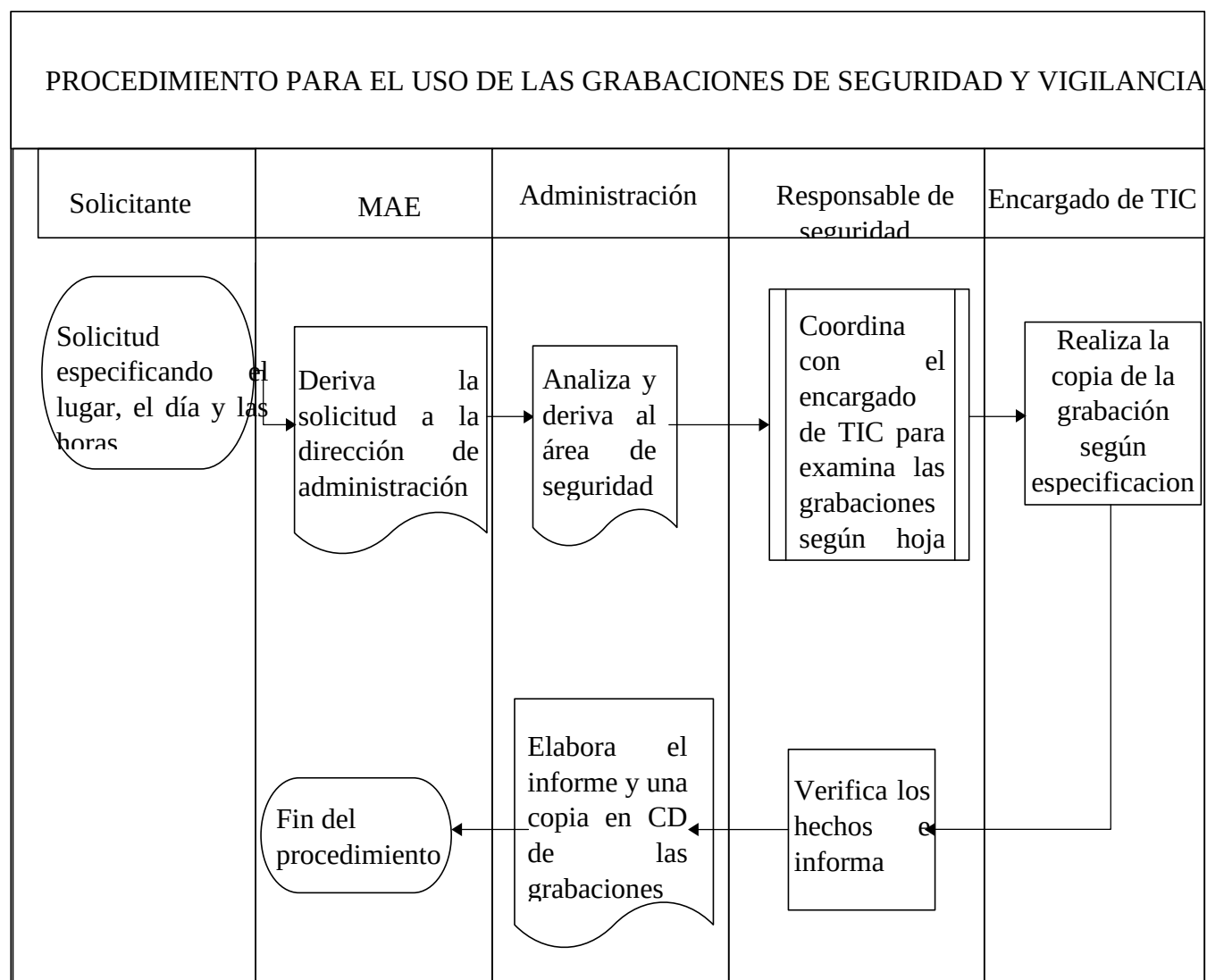


Figura 64. Procedimientos para el uso de las grabaciones de seguridad y vigilancia

CAPÍTULO III
CONCLUSIONES Y
RECOMENDACIONES

Capítulo 3: Conclusiones y Recomendaciones

I.8 Conclusiones

En base a el proyecto finalizado se pudieron sacar las siguientes conclusiones:

- Como resultado se logró diseñar una red de videovigilancia totalmente optima y funcional que cubre eficientemente los puntos críticos del bloque.
- Mediante el análisis de marcas lideres del mercado y las fichas técnicas de cada equipo, se pudo interpretar que la elección de equipos fue certera; corroborando que los equipos seleccionados son totalmente compatibles y funcional al proyecto.
- Se logró determinar las áreas críticas del bloque y de eso modo también definir sitios estratégicos para los equipos, con el fin de garantizar un proyecto competente.
- Se concluyó por optar una topología tipo estrella, ya que esta centralizará la red, haciendo más óptimo y sencilla su administración asi como tambien su mantenimiento.
- De acuerdo a los análisis realizados se concluyó en cuanto a tipos de sistemas de videovigilancia, optar por el cctv ip, este mismo nos brinda muchas ventajas, entre ellas: la adaptabilidad, mayor calidad de imagen, fácil instalación y accesibilidad, más seguridad, entre otras. Características fundamentales para un sistema de seguridad.
- Se obtuvo un manual de procedimientos que proporciona una guía detallada y estructurada para realizar las tareas de manera eficiente y consistente.
- En definitiva, el manual de procedimientos precisa cada tarea a seguir en base a los roles asignados y las actividades que estos desarrollan.
- Para terminar, el manual de procedimientos sirve como referencia para los empleados, proporcionándoles instrucciones claras sobre cómo llevar a cabo sus responsabilidades laborales.
- En pocas palabras el manual funciona como un registro de las operaciones y procedimientos utilizados en la organización, lo que facilita la revisión y la auditoría interna.

I.9 Recomendaciones

- En cuanto al calentamiento de equipos es recomendable tener una ventilación adecuada, ya sea en el cuarto de equipos y en el de monitoreo.
- Es recomendable contratar un servicio de ancho de banda que brinde un servicio optimo y estable, además de un ancho que cubra nuestras necesidades.
- Se recomienda usar otros softwares de monitoreo como zabbix, los cuales son más sencillos y completos, de otro modo igual el software del nvr es bastante cumplidor.
- Es recomendable tener equipos de una misma marca, esto es sumamente factible en cuanto a compatibilidad para garantizar el buen funcionamiento entre los equipos.
- En la emulación de las cámaras como en cálculo de ancho de banda se deben de cuidar el tener los parámetros correctamente definidos.
- Es sumamente recomendable primero analizar los puntos ciegos de una infraestructura para consecutivamente determinar los equipos, diseño, etc.
- Colocar tuberías, canaletas y bandejas por el recorrido del cableado para así proteger el cableado de daños, además de brindar una red organizada y estética visualmente.