**Universidad Nacional Autónoma de Nicaragua, UNAN – León**
**Facultad de Ciencias y Tecnología**
**Ingeniería en Telemática**

# *Re-activación del sistema de vídeo vigilancia IP dentro de los laboratorios del Dpto. de Computación de la Facultad de Ciencias y Tecnología de la Universidad Nacional Autónoma de Nicaragua, León. Agosto 2017 - Marzo 2018.*

**Monografía para optar al título de Ingeniero en Telemática**

Autores:
Br. José Aurelio Medina Quintero.
Br. Franklin Javier Reyes Paniagua.

Tutor:
Julio César Moreno

León, Nicaragua
29 de enero de 2019

*Re-activación del sistema de vídeo vigilancia IP dentro de los laboratorios del Dpto. de Computación de la Facultad de Ciencias y Tecnología de la Universidad Nacional Autónoma de Nicaragua, León. Agosto 2017 - Marzo 2018.*

# Resumen

La presente monografía se realizó en el Dpto. de Computación de la UNAN-León, cuidad de León, Nicaragua en el año 2018. En dicho recinto universitario se ofertan las carreras de Ing. En Telemática e Ing. en Sistemas de Información con un promedio de 512 estudiantes por carrera, los laboratorios de Computación albergan equipos de cómputo con un total de 320 PC distribuidas entre si y son usadas por estudiantes y docentes entre las horas de 7:00 AM – 7:00 PM. El cual cuenta con un sistema de video vigilancia con un aproximado de 2 cámaras de video vigilancia IP dentro de cada uno de los siguientes laboratorios: Hardware, Alcalá I, Alcalá II, Laboratorio CISCO y Laboratorio I.

El desarrollo de este trabajo está pensado para resolver los problemas relacionados con el control de concurrencia de personas y el cuidado de los laboratorios de computación utilizando las herramientas de video vigilancia IP que hasta antes de la realización del presente trabajo estaban prácticamente en desuso en estos laboratorios. Debido a la falta del uso en el sistema de video vigilancia IP instalados en los laboratorios de computación.

Dada la situación actual del sistema de video instalado se han realizado pruebas con el software libre llamado Zoneminder para la mejoría de dicho sistemas como son el aumento de disco duro en el sistema, seguridad al usuario a través de recaptcha, creación de certificados SSl con el objetivo de que la información de la web vaya cifrada y enmascarar los datos que ahí se manejan para la configuración de zoneminder , optimización de la base de datos del servidor, configuración de filtros de limpieza de datos guardados, grabación de vídeo al detectar movimiento, entre otras. El servidor empleado utiliza sistema operativo Debian v9 con sistema de gestión de ventanas LightDM para dar soporte a equipos con características y prestaciones reducidas; y sistema de administración de volúmenes de datos LVM.

El presente trabajo se trata de una investigación centrada en encontrar mecanismos o estrategias que permitan alcanzar con los objetivos propuesto, por tal razón el tipo de investigación es: Investigación aplicada.

# Dedicatoria

El presente trabajo investigativo lo dedicamos principalmente a Dios, por ser el inspirador y darnos fuerza para continuar en este proceso de obtener uno de los anhelos más deseados.

A nuestros padres, por su amor, trabajo y sacrificio en todos estos años, gracias a ustedes hemos logrado llegar hasta aquí y convertirnos en lo que somos. Ha sido el orgullo y el privilegio de ser sus hijas, son los mejores padres.

A nuestros hermanos (as) por estar siempre presentes, acompañándonos y por el apoyo moral, que nos brindaron a lo largo de esta etapa de nuestras vidas.

A todas las personas que nos han apoyado y han hecho que el trabajo se realice con éxito en especial a aquellos que nos abrieron las puertas y compartieron sus conocimientos.

# Agradecimientos

Agradecemos a Dios por bendecirnos la vida, por guiarnos a lo largo de nuestra existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

Gracias a nuestros padres, por ser los principales promotores de nuestros sueños, por confiar y creer en nuestras expectativas, por los consejos, valores y principios que nos han inculcado.

Agradecemos a nuestros docentes de la Universidad UNAN-León Nicaragua, por haber compartido sus conocimientos a lo largo de la preparación de nuestra profesión, de manera especial, al master Julio Cesar Gonzales Moreno tutor de nuestro proyecto de investigación quien ha guiado con su paciencia, y su rectitud como docente.

# Índice general

# Índice de ilustraciones

# Introducción

Muchos administradores suelen utilizar sistemas de video vigilancia, ya sea de conexión directa o a través de IP con diferentes fines. Los fabricantes de cámaras web suelen ofrecer a los usuarios un sencillo software que permite ver lo que la cámara capta en el momento exacto, sin embargo, este software generalmente es bastante sencillo y sus funciones son insuficientes para la mayoría de administradores. Estos sistemas son muy comunes en edificios de oficinas, áreas de seguridad, universidades, etc., ya que es fundamental controlar los accesos a determinadas zonas, tanto dentro como fuera del horario de trabajo.

En el Dpto. de Computación de la UNAN-León se ofertan las carreras de Ing. En Telemática e Ing. en Sistemas de Información con un promedio de 512 estudiantes por carrera, los laboratorios de Computación albergan equipos de cómputo con un total de 320 PC distribuidas entre si y son usadas por estudiantes y docentes entre las horas de 7:00 AM – 7:00 PM. Con el fin de proteger los bienes pertenecientes a la UNAN-León , el sistema de video vigilancia IP en los laboratorios se instaló por vez primera en el año 2010 como una medida ante los equipos sustraídos de forma ilegal por los usuarios de dichos laboratorios ya que en su momento se encontraron a dos estudiantes sustrayendo hardware sin permiso; el responsable de la instalación fue el Ing. Denis Berrios, con un total de 2 cámaras de video vigilancia IP dentro de cada uno de los siguientes laboratorios: Hardware, Alcalá I, Alcalá II y Laboratorio I. Las marcas se corresponden a: D-link, modelo: DCS 2102 junto con un servidor Windows 7.

Debido a la capacidad de 500 Gb de almacenamiento en el servidor, este sistema era capaz de grabar durante una semana de corrido y de forma continua (sin detección de movimiento) y se podía acceder a estas grabaciones desde el servidor ubicado en la oficina del personal encargado de la motorización (contiguo al Laboratorio I). Véase Anexos sección 1. Entrevistas. En el periodo de realización del presente trabajo, debido al daño en el hardware del equipo servidor de almacenamiento de las grabaciones y por la falta de presupuesto para el remplazo de piezas en mal estado, este sistema no está funcionando siendo así más difícil para los encargados poder mantener un control y regulación en el acceso a estos laboratorios pudiendo notar una gran diferencia entre contar con un sistema funcionando a un sistema que no lo este. La propuesta elaborada en el presente trabajo surge por la necesidad de reactivar el sistema de video vigilancia debido a las pérdidas o daños continuos en los equipos de cómputo que se tiene en los diferentes laboratorios de computación y con el fin de beneficiar al Dpto. de computación, a sus estudiantes y a todo el personal que labora en dicho Dpto. 1El desarrollo de este trabajo está pensado para resolver los problemas relacionados con el control de concurrencia y el cuidado de los laboratorios de computación utilizando las herramientas de video vigilancia IP que actualmente están prácticamente en desuso en estos laboratorios. Debido a la falta del uso en el

sistema de video vigilancia IP instalados en los laboratorios de computación, se han detectado pérdidas monetarias a consecuencias del mal uso o la sustracción de equipos por usuarios que con frecuencia acceden, por lo cual el Dpto. de Computación ha determinado que es una necesidad contar con la presencia de este tipo de sistemas que permitan mantener una vigilancia remota y constante. Lo que se pretende es controlar y disminuir las perdidas y sustracciones de los equipos y accesorios del laboratorio de computación mediante la reactivación del sistema de video vigilancia IP. No solo es una reactivación del sistema sino más bien una mejora para obtener un sistema más eficiente, confiable, funcional y de bajo coste, este sistema deberá ser capaz de soportar, a futuro, un incremento de cámaras que este asociado con la cantidad de laboratorios disponibles, permitir la captura y envió del video a través de una red, él envió de notificaciones con destinos a correos electrónicos previamente seleccionados y admitirá a usuarios autorizados acceder simultáneamente a las imágenes captadas.

# Antecedentes

Se ha hecho una revisión de las publicaciones de investigaciones realizadas en el Departamento de Computación de la UNAN-León de forma específica, no se han encontrado trabajos que se refieran a reactivación de sistemas de video vigilancia IP. Por lo tanto, se extendió la revisión de antecedentes hacia otras universidades tanto en Nicaragua como internacionales; y se encontraron los siguientes:

1) ***Sistema de seguridad electrónica utilizando la red de datos en la Cooperativa Masiguito ubicado en el municipio de Camoapa, Departamento de Boaco en el año 2016.***

Autores: Holman Yasir Rivera Guevara y Douglas Javier Sequeira Ortiz.
Universidad Nacional de Ingeniería, Managua, Nicaragua. Año: 2016.

El presente trabajo se desarrolló para la empresa de lácteos Cooperativa Masiguito ubicada en la ciudad de Camoapa, Departamento de Boaco, Nicaragua en el año 2016 con la finalidad de aportarles los conocimientos necesarios tanto en especificaciones técnicas como en costos requeridos para implementar un sistema de seguridad electrónica que corresponde a un circuito cerrado de televisión (CCTV) y control de acceso(CAA) utilizando la red de datos que poseen actualmente, para erradicar las problemáticas en cuanto a pérdidas de bienes y producción de la empresa. En la visita de campo al lugar se logró determinar las áreas a monitorear y los sitios en donde se requiere tener un control de acceso, estos puntos se decidieron en conjunto con el gerente general y el responsable de informática cumpliendo con los requerimientos de la empresa. Para el diseño y propuesta de ubicación de equipos electrónicos que garanticen la seguridad del sitio, se utilizaron herramientas informáticas como lo es el software AutoCAD, el cual visualizando un plano de conjunto y de almacén proporcionado por el responsable de informática, se lograron identificar las medidas aproximadas de los puntos críticos de la empresa. Además se utilizaron las normas NFPA731 que rigen la instalación y canalización de sistemas de seguridad en establecimientos, así como también los requerimientos que establece el fabricante de la marca que se propone. Recopilando información en la empresa Ultra de Nicaragua (ULTRANIC) se seleccionó la marca Samsung con la serie de cámaras de seguridad Wisenet lite que cumple con los estándares de calidad que se necesita, ya que el municipio de Camoapa presenta un clima bastante húmedo a lo largo del año.

2) *Vigilancia electrónica monitorearle remotamente en las oficinas centrales de la escuela superior politécnica agropecuaria de Manabí Manuel Félix López.*

Autor: Manuel De Jesús Macías Ramírez.
Escuela superior politécnica agropecuaria de Manabí Manuel Félix López. Ecuador.
Año: 2012.

El objetivo principal del presente trabajo de monografía es implementar un sistema vigilancia electrónica monitorearle remotamente en las oficinas centrales de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, misma que permitió registrar audio y video desde Internet. El sistema incorpora audio bidireccional, lo que permitió escuchar lo que pasa en el área de monitoreo a través del PC. Para la ejecución del sistema se trabajó con la metodología SOFTCAL, misma que mediante procesos secuenciales permitió el desarrollo cabal del sistema. Fue necesario recopilar información, que permitió desarrollar un diseño en base a los requerimientos de la institución, se codificó el sistema con IP público según especificaciones técnicas. El software empleado para el monitoreo de las cámaras de vigilancia IP fue DCS-2121, D-Viewcam 2,0 diseñado para centralizar la gestión de múltiples cámaras IP. El Sistema de vigilancia es una solución versátil y única, que permite acceder de forma remota y controlada desde cualquier PC o portátil a través de la red local o a través de Internet mediante un navegador web.

### *3) Diseño de un sistema de video-monitoreo IP para la sala de Manufactura del Centro de Tecnologías Avanzadas de Manufactura (CETAM)*

Autor: Gigi Vanessa Laura Namuche.
PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ FACULTAD DE CIENCIAS E INGENIERÍA. Lima-Perú.
Año: 2013.

La presente monografía se enfocó en el diseño del sistema de video monitoreo IP en el laboratorio de Manufactura del Centro de Tecnologías Avanzadas de Manufactura (CETAM) que se encuentra ubicado en la Pontificia Universidad Católica del Perú (PUCP), el cual basa su funcionamiento en el desarrollo de un prototipo conformado por cámaras IP, las cuales serán los dispositivos de transmisión de video; inyectadoras Poe, encargados de transmitir energía eléctrica a través de cable de datos Ethernet; un switch; servidores de Streaming y Web para la transmisión de datos a través de Internet.

Estos antecedentes fueron seleccionados debido a su gran aporte para el desarrollo de las bases del presente trabajo; así como también la vinculación cercana que estos trabajos tienen asociada a la problemática que se está intentando resolver.

# Planteamiento del problema

Las cámaras de video vigilancia a través del protocolo IP han evolucionado a lo largo de los años desde su creación en el año 1996 por Martin Gren cofundador de Axis Communications empresa que brinda los servicios de vídeo en red. A pesar de la creación de las cámaras IP en 1996 no fue hasta el año 2002 que se empezaron a implementar con mayor significación las cámaras en red, de ahí la importancia de las cámaras en red en la vigilancia ya sea de empresas, instituciones, negocios pequeños y hogar.

En Centro América los sistemas de video vigilancia cada vez se están volviendo más útiles e indispensables haciendo cada vez más importante el uso de las cámaras IP para realizar tareas tanto de video vigilancia, como también tareas más básicas como la supervisión de empleados en una empresa y supervisión de procesos automatizados realizados por algún tipo de maquinaria dentro de las empresas.

Estos sistemas y servicios actualmente en Nicaragua muchas veces son limitados ya generalmente los servicios instalados en las empresas o negocios como tiendas y tramos de mercados no brindan muchas opciones de almacenamiento y reconocimiento facial o las cámaras no tienen mucha resolución dificultando así el monitoreo o revisión al momento de un acontecimiento como por ejemplo un robo en donde no es posible reconocer a los malhechores o la calidad/cantidad del vídeo es muy limitada al momento de reproducirlo.

Actualmente el servicio de video vigilancia instalado en la UNAN-León específicamente en algunos laboratorios de computación, está prácticamente en desuso y las cámaras instaladas están deteriorándose cada vez más sin sacarle provecho alguno, permitiendo así un descontrol o incertidumbre a la hora del extravió de algún accesorio olvidado o de equipo sustraído en dichos laboratorios.

Por lo dicho antes es necesario una reactivación en el sistema de video vigilancia IP instalado en los laboratorios; puesto que la instalación a la fecha de realización del presente trabajo estaba en prácticamente en desuso e implicó una inversión que el Dpto. de Computación tuvo que realizar para tratar evitar las pérdidas. La reactivación ayudaría a mantener un control de los accesorios olvidados por los estudiantes y a la vez un control y vigilancia de los accesorios pertenecientes al Dpto. de Computación alojados dentro de dichos laboratorios.

Actualmente la vigilancia y supervisión de los accesorios e ingreso de los estudiantes a los laboratorios recae en los propios docentes solamente en el horario de las clases asignadas en dichos laboratorios; los encargados de la seguridad interna solo están a cargo de la apertura y cierre de dichos laboratorios, más no así de su respectiva revisión. La situación actual en cuanto a los accesorios y laboratorios como tal es un poco limitada ya que no se tiene control al momento de extravió de alguno de sus accesorios, siendo los laboratorios muy concurridos por los estudiantes y personal

docente se hace aún más difícil la tarea de realizar un control más efectivo.

Si no se lleva a cabo la reactivación del sistema de video vigilancia ya instalado; significaría un derroche de los recursos con los cuales cuenta el Dpto. de Computación ya que las cámaras instaladas se deteriorarían sin haber sido usadas para el fin con el que fueron originalmente adquiridas.

## *Preguntas de investigación.*

¿Cómo llevar a cabo la reactivación del sistema de video vigilancia IP instalado en algunos de los laboratorios del Dpto. de Computación de la UNAN-León?

### *Preguntas Directrices.*

¿Cuál es la situación actual del sistema de video vigilancia IP instalado en los laboratorios del Dpto. de Computación?

¿Qué modificaciones hay que realizar en el sistema actualmente instalado?

¿Qué equipos y tecnologías serían necesarias para llevar a cabo el proceso de reactivación?

¿Qué mejoras se podrían aportar al sistema de video vigilancia IP ya instalado para hacer que la tarea de video vigilancia sea más efectiva?

# Justificación

Los usuarios que tienen acceso a los laboratorios de computación son numerosos (aproximadamente 35 estudiantes en cada sesión de laboratorio) esto conlleva a que los equipos de cómputo estén expuestos a un mal uso o a ser sustraídos. A los administradores de los laboratorios cada vez se les hace más difícil poder mantener un control para evitar pérdidas y daños de los equipos, Por tanto, en el presente trabajo se pretende llevar a cabo la reactivación del sistema de video vigilancia IP instalado en algunos de estos laboratorios como una posible solución a la problemática planteada.

La reactivación del sistema de video vigilancia IP ya instalado en los laboratorios del Dpto. de Computación de la UNAN-León es necesaria, ya que en el periodo de realización del presente trabajo, se comprobó el desuso de dicho sistema; según indicaciones del responsable de gestión y supervisión del sistema Ing. Denis Berrios a través de una entrevista realizada por medio de un formulario electrónico (véase Anexos sección 1. Entrevistas), en donde confirma el desuso y su falta de funcionamiento. Es necesario recalcar que los encargados de la gestión y funcionamiento de la red de la UNAN-León quienes pertenecen al equipo de trabajo de la división de informática; son también usuario del sistema de video vigilancia IP para llevar a cabo un control de daños y manipulaciones inadecuadas dentro de la red física desplegada en cada uno de los laboratorios de Computación de la UNAN-León. Permitiéndoles, en su momento, detectar usuarios que hacían un uso indebido de la red y manipulaciones del cable, provocando bucles y afectaciones en el correcto funcionamiento de la red institucional.

La reactivación de este sistema permitirá aumentar la seguridad en los laboratorios y reducir el índice de delincuencia debido a la sustracción; y evitar el deterioro acelerado por mal uso en los equipos de cómputo. En más de una ocasión, los sistemas de video vigilancia IP se ha convertido en un aliado perfecto de los encargados de los laboratorios, ya que las grabaciones han servido para evitar pérdidas, o como indicio para conseguir pruebas en el caso de que éstos se hayan producido.

La ventaja de tener a la disposición estos sistemas, es que, el personal encargado de los laboratorios no necesita estar físicamente en el lugar de monitoreo para poder realizar el trabajo de mantener la seguridad; cada vez que ocurra algún incidente, se pueden consultar las grabaciones para comprobar lo que ocurrió. El objetivo de la reactivación de este sistema es identificar situaciones anormales mediante la utilización de cámaras IP ubicadas en sitios estratégicos, para controlar y vigilar el ingreso y salida de personas.

# Objetivos

## Objetivo general

- Reactivar el sistema de video vigilancia IP instalado en algunos de los laboratorios Del Dpto. de Computación de la UNAN-León a través de software web libre zoneminder instalado en sistema operativo Debian v9.

## Objetivos específicos

- Por medio de una entrevista determinar la situación actual del sistema de video vigilancia IP instalado en los laboratorios del Dpto. de Computación.

- Identificar las modificaciones que sean necesarias para realizar la reactivación del sistema de video vigilancia IP actualmente instalado.

- Evaluar los equipos y tecnologías necesarias para llevar a cabo el proceso de reactivación.

- Aplicar mejoras al sistema de video vigilancia IP ya instalado para hacer que la tarea de video vigilancia sea más efectiva.

# Marco teórico

A continuación, se desarrollan los conceptos teóricos necesarios para el adecuado entendimiento de los apartados que serán utilizados posteriormente y forman la base teórica para el desarrollo del presente trabajo.

## Conceptos generales.

1. Circuito Cerrado de Televisión (CCTV).

Originalmente, la video vigilancia se realizó utilizando un circuito cerrado de televisión. Esta tecnología utiliza cámaras de vídeo analógicas, cable coaxial y grabadoras de vídeo. Las cámaras transmiten una señal a un conjunto específico y limitado de monitores. Los sistemas de circuito cerrado de televisión suelen incluir un enlace de comunicaciones fijo entre cámaras y monitores, utilizando alambres y cables. (deskshare)

El Circuito Cerrado de Televisión es un sistema que se compone de tres partes principales: el grabador de video digital, el medio de transmisión y las cámaras de seguridad.

### 1.1. Cámaras

Estas pueden operar de acuerdo al requerimiento del usuario: de uso exterior o interior, diferentes tamaños de lentes, de estilos o de tecnologías de transmisión de video. (comocomprarcctv)

### 1.2. Medio de transmisión.

Estos medios pueden ser: cable UTP, cable coaxial, cable dúplex y de manera inalámbrica. En la elección del tipo de conductor y aleaciones tendrá que tener en cuenta: la distancia del tendido de cable que se necesita, la calidad del cable y sus componentes que escoja. Ten en cuenta que estos podrán asegurar, o no, la durabilidad de la instalación, la rápida y eficaz trasmisión de imágenes nítidas. Un buen cable garantiza que el sistema opere de manera óptima durante muchos años. Existen accesorios que trabajan en conjunto con los elementos anteriormente mencionados. Adaptadores de corriente, alarmas o bocinas son algunos de ellos. (comocomprarcctv)

### 1.3. Digital Video Recorder (DVR).

El grabador de video digital se encarga de recibir, digitalizar, comprimir y almacenar en un disco sucesos registrados por un conjunto de cámaras. Hay diferentes tipos de

DRVs que pueden variar en: número de canales, tipo de tecnología que utiliza (análogas, HD, digitales), capacidad de almacenamiento y procesamiento. (comocomprarcctv)

## 2. Vídeo en red

El vídeo en red, a menudo denominado videovigilancia basada en IP o vigilancia IP; tal como se aplica en el sector de la seguridad, utiliza una red IP inalámbrica o con cable como red troncal para transportar vídeo, audio digital y otros datos. Cuando se aplica la tecnología de alimentación a través de Ethernet (PoE), la red también se puede utilizar para transportar alimentación a los productos de vídeo en red. Un sistema de vídeo en red permite supervisar vídeo y grabarlo desde cualquier lugar de la red, tanto si se trata de una red de área local (LAN) o de una red de área extensa (WAN) como Internet.

Los componentes básicos de un sistema de vídeo en red son la cámara de red, el codificador de vídeo (que se utiliza para la conexión a cámaras analógicas), la red, el servidor y el almacenamiento, así como el software de gestión de vídeo. Como la cámara de red y el codificador de vídeo son equipos basados en ordenadores, cuentan con capacidades que no pueden compararse con las de una cámara CCTV analógica. La cámara de red, el codificador de vídeo y el software de gestión de vídeo y se consideran las piedras angulares de toda solución de vigilancia IP. Los componentes de red, servidor y almacenamiento forman parte del equipo de TI estándar. La posibilidad de utilizar un equipo listo para su uso común constituye una de las ventajas principales del video en red.

### 2.1. Ventajas del uso de un sistema de videovigilancia IP.

El sistema de videovigilancia IP ofrece toda una serie de ventajas y funcionalidades avanzadas que no puede proporcionar un sistema de videovigilancia analógico. Entre las ventajas se incluyen la accesibilidad remota, la alta calidad de imagen, la gestión de eventos, así como la posibilidad de una integración sencilla y una escalabilidad, flexibilidad y rentabilidad mejoradas.

#### *2.1.1. Accesibilidad remota.*

Se pueden configurar las cámaras de red y los codificadores y acceder a ellos de forma remota, lo que permite a diferentes usuarios autorizados visualizar video en vivo y grabado en cualquier momento y desde prácticamente cualquier ubicación en red. En un sistema CCTV analógico tradicional, los usuarios necesitarían encontrarse en una ubicación de supervisión in situ para ver y gestionar video, y el acceso al video desde fuera del centro no sería posible sin un equipo como un codificador de video o un grabador de video digital (DVR) de red. Un DVR es el sustituto digital de la grabadora de cintas de video.

### *2.1.2. Alta calidad de imagen.*

En una aplicación de videovigilancia, es esencial una alta calidad de imagen para poder capturar con claridad un incidente en curso e identificar a las personas u objetos implicados. Una cámara de red puede producir una mejor calidad de imagen y una resolución más alta que una cámara CCTV analógica.

En un sistema de vigilancia IP, las imágenes de una cámara de red se digitalizan una vez y se mantienen en formato digital sin conversiones innecesarias y sin degradación de las imágenes debido a la distancia que recorren por una red. Además, las imágenes digitales se pueden almacenar y recuperar más fácilmente que en los casos en los que se utilizan cintas de video analógicas.

### *2.1.3. Integración sencilla y preparada para el futuro.*

Los productos de videovigilancia en red basados en estándares abiertos se pueden integrar fácilmente con sistemas de información basados en ordenadores y Ethernet, sistemas de audio o de seguridad y otros dispositivos digitales, además del software de gestión de video y de la aplicación.

### *2.1.4. Escalabilidad y flexibilidad.*

Un sistema de videovigilancia en red puede crecer a la vez que las necesidades del usuario. Los sistemas basados en IP ofrecen a muchas cámaras de red y codificadores de video, así como a otros tipos de aplicaciones, una manera de compartir la misma red inalámbrica o con cable para la comunicación de datos; de este modo, se puede añadir al sistema cualquier cantidad de productos de video en red sin que ello suponga cambios significativos o costosos para la infraestructura de red.

### *2.1.5. Rentabilidad de la inversión.*

Un sistema de vigilancia IP tiene normalmente un coste total de propiedad inferior al de un sistema CCTV analógico tradicional. Una infraestructura de red IP a menudo ya está implementada y se utiliza para otras aplicaciones dentro de una organización, por lo que una aplicación de video en red puede aprovechar la infraestructura existente. Las redes basadas en IP y las opciones inalámbricas constituyen además alternativas mucho menos caras que los componentes utilizados por un sistema CCTV analógico. Los costes de gestión y equipos también son menores ya que las aplicaciones back-end y el almacenamiento se ejecutan en servidores basados en sistemas abiertos, de estándar industrial, no en hardware propietario como un DVR en el caso de un sistema CCTV analógico.

## 2.2. Protocolos.

El modelo de servicio best effort de IP ha demostrado ser una solución adecuada para el transporte de texto. (Jaun) En este modelo, IP hace todo lo posible para entregar los paquetes, pero no da ninguna garantía de que vayan a ser entregados. Por lo tanto, los paquetes se pueden perder o entregar desordenados y el retraso es impredecible.

El protocolo de transporte TCP (Transmission Control Protocol) permite aumentar la fiabilidad de los servicios extremo a extremo. De esta manera se soluciona la falta de fiabilidad de IP, ya que permite entregar los paquetes ordenados y retransmitir los paquetes perdidos. (Jaun)

TCP sobre IP es una buena solución, pero no es suficiente para transportar tráfico multimedia. En el caso de producirse pérdidas de paquetes, TCP retransmite los paquetes perdidos, pero no garantiza el retardo. Por este motivo, TCP no es adecuado para transportar el tráfico multimedia. La solución más adecuada seria utilizar UDP (User Datagram Protocol) como capa de transporte sobre IP. (Jaun)

Las aplicaciones multimedia precisan de ciertos servicios de transporte con características distintas de TCP y más funcionalidades que UDP. El protocolo diseñado para proporcionar estos servicios es RTP y RTSP.

### *2.2.1. Protocolo de transmisión de tiempo real.-RTP*

RTP proporciona funciones de transporte extremo a extremo adecuadas para las aplicaciones en tiempo real, como audio, vídeo o simulación de datos. RTP no se encarga de la reserva de recursos ni garantiza la calidad de servicio. (H. Schulzrinne S. C., 2003) El estándar RTP define dos protocolos: RTP y RTCP.

RTP se ocupa del intercambio de datos multimedia, mientras que RTCP se encarga de obtener información de control sobre la calidad de la transmisión en los receptores. Ambos protocolos están diseñados para ser independientes de las capas de transporte.

El vídeo y/o audio transportado por RTP se digitaliza utilizando un códec particular Estos bloques generados se encapsulan en paquetes RTP y, habitualmente, después en paquetes UDP e IP. (Jaun)

Cada paquete generado tiene una cabecera RTP en la que se incluye información especialmente útil para la reconstrucción de los datos multimedia. En esta cabecera se incluye el valor Payload Type para indicar qué tipo de codificación de audio o vídeo se ha utilizado en el transmisor, de manera que el receptor puede seleccionar el esquema de decodificación adecuado. También contiene información de los tiempos de los paquetes (Timestamp) y el número de secuencia, lo cual permite al receptor reconstruir la línea de tiempos generada en el transmisor para audio y vídeo. (H. Schulzrinne S. C., 2003)

### *2.2.2. Protocolo de transmisión streaming en tiempo real.*

En concreto, el propósito de este protocolo es controlar sesiones múltiples de transmisión de datos, proporcionar un medio para seleccionar los canales de transmisión como UDP, UDP multicast y TCP, y proporcionar un medio para seleccionar mecanismos de transmisión basados en RTP. Trabaja entre los clientes y los servidores RTSP. Además, está diseñado para trabajar con protocolos de nivel inferior como RTP. (Jaun)

Es un protocolo bidireccional para peticiones y respuestas, que primero se encarga de establecer un contexto incluyendo los contenidos y después controla la transmisión de estos contenidos desde el emisor hasta el receptor. RTSP tiene tres partes fundamentales: establecimiento de la sesión, control de la transmisión de datos y un modelo de ampliación del sistema. (H. Schulzrinne A. R., 2014)

Los servicios y operaciones que ofrece RTSP se utilizan por medio de llamadas a métodos. Los métodos indican qué se debe hacer sobre el recurso identificado con un URI en la petición.

Estos métodos son: OPTIONS, DESCRIBE, ANNOUNCE, SETUP, PLAY, PAUSE, TEARDOWN, GET_PARAMETER, SET_PARAMETER, REDIRECT y RECORD. Sin embargo, no es necesario utilizar todos los métodos RTSP para que una transmisión sea completamente funcional. (Jaun)

A continuación se va a describir brevemente cada uno de ellos:

- OPTIONS: El cliente o el servidor informa al otro extremo de las opciones que acepta.
- DESCRIBE: El cliente recupera del servidor la descripción de un recurso identificado con el URI incluida en la petición.
- ANNOUNCE: Al enviarse desde el cliente al servidor, establece la descripción de un recurso en el servidor. Si se envía desde el servidor al cliente, actualiza la descripción de la sesión en tiempo real.
- SETUP: El cliente solicita al servidor asignar recursos para un flujo de datos e inicia una sesión RTSP.
- PLAY: El cliente pide al servidor que comience la transmisión de datos a través del flujo asignado con SETUP.
- PAUSE: El cliente detiene temporalmente el flujo de datos, pero sin liberar los recursos del servidor.
- TEARDOWN: El cliente solicita al servidor detener la transmisión de un flujo concreto y libera los recursos asociados.
- GET_PARAMETER: Obtiene el valor de un parámetro concreto del recurso especificado en el URI.
- SET_PARAMETER: Establece el valor de un parámetro concreto del recurso especificado en el URI.
- REDIRECT: El servidor informa a los clientes de que se deben conectar a otro

servidor.
- RECORD: El cliente inicia la grabación de un conjunto de datos multimedia.

El valor del puerto por defecto con el que se asocia el protocolo RTSP es el puerto 554 tanto para TCP como para UDP.

## 3. Cámaras de red.

Son cámaras de seguridad pensadas para ser visualizadas mediante Internet o desde una red local. Las más clásicas y profesionales poseen un puerto Ethernet con terminal Rj45 y se conectan al switch o router mediante cable UTP. También hay cámaras IP inalámbricas, las cuales se conectan a nuestra red WIFI por una antena. Estas últimas cámaras si bien pueden ser efectivas para algunos casos, no entran dentro de la categoría de cámaras de seguridad profesionales debido a que la gran mayoría son de escasa calidad y los enlaces inalámbricos WIFI son muy fáciles de bloquear con un simple jammer.

### 3.1. Tipos de cámaras de red.

#### *3.1.1. Cámaras de red fijas*

**ILUSTRACIÓN 1. CÁMARA DE RED FIJA**

Una cámara de red satisface una gran variedad de necesidades de aplicación, y su diseño de cámara tradicional añade un efecto de disuasión. La dirección de visualización se determina una vez montada la cámara. Hay varios modelos con objetivos varifocales y/u objetivos intercambiables para disponer de más flexibilidad.

#### *3.1.2. Cámaras de red domo fijas*


**ILUSTRACIÓN 2. CÁMARA DE RED DOMO**

Una cámara de red domo fija consta de una cámara de pequeño tamaño pre instalada en una carcasa de forma abovedada. La ventaja principal radica en su discreto y disimulado diseño, así como en la dificultad de ver hacia qué dirección apunta la cámara. La carcasa abovedada de la cámara la protege de forma eficaz contra el re direccionamiento y el desenfoque. Se suelen instalar en el techo o en la pared.

### *3.1.3. Cámaras de red PTZ.*


**ILUSTRACIÓN 3. CÁMARA DE RED PTZ**

Una cámara de red PTZ ofrece funciones de vídeo en red combinadas con funciones de movimiento horizontal, vertical y zoom. El movimiento de la cámara se controla fácilmente mediante un ordenador conectado a la red. Según la aplicación, puede optar por una cámara de red PTZ en la que tanto el movimiento como la dirección de visualización sean visibles o un modelo más discreto, con todas las partes móviles dentro de la carcasa, o bien un modelo que no tenga partes móviles.

### *3.1.4. Cámaras de red domo PTZ.*

**ILUSTRACIÓN 4. CÁMARA DE RED DOMO PTZ**

Una cámara de red domo PTZ proporciona una gran flexibilidad gracias a su movimiento horizontal de 360°,amplias funciones de zoom, 180° de movimiento vertical y el avanzado diseño mecánico que permite un movimiento continuo. Las cámaras domo PTZ son ideales para la supervisión en directo, cuando el usuario desea seguir a una persona o un objeto. También pueden manejarse en el modo de recorrido protegido, en el que la cámara se mueve de una posición preestablecida a otra. En su uso en interiores, la cámara se instala en el techo o en un poste o esquina para instalaciones exteriores. (Communications)

## 3.2. Directrices para seleccionar una cámara de red

Dada la variedad de cámaras de red disponibles, resulta útil disponer de algunas directrices para seleccionar el tipo que mejor se adapte a sus necesidades.

### *3.2.1. Calidad de imagen.*

La calidad de imagen es uno de los aspectos más importantes de cualquier cámara, pero resulta difícil de cuantificar y medir. La mejor forma de determinar la calidad de imagen es instalar distintas cámaras y visualizar el video. En caso de que la prioridad sea la captura de objetos en movimiento.

### *3.2.2. Resolución.*

Para las aplicaciones que exijan imágenes con un alto nivel de detalle, las cámaras con resolución megapíxel pueden ser la mejor opción.

### *3.2.3. Compresión.*

Los tres estándares de compresión de video que ofrecen los productos de video más populares son H.264, MPEG-4 y Motilón JPEG. H.264 es el estándar más reciente y ofrece significativos ahorros en lo que a ancho de banda y almacenamiento se refiere.

### *3.2.4. Audio.*

En caso de que sea necesario disponer de audio, evalúe si se requiere audio mono direccional o bidireccional. Existen cámaras de red con soporte para audio se entregan con un micrófono incorporado y/o una entrada para micrófonos externos, así como un altavoz o una salida para altavoces externos.

### *3.2.5. Funcionalidades de red*

Las consideraciones incluyen PoE, cifrado HTTPS para cifrado de secuencias de video antes de que se envíen a través de la red, filtrado de direcciones IP, que permite o deniega los derechos de acceso a direcciones IP definidas, IEEE802.1X para controlar el acceso a una red, IPv6 y funcionalidad inalámbrica.

### ***3.2.6. Ubicación y cantidad cámaras IP.***

En el presente trabajo no se abordaran aspectos asociados a las ubicaciones de las cámaras IP y a la cantidad que son necesarias para monitorear un espacio físico utilizando un sistema de video vigilancia IP, pero se considera oportuno hacer una revisión sobre las ubicaciones y cantidad de cámaras IP instaladas. Para ello, es posible emplear el siguiente algoritmo.

#### *3.2.6.1. Algoritmo de galería de arte*

El algoritmo de galería de arte es un problema matemático, el cual se puede aplicar y relacionar con elementos reales de la vida cotidiana. Las personas suelen entender los problemas matemáticos si se aplican en ejemplos concretos en este caso en una “galería de arte” lo cual permite analizar el problema con mayor comprensión y profundidad permitiendo entenderlo y aplicándolo de manera más concreta, ya que los resultados matemáticos obtenidos tienen aplicaciones reales. (Ibáñez)

Este problema fue propuesto por el profesor matemático *Victor Klee* en 1973, a raíz del problema que se presentaba en una galería de arte en el área de matemática llamada “geometría combinatoria o computacional”, del cual surgió la pregunta *¿Cuál es el mínimo número de guardas, o cámaras de vigilancia, que se necesitan para vigilar una galería de arte?* (Anastopoulou Nicky, 2012)

Václav Chvátal (nacido en 1946), profesor en el Departamento de Ciencias de la Computación y Software Informático de la Universidad Concordia de Montreal, Canadá, dio la primera solución en 1975. El modelo está representado por la planta del museo, que es un polígono convexo o no convexo, cuyos bordes no se intersectan entre sí.

#### *3.2.6.1.1. Polígono convexo*

Un polígono convexo es un polígono en el que todos los ángulos interiores miden menos de 180 grados ó π radianes y todas sus diagonales son interiores. Cualquier recta que pase por un lado de un polígono convexo deja a todo el polígono completamente en uno delos semiplanos definidos por la recta. En un polígono convexo, todos los vértices "apuntan" hacia el exterior del polígono. Todos los triángulos son polígonos convexos. Todos los polígonos regulares son convexos. (academic)

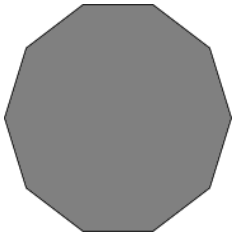

**ILUSTRACIÓN 5. POLÍGONO CONVEXO**

#### *3.2.6.1.2. Los polígonos cóncavos o no convexos*

Un polígono que no cumple las condiciones para ser clasificado como convexo se denomina polígono cóncavo. Ni todos sus ángulos son menores que 180°, ni todas sus diagonales son interiores.

Los polígonos estrellados son polígonos cóncavos.

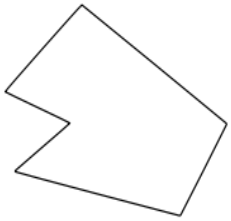

**ILUSTRACIÓN 6. POLÍGONO ESTRELLADO.**

Por supuesto que la sala del museo puede tener obstáculos. Para un verdadero museo. Los obstáculos son las columnas, muros que dividen la sala, y las exposiciones. Para nuestro problema, cada obstáculo se enfrentará como un “agujero” del polígono. Los lugares vigilados de la galería son trivialmente aquellos puntos de la galería que son visibles por una cámara, o vigilante, es decir, aquellos puntos del interior de la galería

poligonal que se pueden conectar mediante un segmento con el punto en el que está la vigilancia.

**Teorema**: Para vigilar una galería de arte poligonal de n vértices son suficientes n/3 cámaras (para ser exactos el número suficiente de cámaras es [n/3], el mayor entero que es menor o igual que n/3).

3.2.6.1.3. **Ejemplo 1:** Se analiza el siguiente polígono como referencia del laboratorio Alcalá 1 del Dpto. de Computación de la UNAN-León.

**ILUSTRACIÓN 7. POLÍGONO ASOCIADO AL LABORATORIO ALCALÁ 1**

Se define el número de lados.
El lugar de los puntos fue puesto a conveniencia, pero no afecta en nada en el procedimiento y el resultado de dicho ejercicio.


**ILUSTRACIÓN 8. UBICACIÓN DE LOS PUNTOS EN EL POLÍGONO LABORATORIO ALCALÁ 1**

N = 6
Numero de cámaras a instalar = 6/3
Numero de cámaras a instalar = 2.
*Si se aplica el teorema según el número de lados que en este caso serían 6, el total de cámaras que se deberían instalar son 2.*

**Ubicación de las cámaras.**

Primeramente, se triangula el polígono anterior, es decir, se divide el polígono en triángulos.

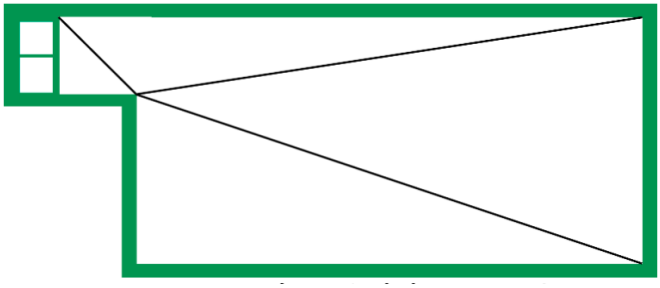

**ILUSTRACIÓN 9. TRIANGULACIÓN DEL POLÍGONO LABORATORIO ALCALÁ 1**

Basándose en una conveniencia, dirección y análisis de triangulación de visión de las cámaras, es posible proponer la siguiente ubicación para cumplir con la cantidad de cámaras arrojados por el teorema de la galería de arte.

A partir de los cálculos anteriores se puede determinar que las posibles ubicaciones donde colocar las cámaras son las siguientes.

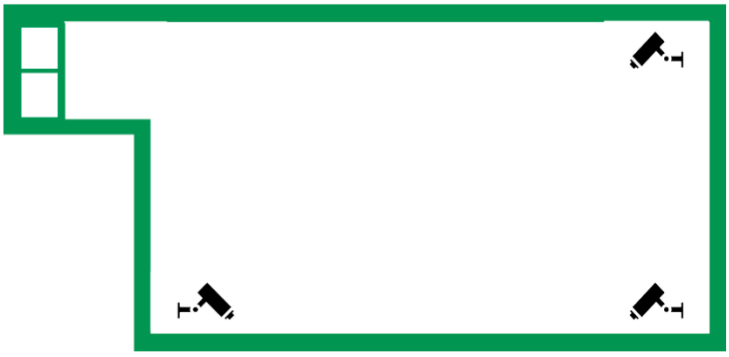

**ILUSTRACIÓN 10. POSIBLES UBICACIONES DE LAS CÁMARAS EN LABORATORIO ALCALÁ 1**

De las anteriores posiciones propuestas habría que elegir dos de ellas para ubicar las dos cámaras que definen le teorema.

3.2.6.1.4. **Ejemplo 2:** Se analiza el siguiente polígono como referencia del laboratorio Cisco del Dpto. de Computación de la UNAN-León.

ILUSTRACIÓN 11 - POLÍGONO ASOCIADO AL LABORATORIO DE CISCO

*Se define el número de lados como en ejemplo anterior.*
*El lugar de los puntos fue puesto a conveniencia, pero no afecta en nada en el procedimiento y el resultado de dicho ejercicio.*

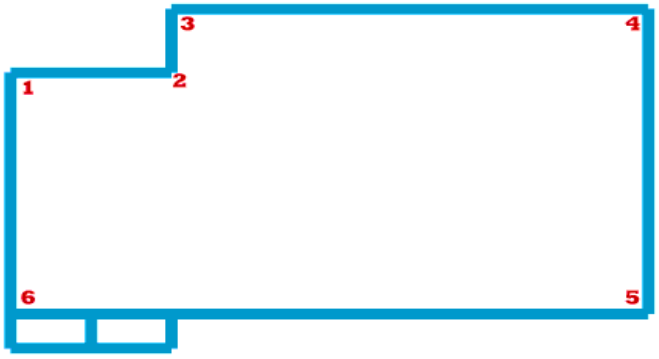


ILUSTRACIÓN 12 UBICACIÓN DE LOS PUNTOS EN EL POLÍGONO LABORATORIO DE CISCO

N = 6
Numero de cámaras a instalar = 6/3
Numero de cámaras a instalar = 2.
*Si se aplica el teorema según el número de lados que en este caso serían 6, el total de cámaras que se deberían instalar son 2.*

**Ubicación de las cámaras.**

Primeramente, se triangula el polígono anterior, es decir, se divide el polígono en triángulos.

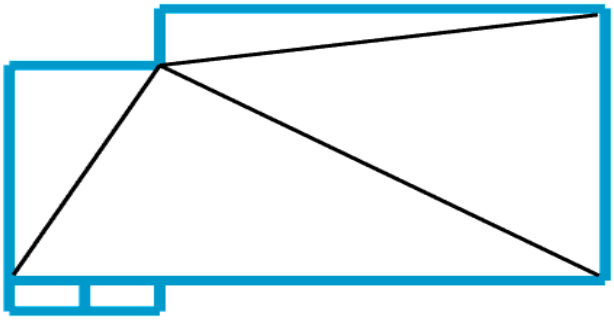

ILUSTRACIÓN 13 TRIANGULACIÓN DEL POLÍGONO CISCO

Basándose en una conveniencia, dirección y análisis de triangulación de visión de las cámaras, es posible proponer la siguiente ubicación para cumplir con la cantidad de cámaras arrojados por el teorema de la galería de arte.

A partir de los cálculos anteriores se puede determinar que las posibles ubicaciones donde colocar las cámaras son las siguientes.

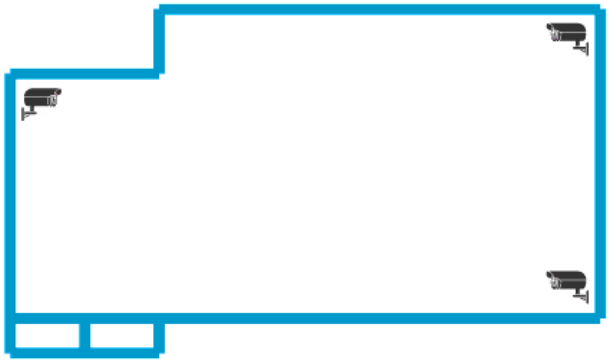

ILUSTRACIÓN 14 - POSIBLES UBICACIONES DE CÁMARAS EN LABORATORIO CISCO

De las anteriores posiciones propuestas habría que elegir dos de ellas para ubicar las dos cámaras que definen le teorema.

3.2.6.1.5. **Ejemplo 3:** Se analiza el siguiente polígono como referencia del laboratorio de hardware del Dpto. de Computación de la UNAN-León.

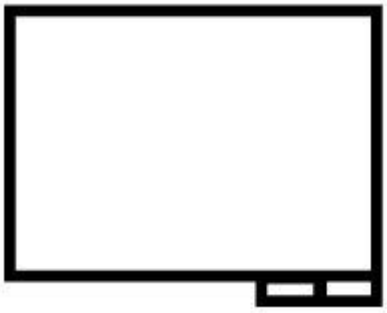

**ILUSTRACIÓN 15 - POLÍGONO ASOCIADO AL LABORATORIO DE HARDWARE**

Se define el número de lados como en ejemplo anterior. El lugar de los puntos fue puesto a conveniencia, pero no afecta en nada en el procedimiento y el resultado de dicho ejercicio


**ILUSTRACIÓN 16 - UBICACIÓN DE LOS PUNTOS EN EL POLÍGONO LABORATORIO DE HARDWARE**

N = 1
Numero de cámaras a instalar = 4/3
Numero de cámaras a instalar = 1.
*Si se aplica el teorema según el número de lados que en este caso serían 6, el total de cámaras que se deberían instalar son 1.*

**Ubicación de las cámaras.**

Primeramente, se triangula el polígono anterior, es decir, se divide el polígono en triángulos.

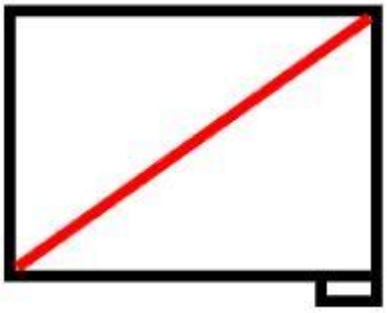

**ILUSTRACIÓN 17 - TRIANGULACIÓN DEL POLÍGONO DEL LABORATORIO DE HARDWARE**

Basándose en una conveniencia, dirección y análisis de triangulación de visión de las cámaras, es posible proponer la siguiente ubicación para cumplir con la cantidad de cámaras arrojados por el teorema de la galería de arte.

A partir de los cálculos anteriores se puede determinar que las posibles ubicaciones donde colocar las cámaras son las siguientes.

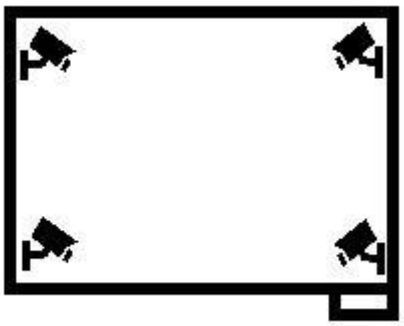

**ILUSTRACIÓN 18 - POSIBLES UBICACIONES DE CÁMARAS EN LABORATORIO DE HARDWARE**

De las anteriores posiciones propuestas habría que elegir una de ellas para ubicar la cámaras que definen le teorema. Pero el laboratorio cuenta con dos cámaras disponible así que pueden estar en calquiera de estas posiciones.

3.2.6.1.6. **Ejemplo 4:** Se analiza el siguiente polígono como referencia del laboratorio de hardware del Dpto. de Computación de la UNAN-León.

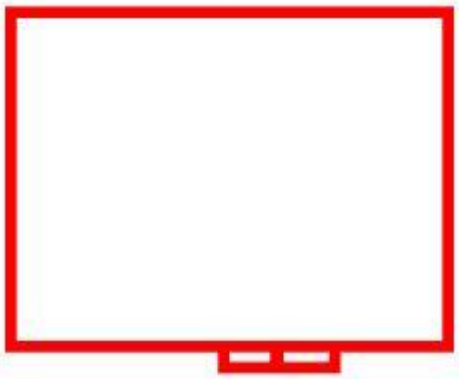

**ILUSTRACIÓN 19 - POLÍGONO ASOCIADO AL LABORATORIO DE ALCALÁ 2**

Se define el número de lados como en ejemplo anterior. El lugar de los puntos fue puesto a conveniencia, pero no afecta en nada en el procedimiento y el resultado de dicho ejercicio


**ILUSTRACIÓN 20 - UBICACIÓN DE LOS PUNTOS EN EL POLÍGONO LABORATORIO DE ALCALÁ 2**

N = 1
Numero de cámaras a instalar = 4/3
Numero de cámaras a instalar = 1.
*Si se aplica el teorema según el número de lados que en este caso serían 6, el total de cámaras que se deberían instalar son 1.*

**Ubicación de las cámaras.**

Primeramente, se triangula el polígono anterior, es decir, se divide el polígono en triángulos.

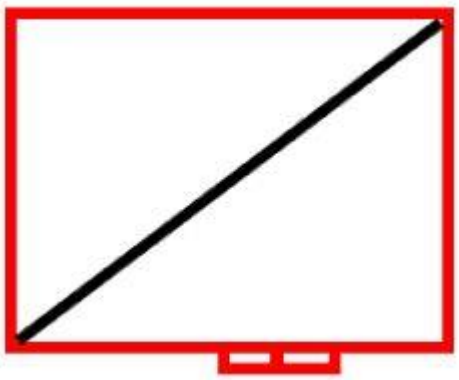

**ILUSTRACIÓN 21 - TRIANGULACIÓN DEL POLÍGONO ALCALÁ 2**

Basándose en una conveniencia, dirección y análisis de triangulación de visión de las cámaras, es posible proponer la siguiente ubicación para cumplir con la cantidad de cámaras arrojados por el teorema de la galería de arte.

A partir de los cálculos anteriores se puede determinar que las posibles ubicaciones donde colocar las cámaras son las siguientes.

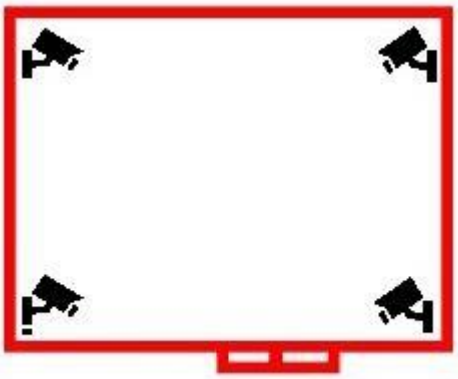

**ILUSTRACIÓN 22 - POSIBLES UBICACIONES DE CÁMARAS EN LABORATORIO DE ALCALÁ 2**

De las anteriores posiciones propuestas habría que elegir una de ellas para ubicar las cámaras que definen le teorema. Pero el laboratorio cuenta con dos cámaras disponible así que pueden estar en cualquiera de estas posiciones.

### 3.3. Almacenamiento de imágenes multimedia y uso de ancho de banda.

Las imágenes provenientes de las cámaras de vigilancia requieren gran almacenamiento en disco dependiendo del tiempo que se desea conservar, la resolución de las imágenes y el tipo de grabación. Y en caso de necesitar

almacenamiento adicional se tiene como solución el aumento, ya sea en el equipo de grabación o almacenamiento remoto. En el ancho de banda, los factores que influyen así como en el almacenamiento son: el número de cámaras, la resolución de imagen utilizada, el tipo y relación de compresión, frecuencias de imagen y complejidad de las escenas.

### *3.3.1. Comparación de estándares*

Al comparar los rendimientos de los estándares MPEG como el MPEG-4 y H.264, es importante tener en cuenta que los resultados pueden variar entre codificadores que usen el mismo estándar. Esto se debe a que el diseñador de un codificador puede elegir implementar diferentes conjuntos de herramientas definidas por un estándar. Siempre que los datos de salida de un codificador se ajusten al formato de un estándar, se pueden realizar implementaciones diferentes. De ahí que un estándar MPEG no pueda garantizar una frecuencia de bits o calidad determinadas, del mismo modo que no se puede realizar una comparación como es debido sin definir primero cómo se han implementado los estándares en un codificador. Un decodificador, a diferencia de un codificador, debe implementar todas las partes necesarias de un estándar para descodificar una transmisión de bits compatible. Un estándar especifica exactamente la forma en la que el algoritmo de descompresión debe restaurar cada bit de un vídeo comprimido. (Communication)

El gráfico siguiente compara la frecuencia de bits, partiendo de la misma calidad de imagen, entre los siguientes estándares de vídeo: Motion JPEG, MPEG-4 Parte 2 (sin compensación de movimiento), MPEG-4 Parte 2 (con compensación de movimiento) y H.264 (perfil de base).

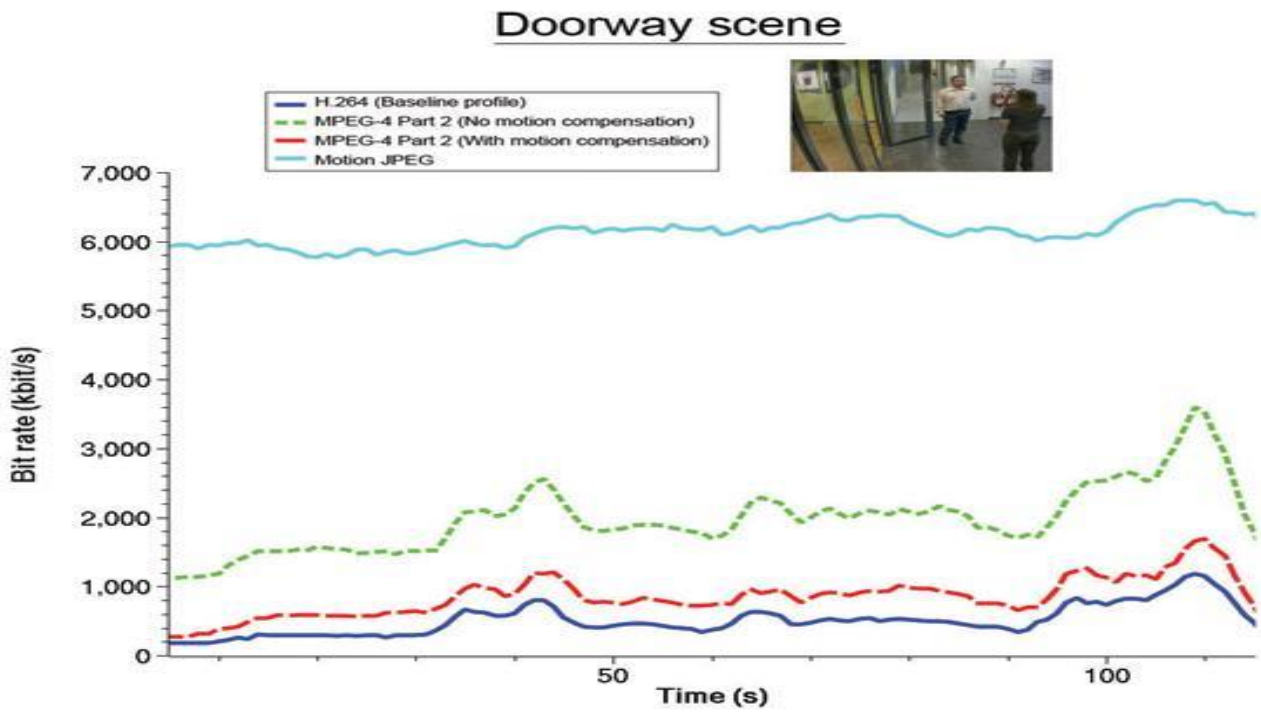


**ILUSTRACIÓN 23. COMPARATIVA ENTRE FRECUENCIA DE BITS Y ESTÁNDARES DE VÍDEO: MOTION JPEG, MPEG-4 PARTE 2 (CON Y SIN COMPENSACIÓN DE MOVIMIENTO) Y H.264**

### *3.3.2. Ancho de banda.*

El ancho de banda es la velocidad de transmisión simultánea que un medio de comunicación puede transmitir. (Implementación de un sistema de vigilancia y control de eventos con acceso a través de red, en el área de tesorería en la UNAN – Managua)

La siguiente ecuación, se emplea para calcular el consumo de ancho de banda:

$$\text{AB} = tamaño\ de\ la\ imagen \times FPS \times canales$$

Una cámara PAL en tiempo real (30 cuadros por segundo) a compresión normal y tamaño normal consume:

$$8\text{kb} \times 3\text{FPS} \times 1 = 240\text{kbps}$$

Como se puede observar en el resultado del ejemplo anterior, el ancho de banda requerido, después de la compresión de video hecha por la cámara, no es un valor muy elevado, por lo cual, se llevaría a cabo una buena transmisión y almacenamiento de video, sin interferir en el desempeño de otros equipos conectados a la misma red.

### *3.3.3. Espacio de almacenamiento.*

Primero se tiene que calcular el ancho de banda. Esto dará los (Bytes o Kbyte) por segundo. Ahora se debe multiplicar este valor por la cantidad de segundos que se desea almacenar.

Para determinar espacio de disco duro, se debe aplicar la siguiente ecuación:

$$\text{Espacio en disco duro} = \frac{(velocidad \times tiempo\ degrabación)}{8}$$

Dónde:
La velocidad se expresa en cuadros por segundo
Tiempo de grabación expresado en minutos

Se observa la importancia de determinar el mínimo necesario de cuadros por segundo a transmitir, el tamaño y nivel de compresión de la imagen, ya que se consumen demasiados recursos que pueden no ser necesarios en función del objetivo y área a cubrir por la cámara.

### *3.3.4. Resolución y métodos de compresión de video.*

Los parámetros resolución y métodos de compresión de video permiten obtener un nuevo parámetro llamado Tamaño del Cuadro, el cual es medido en Kilobytes.

En la tabla se indican los valores de tamaño del cuadro en función de la resolución y de la compresión MJPEG.

| Resolución | Compresión de video | | | | | | |
|---|---|---|---|---|---|---|---|
| | MJPEG-10 | MJPEG-20 | MJPEG-30 | MJPEG-40 | MJPEG-50 | MJPEG-70 | MJPEG-90 |
| 1280x1024 (1.3 MP) | 198 KB | 160 KB | 138 KB | 121 KB | 108 KB | 86 KB | 67 KB |
| 1600x1200 (2MP) | 290 KB | 235 KB | 202 KB | 178 KB | 158 KB | 125 KB | 97 KB |
| 1920x1080 (Full HD) | 314 KB | 253 KB | 218 KB | 192 KB | 171 KB | 135 KB | 105 KB |
| 2048x1536 (3 MP) | 476 KB | 384 KB | 331 KB | 291 KB | 259 KB | 203 KB | 160 KB |
| 2288x1712 (4 MP) | 592 KB | 479 KB | 412 KB | 363 KB | 323 KB | 256 KB | 199 KB |
| 2600X1950 (5 MP) | 767 KB | 619 KB | 533 KB | 470 KB | 418 KB | 331 KB | 257 KB |

**TABLA 1. TAMAÑO DEL CUADRO EN FUNCIÓN DE LA RESOLUCIÓN Y DE LA COMPRESIÓN**

| Resolución | Compresión de video | | | | | | |
|---|---|---|---|---|---|---|---|
| | MJPEG-10 | MJPEG-20 | MJPEG-30 | MJPEG-40 | MJPEG-50 | MJPEG-70 | MJPEG-90 |
| 320x240 (QVGA) | 12 KB | 9 KB | 8 KB | 7 KB | 6 KB | 5 KB | 4 KB |
| 352x240 (CIF NTSC) | 13 KB | 10 KB | 9 KB | 8 KB | 7 KB | 6 KB | 4 KB |
| 352x288 (CIF PAL) | 15 KB | 12 KB | 11 KB | 9 KB | 8 KB | 7 KB | 5 KB |
| 480X360 | 26 KB | 21 KB | 18 KB | 16 KB | 14 KB | 11 KB | 9 KB |
| 640X480 (VGA) | 46 KB | 38 KB | 32 KB | 28 KB | 25 KB | 20 KB | 16 KB |
| 704x240 (2CIF NTSC) | 26 KB | 21 KB | 18 KB | 16 KB | 14 KB | 11 KB | 9 KB |
| 704x288 (2CIF PAL) | 31 KB | 25 KB | 21 KB | 19 KB | 17 KB | 13 KB | 10 KB |
| 704x480 (4CIF NTSC) | 51 KB | 41 KB | 36 KB | 31 KB | 28 KB | 22 KB | 17 KB |
| 704x576 (4CIF PAL) | 61 KB | 50 KB | 43 KB | 38 KB | 33 KB | 26 KB | 21 KB |
| 800x600 (SVGA) | 73 KB | 59 KB | 50 KB | 44 KB | 40 KB | 31 KB | 24 KB |
| 1280x720 (HD) | 139 KB | 113 KB | 97 KB | 85 KB | 76 KB | 60 KB | 47 KB |
| 1280x960 (1.22 MP) | 186 KB | 150 KB | 129 KB | 114 KB | 101 KB | 80 KB | 62 KB |

**TABLA 2. TAMAÑO DEL CUADRO EN FUNCIÓN DE LA RESOLUCIÓN Y DE LA COMPRESIÓN MPEG4**

| Resolución | Compresión de video | | | | | |
|---|---|---|---|---|---|---|
| | MPEG4-10 | MPEG4-20 | MPEG4-30 | MPEG4-50 | MPEG4-70 | MPEG4-90 |
| 320x240 (QVGA) | 3 KB | 3 KB | 2 KB | 2 KB | 1 KB | 1 KB |
| 352x240 (CIF NTSC) | 4 KB | 3 KB | 2 KB | 2 KB | 1 KB | 1 KB |
| 352x288 (CIF PAL) | 4 KB | 3 KB | 3 KB | 2 KB | 1 KB | 1 KB |
| 480X360 | 7 KB | 6 KB | 5 KB | 3 KB | 3 KB | 2 KB |
| 640X480 (VGA) | 13 KB | 10 KB | 8 KB | 6 KB | 5 KB | 3 KB |
| 704x240 (2CIF NTSC) | 7 KB | 6 KB | 5 KB | 3 KB | 2 KB | 2 KB |
| 704x288 (2CIF PAL) | 9 KB | 7 KB | 6 KB | 4 KB | 3 KB | 2 KB |
| 704x480 (4CIF NTSC) | 14 KB | 11 KB | 9 KB | 7 KB | 5 KB | 4 KB |
| 704x576 (4CIF PAL) | 17 KB | 13 KB | 11 KB | 8 KB | 6 KB | 4 KB |
| 800x600 (SVGA) | 21 KB | 16 KB | 13 KB | 10 KB | 7 KB | 5 KB |
| 1280x720 (HD) | 40 KB | 31 KB | 25 KB | 18 KB | 14 KB | 10 KB |
| 1280x960 (1.22 MP) | 53 KB | 41 KB | 34 KB | 25 KB | 18 KB | 13 KB |

**TABLA 3. TAMAÑO DEL CUADRO EN FUNCIÓN DE LA RESOLUCIÓN Y DE LA COMPRESIÓN MPEG4**

| Resolución | Compresión de video | | | | | |
|---|---|---|---|---|---|---|
| | MPEG4-10 | MPEG4-20 | MPEG4-30 | MPEG4-50 | MPEG4-70 | MPEG4-90 |
| 1280x1024 (1.3 MP) | 56 KB | 44 KB | 30 KB | 20 KB | 19 KB | 14 KB |
| 1600x1200 (2MP) | 82 KB | 64 KB | 53 KB | 38 KB | 28 KB | 21 KB |
| 1920x1080 (Full HD) | 89 KB | 69 KB | 57 KB | 41 KB | 31 KB | 22 KB |
| 2048x1536 (3 MP) | 135 KB | 105 KB | 87 KB | 63 KB | 46 KB | 34 KB |
| 2288x1712 (4 MP) | 168 KB | 130 KB | 108 KB | 78 KB | 58 KB | 42 KB |
| 2600X1950 (5 MP) | 218 KB | 169 KB | 139 KB | 101 KB | 75 KB | 54 KB |

**TABLA 4. TAMAÑO DEL CUADRO EN FUNCIÓN DE LA RESOLUCIÓN Y DE LA COMPRESIÓN MPEG4**

| Resolución | Compresión de video | | | |
|---|---|---|---|---|
| | H264-10 | H264-20 | H264-30 | H264-50 |
| 320x240 (QVGA) | 1 KB | 1 KB | 1 KB | 1 KB |
| 352x240 (CIF NTSC) | 1 KB | 1 KB | 1 KB | 1 KB |
| 352x288 (CIF PAL) | 1 KB | 1 KB | 1 KB | 1 KB |
| 480X360 | 3 KB | 2 KB | 2 KB | 2 KB |
| 640X480 (VGA) | 5 KB | 4 KB | 3 KB | 3 KB |
| 704x240 (2CIF NTSC) | 3 KB | 2 KB | 2 KB | 2 KB |
| 704x288 (2CIF PAL) | 3 KB | 3 KB | 2 KB | 2 KB |
| 704x480 (4CIF NTSC) | 5 KB | 4 KB | 3 KB | 3 KB |
| 704x576 (4CIF PAL) | 6 KB | 5 KB | 4 KB | 4 KB |
| 800x600 (SVGA) | 8 KB | 6 KB | 5 KB | 5 KB |
| 1280x720 (HD) | 14 KB | 11 KB | 10 KB | 9 KB |
| 1280x960 (1.22 MP) | 19 KB | 15 KB | 13 KB | 12 KB |
| 1280x1024 (1.3 MP) | 20 KB | 16 KB | 14 KB | 13 KB |
| 1600x1200 (2MP) | 30 KB | 23 KB | 20 KB | 19 KB |
| 1920x1080 (Full HD) | 32 KB | 25 KB | 22 KB | 21 KB |
| 2048x1536 (3 MP) | 49 KB | 38 KB | 33 KB | 31 KB |
| 2288x1712 (4 MP) | 60 KB | 47 KB | 41 KB | 39 KB |
| 2600X1950 (5 MP) | 78 KB | 61 KB | 53 KB | 50 KB |

**TABLA 5. TAMAÑO DEL CUADRO EN FUNCIÓN DE LA RESOLUCIÓN Y DE LA COMPRESIÓN H264**


**ILUSTRACIÓN 24. CÁMARA HIKVISION DS-2CD2042WD-I**

Se escogió esta cámara IP por ser una de las más vendidas en el año 2017, según la empresa Axis Comunication. Dicha cámara presenta las siguientes características:

| | | |
|---|---|---|
| Vídeo | Compresión de vídeo: | H.264+ / H.264 / MJPEG. |
| | FPS: | Resolución máxima: 2688x1520p (4MP) |
| | Resolución: | 2688x1520@20IPS, 1920x1080@30IPS, 1280x720@30IPS |
| | Vídeo Bit Rate: | 32 Kbps - 16 Mbps. |

**TABLA 6. CARACTERÍSTICAS DE LA CÁMARA HIKVISION DS-2CD2042WD-I**

### *3.3.5. Calculo de ancho de banda y almacenamiento*

Para realizar un ejemplo de cálculo del ancho de banda, la cámara que se escogió tiene una resolución de hasta 268x1520 píxeles (4MP) a continuación se realizan los cálculos.

NOTA: Los parámetros resolución y compresión se seleccionaron arbitrariamente.

Cálculo con una mínima resolución 320x340 (QVGA) con uno de los métodos de compresión más usados el h.264 -50 (el cual la cámara de ejemplo lo soporta):

Tamaño de la imagen = 1 Kb
FPS = 26
Cantidad de canales = 6

AB = $tamaño\ dela\ imagen \times FPS \times canales$

$1\text{kb} \times 26\text{FPS} \times 6 = 208\text{kbps}$

**Almacenamiento**

Espacio en disco duro = $\frac{(velocidad \times tiempo\ degrabación)}{8}$

Almacenamiento =$\left(\frac{(208\ kbps \div 1000\ Mbps \times 604800\ s)}{8}\right) \div 1024 = 15.3Gb$

Nota: 604800 corresponde a la cantidad de segundos comprendidos en una semana.

Nota: AB = $208Kbps \div 1000Mbps$ se dividió en ancho de banda para convertir de Kbps a Mbps

Tiempo de grabación = 604800 segundos que hay en una semana
GB = dividir entre 1024 para convertir de mega a GB

3.3.5.1 Cálculo con una resolución media 800x600(SVGA) con uno de los métodos de compresión más usados el h.264 -20 (Soportado por la cámara de ejemplo).

Tamaño de la imagen = 8 Kb
FPS = 30
Cantidad de canales = 6

AB =$tamaño\ dela\ imagen \times FPS \times canales$

$8\text{kb} \times 30\text{FPS} \times 6 = 1440\text{kbps} \div 1000 = 1.44\text{Mpbs}$

**Almacenamiento**

Espacio en disco duro= $\frac{(velocidad \times tiempo\ degrabación)}{8}$

Almacenamiento = $\left(\frac{(1.44\ Mbps \times 604800\ s)}{8}\right) \div 1024 = 106.3Gb$

3.3.5.2 Calculo con una alta resolución 2048x1536(3MP) con uno de los métodos de compresión más usados el h.264 -10 (el cual la cámara de ejemplo la soporta).

Tamaño de la imagen = 49 Kb
FPS = 20
Cantidad de canales = 6

AB =$tamaño\ dela\ imagen \times FPS \times canales$

$$49\text{kb} \times 20\text{FPS} \times 6 = 5880\text{kbps} \div 1000 = 5.88\text{Mpbs}$$

**Almacenamiento**

Espacio en disco duro= $\frac{(velocidad \times tiempo\ degrabación)}{8}$

Almacenamiento = $\left(\frac{(5.88\ Mbps \times 604800\ s)}{8}\right) \div 1024 = 434.1Gb$

Resultados:

| Resolución | Tamaño de imagen | FPS | Cantidad de canales | AB | HDD |
|---|---|---|---|---|---|
| 320x340 (QVGA) | 1kb | 26 | 6 | 208kbps | 15.3 GB |
| 800x600 (SVGA) | 8kb | 30 | 6 | 1.44 Mbps | 106.3 GB |
| 2048x1536 (3MP) | 49kb | 20 | 6 | 5.88 Mbps | 434.1 GB |

**TABLA 7. RESULTADOS DEL CALCULO DE ALMACENAMIENTO Y ANCHO DE BANDA**

4. Sistemas de almacenamiento.

4.1. Almacenamiento en Volúmenes Lógicos.

La administración de volumen crea una capa de abstracción en el almacenaje físico, lo que permite crear volúmenes lógicos de almacenaje. Proporciona mucha más flexibilidad en una cantidad de formas que el uso directo de almacenaje físico. Con un volumen lógico no hay restricción física de espacio del disco. Además, la configuración de almacenaje del hardware se oculta del software permitiendo así redimensionar y desplazar sin tener que detener la aplicación o desmontar el sistema de archivos. (Landmann)

Los volúmenes lógicos proporcionan las siguientes ventajas sobre el uso directo de almacenamiento físico:

- Grupos de almacenaje dimensionables: Puede extender o reducir los volúmenes lógicos con comandos de software sencillos, sin necesidad de volver a dar

formato o crear particiones en los dispositivos de discos subyacentes.

- Asignación de datos en línea: Para implementar subsistemas de almacenamiento más modernos, más rápidos o resistentes, puede trasladar los datos mientras su sistema está activo. Los datos pueden ser reorganizados en discos mientras los discos están siendo utilizados.
- Volúmenes en espejos: Los volúmenes lógicos proporcionan una manera conveniente de configurar copias para sus datos.

#### *4.1.1. Ejemplo para la creación de un LVM.*

Este ejemplo crea un volumen lógico LVM llamado nuevo_volumen_logico que consta de discos en /dev/sda1, /dev/sdb1, y /dev/sdc1. Se deben etiquetar los discos como volúmenes físicos LVM para poder usarlos en un grupo de volúmenes.

# pvcreate /dev/sda1 /dev/sdb1 /dev/sdc1

Para crear el grupo de volúmenes se usa el siguiente comando que creara el grupo de volúmenes nuevo_grupo_volumen.

# vgcreate nuevo_grupo_volumen /dev/sda1 /dev/sdb1 /dev/sdc1

El siguiente comando crea el volumen lógico nuevo_volumen_logico desde el grupo de volúmenes nuevo_grupo_volumen. Este ejemplo crea un volumen lógico que utiliza 2GB del grupo de volúmenes.

# lvcreate -L2G -n /dev/nuevo_vol**u**men_logico nuevo_grupo_volumen

#### *4.1.2. Ejemplo de comandos ampliar un volumen lógico ya existente.*

En este paso se le indica al grupo de volúmenes nuevo_volumen_logico que se le agregará un nuevo volumen físico.

# vgextend /dev/nuevo_volumen_logico /dev/hdc1

El siguiente comando toma el volumen nuevo_volumen_logico ya existente y le agrega 0.95G de tamaño, tomados a partir de la integración del nuevo volumen físico.

# lvextend -L +0.95G /dev/ nuevo_volumen_logico

### 4.2. NAS y SAN

Cuando los requisitos de almacenamiento y gestión de datos superan los límites de un almacenamiento de conexión directa, un almacenamiento en red tipo NAS o una red de

área de almacenamiento (SAN) ofrecen la flexibilidad, las opciones de recuperación y el espacio necesario.

Un NAS es un único dispositivo de almacenamiento que se conecta directamente a una LAN y ofrece almacenamiento compartido a todos los clientes de la red. Un dispositivo NAS es fácil de instalar y de administrar, y se trata de una solución de almacenamiento de bajo coste. Sin embargo, su capacidad para la recepción de datos es limitada, ya que solo cuenta con una conexión de red, lo que puede suponer un problema en sistemas de alto rendimiento.

### *4.2.1. Almacenamiento redundante.*

Los sistemas SAN aportan redundancia al dispositivo de almacenamiento. En un sistema de almacenamiento, la redundancia permite guardar el vídeo, o cualquier otro dato, simultáneamente en más de un sitio. Esto abre la puerta a recuperar el vídeo si una parte del sistema de almacenamiento deja de ser legible por algún motivo.

Existen diferentes opciones para disponer de un nivel de almacenamiento extra en un sistema de vigilancia IP, como un sistema RAID (matriz redundante de discos independientes), la replicación de datos, los clústeres de servidores y el uso de distintos destinatarios del vídeo.

Las SAN son redes de alta velocidad destinadas específicamente a fines de almacenamiento, que suelen conectarse a uno o varios servidores a través de una conexión de fibra. Los usuarios pueden acceder a cualquiera de los dispositivos de almacenamiento de la SAN a través de los servidores, y la capacidad de almacenamiento puede llegar hasta varios cientos de terabytes. El almacenamiento centralizado reduce la parte de administración y ofrece un sistema flexible y de alto rendimiento ideal para entornos con varios servidores. La tecnología de canal de fibra se utiliza normalmente para conseguir transferencias de datos a cuatro gigabits por segundo y para almacenar grandes cantidades de datos con un alto nivel de redundancia.

## *4.3. Almacenamiento basado en el servido*

En función de la CPU del servidor de PC, la tarjeta de red y la RAM interna, un servidor puede gestionar un determinado número de cámaras, imágenes por segundo y tamaño de imágenes. La mayoría de los PC admiten entre dos y cuatro discos duros con una capacidad cada uno que puede llegar a aproximadamente 300 gigabytes (GB). En una instalación entre pequeña y media, el PC que ejecuta el software de gestión de vídeo también se utiliza para la grabación de vídeo. Esto se denomina almacenamiento directamente conectado.

## 5. Tipo de resoluciones

La resolución en un mundo digital o analógico es parecida, pero existen algunas diferencias importantes sobre su definición. En el video analógico, una imagen consta de líneas o líneas de TV, puesto que la tecnología de video deriva de la industria de la televisión. En un sistema digital, una imagen está formada por pixeles cuadrados. Las distintas resoluciones que puede proporcionar el video en red son: NTSC, PAL, VGA, megapíxel y HDTV. (rnds)

### 5.1. Resoluciones NTSC y PAL

Las resoluciones NTSC (National Television System Comité, Comité Nacional de Sistemas de Televisión) y PAL (Phase Alternating Line, Línea de Alternancia de Fase) son estándares de video analógico. Son relevantes para el video en red, ya que los codificadores de video proporcionan dichas resoluciones al digitalizar señales de cámaras analógicas. Las cámaras de red PTZ actuales y las cámaras domo de red PTZ también ofrecen resoluciones NTSC y PAL, puesto que en la actualidad utilizan un bloque (que incorpora la cámara, zoom, enfoque automático y funciones de iris automático) hecho para cámaras de video analógico, conjuntamente con una tabla de codificación de video integrada. En Norteamérica y Japón, el estándar NTSC es la norma de video analógico que predomina, mientras que en Europa y en muchos países de Asia y África se utiliza la norma PAL. Ambos estándares proceden de la industria de la televisión. El NTSC tiene una resolución de 480 líneas y utiliza una frecuencia de actualización de 60 campos entrelazados por segundo (o 30 imágenes completas por segundo). Para este estándar existe una nueva convención llamada 480i60 (donde “i” significa escaneado entrelazado), que define el número de líneas, el tipo de escaneado y la frecuencia de actualización. El PAL tiene una resolución de 576 líneas y utiliza una frecuencia de actualización de 50 campos entrelazados por segundo (o 25 imágenes completas por segundo). La nueva convención para este estándar es 576i50. La cantidad total de información por segundo es la misma en ambos estándares.

Cuando el vídeo analógico se digitaliza, la cantidad máxima de píxeles que pueden crearse se basará en el número de líneas de TV disponibles para ser digitalizadas. El tamaño máximo de una imagen digitalizada suele ser D1, y la resolución más común es 4CIF. Cuando se muestra en una pantalla de ordenador, el video analógico digitalizado puede mostrar efectos de entrelazado como el desgaste y las formas pueden aparecer ligeramente deformadas, ya que es posible que los píxeles generados no concuerden con los píxeles cuadrados de la pantalla. Los efectos de entrelazado se pueden reducir mediante técnicas de desentrelazado mientras que la relación de aspecto del video se corrige antes de visualizarlo para asegurarse, por ejemplo, de que un círculo de un video analógico siga siendo un círculo cuando se muestre en una pantalla de ordenador.

## 5.2. Resoluciones VGA

Con los sistemas 100% digitales basados en cámaras de red se pueden proporcionar resoluciones derivadas de las industrias informáticas y normalizadas en todo el mundo, de modo que la flexibilidad es mayor. Las limitaciones del NTSC y el PAL son insignificantes. VGA (Tabla de Gráficos de Video) es un sistema de pantalla de gráficos para PC desarrollado originalmente por IBM. Esta resolución es de 640 x 480 píxeles, un formato habitual en las cámaras de red que no disponen de mega píxeles.

La resolución VGA suele ser más adecuada para cámaras de red, ya que el video basado en VGA produce píxeles cuadrados que coinciden con los de las pantallas de ordenador.

Los monitores de ordenador manejan resoluciones en VGA o múltiplos de VGA.

## 5.3. Resoluciones megapíxel

Una cámara de red que ofrece una resolución mega píxel utiliza un sensor mega píxel para proporcionar una imagen que contiene un millón de mega píxeles o más. Cuántos más píxeles tenga el sensor, mayor potencial tendrá para captar más detalles y ofrecer una calidad de imagen mayor. Con las cámaras de red mega píxel los usuarios pueden obtener más detalles (ideal para la identificación de personas y objetos) o para visualizar un área mayor del escenario. Esta ventaja supone una importante consideración en aplicaciones de video vigilancia.

La resolución mega píxel es un área en la que las cámaras de red se distinguen de las analógicas. La resolución máxima que puede proporcionar una cámara analógica convencional tras haber digitalizado la señal de video en una grabadora o codificador de video es D1, es decir, 720x480 píxeles (NTSC) o 720x576 píxeles (PAL). La resolución D1 corresponde a un máximo de 414.720 píxeles o 0,4 mega píxeles. En comparación, un formato mega píxel común de 1280x1024 píxeles consigue una resolución de 1,3 mega píxeles. Esto es más del triple de la resolución que pueden proporcionar las cámaras analógicas de CCTV. También se encuentran disponibles cámaras de red con resoluciones de 2 mega píxeles y 3 mega píxeles e incluso se esperan resoluciones superiores en el futuro. La resolución mega píxel también consigue un mayor grado de flexibilidad, es decir, es capaz de proporcionar imágenes con distintas relaciones de aspecto (la relación de aspecto es la relación entre la anchura y la altura de una imagen). Una pantalla de televisión convencional muestra una imagen con una relación de aspecto de 4:3. Las cámaras de red con resolución mega píxel pueden ofrecer la misma relación, además de otras, como 16:99. La ventaja de la relación de aspecto 16:99 es que los detalles insignificantes, que suelen encontrarse en las partes superior e inferior de una imagen con un tamaño convencional, no aparecen y, por lo tanto, puede reducirse el ancho de banda y los requisitos de almacenamiento.

### 5.4. Resoluciones de televisión de alta definición (HDTV)

La HDTV proporciona una resolución hasta cinco veces más alta que la televisión analógica estándar. También ofrece una mejor fidelidad de color y un formato 16:99. Las dos normas HDTV más importantes, definidas por la SMPTE (Society of Motion Picture and Television Engineers, Sociedad de Ingenieros de Cine y Televisión), son la SMPTE 296M y la SMPTE 274M. La norma SMPTE 296M (HDTV 720P) define una resolución de 1280x720 píxeles con una alta fidelidad de color en formato 16:9 y utiliza el barrido progresivo a 25/330 hercios (Hz) (que corresponde a 25 o 30 imágenes por segundo, en función del país) y 50/60 Hz (50/60 imágenes por segundo).

La norma SMPTE 274M (HDTV 1080) define una resolución de 1920x1080 píxeles con una alta fidelidad de color en formato 16:9 y utiliza el barrido entrelazado o progresivo a 25/ 30 Hz y 50/60 Hz. El hecho de que una cámara cumpla con las normas SMPTE indica que cumple la calidad HDTV y debe proporcionar todas las ventajas de la HDTV en cuanto a resolución, fidelidad de color y frecuencia de imagen.

La norma HDTV se basa en píxeles cuadrados, similares a las pantallas de ordenador, de modo que el video HDTV de productos de video en red se puede visualizar tanto en pantallas HDTV como en monitores de ordenador estándares. Con el video HDTV de barrido progresivo no es necesario aplicar ninguna conversión o técnica de desentrelazado cuando se procesa el video con un ordenador o se muestra en un monitor.

## 6. Compresión de video

Las técnicas de compresión de video consisten en reducir y eliminar datos redundantes del video para que el archivo de video digital se pueda enviar a través de la red y almacenar en discos informáticos. Con técnicas de compresión eficaces se puede reducir considerablemente el tamaño del fichero sin que ello afecte muy poco, o en absoluto, la calidad de la imagen. Sin embargo, la calidad del video puede verse afectada si se reducen exceso el tamaño del fichero aumentando el nivel de compresión de la técnica que se utilice.

Hoy en día, la mayoría de proveedores de video en red utilizan técnicas de compresión estándar. Los estándares son importantes para asegurar la compatibilidad y la interoperabilidad. Tienen un papel especialmente relevante en la compresión de video, puesto que este se puede utilizar para varias finalidades y, en algunas aplicaciones de videovigilancia, debe poderse visualizar varios anos después de su grabación. Gracias al desarrollo de estándares, los usuarios finales tienen la opción de escoger entre diferentes proveedores, en lugar de optar a uno solo para su sistema de videovigilancia.

## 6.1. Códec de vídeo

En el proceso de compresión se aplica un algoritmo al video original para crear un archivo comprimido y ya listo para ser transmitido o guardado. Para reproducir el archivo comprimido, se aplica el algoritmo inverso y se crea un video que incluye prácticamente el mismo contenido que el video original. El tiempo que se tarda en comprimir, enviar, descomprimir y mostrar un archivo es lo que se denomina latencia. Cuanto más avanzado sea el algoritmo de compresión, mayor será la latencia.

## 6.2. Formatos de compresión

### *6.2.1. Motion JPEG*

Motion JPEG (MJPEG o M-JPEG) es un formato de compresión de video en el que cada cuadro de video o campo entrelazado de una secuencia de video digital (incluidos video y metadatos como subtítulos y subtítulos) se comprime por separado como una imagen JPEG. Originalmente desarrollado para aplicaciones de PC multimedia, ahora MJPEG es utilizado por dispositivos de captura de video tales como cámaras digitales, cámaras IP, cámaras web y sistemas de edición de video no lineales.

MJPEG es un esquema de compresión de solo intratrama. Debido a que los marcos se comprimen independientemente el uno del otro, MJPEG impone requisitos de procesamiento y memoria más bajos en los dispositivos de hardware. Como tal, la calidad de imagen de MJPEG es directamente una función de la complejidad espacial de cada cuadro de video. Los marcos con grandes transiciones suaves o superficies monótonas se comprimen bien y es más probable que mantengan sus detalles originales con pocos artefactos de compresión visibles. Los marcos que exhiben texturas complejas, curvas finas y líneas son propensos a exhibir artefactos DCT tales como timbre, borrones y macrobloques. Esto le da a MJPEG una ventaja sobre los esquemas de compresión entre cuadros, que no admiten movimientos rápidos entre cuadros y requieren más hardware para cumplir con las demandas de memoria de la compresión entre cuadros.

Muchas cámaras habilitadas para red proporcionan transmisiones MJPEG a las que los clientes de red se pueden conectar. Los navegadores basados en Mozilla y Webkit tienen soporte nativo para ver las transmisiones MJPEG. Algunas cámaras habilitadas para red proporcionan sus propias interfaces MJPEG como parte del conjunto de funciones normales. Para las cámaras que no proporcionan esta función de forma nativa, se puede usar un servidor para transcodificar las imágenes de la cámara en una secuencia MJPEG y luego proporcionar esa transmisión a otros clientes de la red.

### *6.2.2. MPEG-4*

MPEG-4 es un estándar ISO / IEC desarrollado por MPEG (Moving Picture Experts Group) para la creación, entrega y reproducción multimedia interactivas para Internet.

MPEG-4 no solo se puede usar para televisión digital, sino también para aplicaciones multimedia interactivas y gráficos interactivos. Para hacerlo, MPEG-4 no solo puede comprimir video y audio, sino que también puede manejar texto, imágenes, animaciones, objetos 2D y 3D. Todos estos elementos se pueden utilizar para crear presentaciones multimedia interactivas que se pueden adaptar para ser transportadas a través de redes de ancho de banda bajo, así como redes de transmisión de banda ancha de alta definición. (telecomabc)

MPEG-4 se basa en diferentes objetos que pueden codificarse y transmitirse por separado. Los objetos se usan para construir la escena después de decodificar. Para construir las composiciones, MPEG-4 incluye un lenguaje de descripción de escena, llamado BiFS, formato binario para escenas. Las escenas pueden comprender interactividad. Diferentes objetos pueden aparecer, desaparecer o, p. cambia su color según la entrada del usuario. Los objetos pueden ser sobre cualquier cosa, por ejemplo, video, texto, gráficos, objetos 2D, objetos 3D, audio, voz. Todos los objetos están codificados con su propio esquema de codificación óptimo. El video, el audio y otros objetos pueden estar estrechamente sincronizados.

### *6.2.3. H.264 o MPEG-4 Part 10/AVC*

El estándar de codificación avanzada de video H.264 / MPEG-4 (H.264 / AVC) es el estándar de codificación de video más reciente desarrollado conjuntamente por el Grupo de expertos en codificación de video ITU-T (VCEG) y el Grupo de expertos en imagen en movimiento ISO / IEC (MPEG ) H.264 / AVC ha logrado una mejora significativa en el rendimiento de compresión en comparación con los estándares anteriores, y proporciona una representación del video que es compatible con la red y que aborda aplicaciones conversacionales (video telefonía) y no conversacionales (almacenamiento, transmisión o transmisión). Este artículo proporciona una descripción de la estructura, tecnología, rendimiento y recursos de H.264 / AVC, que se conoce formalmente como la Recomendación UIT-T H.264 e ISO / CEI 14496-10 (MPEG-4 Parte 10). El estándar de codificación avanzada de video H.264 / MPEG-4 (H.264 / AVC) es el estándar de codificación de video más reciente desarrollado conjuntamente por el Grupo de expertos en codificación de video ITU-T (VCEG) y el Grupo de expertos en imagen en movimiento ISO / IEC (MPEG ) H.264 / AVC ha logrado una mejora significativa en el rendimiento de compresión en comparación con los estándares anteriores, y proporciona una representación del video que es compatible con la red y que aborda aplicaciones conversacionales (video telefonía) y no conversacionales (almacenamiento, transmisión o transmisión). (Thomas Weigand)

Las aplicaciones previstas para el estándar H.264 / AVC incluyen difusión por cable, satélite, cable módem, x (de cualquier tipo) línea digital de abonado (xDSL) y canales terrestres; almacenamiento interactivo o en serie en dispositivos ópticos y magnéticos como DVD; almacenamiento y distribución de películas profesionales y material de video para la contribución de contenido, distribución de contenido, edición de estudio y procesamiento posterior; servicios de transmisión de video a pedido o multimedia a través de cablemódem, xDSL, red de área local (LAN), red digital de servicio integrado

(ISDN) y redes inalámbricas; servicios de conversación a través de Ethernet, LAN, xDSL, ISDN, redes inalámbricas y móviles y módems; y servicios de mensajería multimedia a través de redes xDSL, Ethernet, LAN, ISDN, inalámbricas y móviles. Con una cobertura de aplicaciones tan amplia, H.264 / AVC recibió rápidamente una gran atención reciente de la industria y encontró una amplia adopción del sistema estándar, así como la implementación en productos.

## 7. Tecnologías de red

Se utilizan diversas tecnologías de red para proporcionar las numerosas ventajas de un sistema de video en red. Este capítulo empieza con unos apartados dedicados a la red de área local, concretamente a las redes Ethernet y sus componentes compatibles con los sistemas de video en red.

### 7.1. Redes Ethernet

Ethernet es la tecnología de acceso al medio más popular, es escalable, económica y fácilmente integrable a nuevas aplicaciones, se pueden obtener arquitecturas de la de alta velocidad de gigabit sobre cobre y la resolución de fallos suele ser simple y rápido. Ethernet opera sobre la capa de enlace de datos y física del modelo OSI. (Ariganello)

Ethernet fue creada en colaboración de Intel, Digital y Xerox originalmente se implementó como Ethernet 802.3, half-duplex, limitada al transporte de datos por un par de cobre a la vez (recibe por un par y transmite por otro, pero no al mismo tiempo). Posteriormente, la tecnología Ethernet full-duplex permitió recibir y enviar datos al mismo tiempo libre de colisiones.

#### *7.1.1. Alimentación a través de Ethernet*

La alimentación a través de Ethernet *(Power over Ethernet, PoE)* es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre a un dispositivo de red (switch, punto de acceso, router, teléfono o cámara IP, etc) usando el mismo cable que se utiliza para la conexión de red. Elimina la necesidad de utilizar tomas de corriente en las ubicaciones del dispositivo alimentado y permite una aplicación más sencilla de los sistemas de alimentación ininterrumpida (SAI) para garantizar un funcionamiento las 24 horas del día, 7 días a la semana.

Power over Ethernet se regula en una norma denominada IEEE 802.3af, y está diseñado de manera que no haga disminuir el rendimiento de comunicación de los datos en la red o reducir el alcance de la red. La corriente suministrada a través de la infraestructura LAN se activa de forma automática cuando se identifica un terminal compatible y se bloquea ante dispositivos preexistentes que no sean compatibles. Esta característica permite a los usuarios mezclar en la red con total libertad y seguridad dispositivos preexistentes con dispositivos compatibles con PoE. (tecnoseguro)

### 7.1.2. PoE Plus

En septiembre de 2005, el IEEE estableció el comité 802.3at para producir un estándar para una mayor potencia sobre Ethernet. Inicialmente esto fue designado como PoE Plus y este se regula en una norma denominada IEEE 802.3at. (rhyshaden)

Se requiere compatibilidad con 802.3af por lo que hay un modo de baja potencia para las PD heredadas. Existe un límite en la cantidad de energía que se puede extraer a través de los cables 24AWG antes de que se produzca un daño eléctrico debido al sobrecalentamiento dentro de los conectores y paquetes de cables, además de problemas de interferencia de señales. Esto significa que es posible que se necesiten múltiples pares para suministrar energía. Por el momento, 802.3at limita el número de pares que pueden llevar potencia a dos. Actualmente, se está considerando un límite actual de 720mA que permite 29.5W por par, sin embargo, el Draft 3.0 de 802.3at está buscando reducir esto a 600mA dando 25W por par, o 50W por dispositivo. 802.3at también están buscando cables de Categoría 5 y superiores para arreglar la especificación y no tener que preocuparse por admitir el cableado de Categoría 3.

## 7.2. Seguridad de red

Una de las configuraciones habituales de los sistemas de videovigilancia IP es la de permitir que únicamente la dirección IP del servidor que hospeda el software de gestión de video pueda acceder a los productos de video en red.

### *7.2.1. Filtro de direcciones IP*

Los filtros IP evitan o permiten el uso de direcciones IP, protocolos IP y puertos TCP/UDP a través de los puertos Ethernet y radio del punto de acceso. Es posible crear un filtro que pase tráfico a todas las direcciones excepto las especificadas o crear un filtro que bloquee el tráfico a todas las direcciones excepto las especificadas. Se pueden crear filtros que contengan elementos de uno, dos o los tres métodos de filtrado IP. Además, puede aplicar los filtros creados tanto a puertos Ethernet o de radio como a ambos, y tanto para paquetes entrantes y salientes como para ambos. (cisco)

### *7.2.2. Firewall*

Es un dispositivo de seguridad de red que supervisa el tráfico de red entrante y saliente y decide si permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad. Los cortafuegos han sido una primera línea de defensa en seguridad de red durante más de 25 años. Establecen una barrera entre redes internas seguras y controladas que pueden ser confiables y no confiables fuera de las redes, como Internet. Un firewall puede ser hardware, software o ambos. (cisco)

### *7.2.3. IPtables.*

El firewall utilizado para gestionar las conexiones entrantes y salientes en GNU/Linux es IPtables. Las posibilidades de IPtables son prácticamente infinitas con un administrador que quiera sacarle el máximo provecho, puede realizar configuraciones extremadamente complejas. Para simplificar, IPtables permite crear reglas que analizarán los paquetes de datos que entran, salen o pasan por el ordenador, y en función de las condiciones que se indiquen, se tomará una decisión que normalmente será permitir o denegar que dicho paquete siga su curso. (ITE)

### *7.2.4. Secure Shell (SSH)*

Es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encriptada la sesión de conexión, haciendo muy difícil que alguien pueda obtener contraseñas no encriptadas.

SSH está diseñado para reemplazar los métodos más viejos y menos seguros para registrarse remotamente en otro sistema a través de la shell de comando, tales como telnet o rsh. Un programa relacionado, el scp, reemplaza otros programas diseñados para copiar archivos entre hosts como rcp. Ya que estas aplicaciones antiguas no encriptan contraseñas entre el cliente y el servidor, por tanto, de debe evitar usarlas mientras sea posible. El uso de métodos seguros para registrarse remotamente a otros sistemas reduce los riesgos de seguridad tanto para el sistema cliente como para el sistema remoto.

Características de SSH:

- Después de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor al que se conectó anteriormente.
- El cliente envía su información de autentificación y la transferencia de datos al servidor usando una encriptación robusta de 128 bits.
- Ya que el protocolo SSH encripta todo lo que envía y recibe, se puede usar para asegurar protocolos inseguros. El servidor SSH puede convertirse en un conducto para convertir en seguros los protocolos inseguros mediante el uso de una técnica llamada reenvío de puertos, como por ejemplo POP, incrementando la seguridad del sistema en general y de los datos.

Si se utiliza SSH para inicios de sesión de shell remota y para copiar archivos, se pueden disminuir las amenazas a la seguridad notablemente. Esto es porque el cliente SSH y el servidor usan firmas digitales para verificar su identidad. Adicionalmente, toda la comunicación entre los sistemas cliente y servidor es encriptada. No servirán de nada los intentos de falsificar la identidad de cualquiera de los dos lados de la comunicación ya que cada paquete está cifrado por medio de una llave conocida sólo por el sistema local y el remoto. (mit)

### *7.2.5. VPN (Red privada virtual)*

Una red privada virtual (VPN) es la extensión de una red privada que abarca enlaces a través de redes públicas o compartidas como Internet. Una VPN le permite enviar datos entre dos computadoras a través de una red compartida o pública de una manera que emule las propiedades de un enlace privado punto a punto. El acto de configurar y crear una red privada virtual se conoce como red privada virtual.

Para emular un enlace punto a punto, los datos se encapsulan, o envuelven, con un encabezado que proporciona información de enrutamiento que le permite atravesar la red de tránsito público o compartido para llegar a su punto final. Para emular un enlace privado, los datos que se envían se encriptan por confidencialidad. Los paquetes que se interceptan en la red compartida o pública son indescifrables sin las claves de cifrado. La parte de la conexión en la que se encapsulan los datos privados se conoce como túnel. La parte de la conexión en la que se cifran los datos privados se conoce como conexión de red privada virtual (VPN).

Las conexiones VPN permiten a los usuarios que trabajan en el hogar o en la carretera conectarse de manera segura a un servidor corporativo remoto utilizando la infraestructura de enrutamiento proporcionada por una red pública (como Internet). Desde la perspectiva del usuario, la conexión VPN es una conexión punto a punto entre la computadora del usuario y un servidor corporativo. La naturaleza de la interred intermedia es irrelevante para el usuario porque parece que los datos se envían a través de un enlace privado dedicado. (microsoft)

## 8. Sistemas de gestión de vídeo

Un aspecto importante del sistema de videovigilancia IP es la gestión de video para la visualización, grabación, reproducción y almacenamiento en directo. Si el sistema está formado por una sola cámara o por pocas cámaras, la visualización y la grabación básica de video se pueden gestionar mediante la interfaz Web incorporada de las cámaras de red y los codificadores de video. Cuando el sistema consta de más cámaras, se recomienda utilizar un sistema de gestión de video en red.

Actualmente, existen cientos de sistemas de gestión de video diferentes, cubriendo diferentes sistemas operativos, segmentos de mercado e idiomas. Los aspectos que deben considerarse son la elección de plataforma de hardware, plataforma de software, características del sistema, que incluyen la instalación y configuración, gestión de eventos, video inteligente, administración y seguridad; y posibilidades de integración con otros sistemas.

### 8.1. Plataformas de hardware

Existen dos tipos diferentes de plataformas de hardware para un sistema de gestión de video en red: una plataforma de servidor de PC formada por uno o más PC que ejecuta

un programa de software de gestión de video y uno basado en una grabadora de video en red (NVR) que es un hardware patentado con software de gestión de video preinstalado.

### 8.2. Plataforma de servidor de PC

Una solución de gestión de video basada en una plataforma de servidor de PC incluye servidores de PC y equipos de almacenamiento que se pueden seleccionar directamente con el fin de obtener un rendimiento superior para el diseño específico del sistema. Una plataforma abierta de estas características facilita la opción de añadir funcionalidades al sistema, como un almacenamiento incrementado o externo, cortafuegos, protección contra virus y algoritmos de video inteligentes, en paralelo con un programa de software de gestión de video. Una plataforma de servidor de PC también se puede ampliar, permitiendo añadir cuantos productos de video en red sean necesarios. El hardware del sistema se puede ampliar o actualizar para satisfacer nuevas necesidades de rendimiento.

### 8.3. Plataforma NVR

Un grabador de vídeo en red se presenta como una caja de hardware con funcionalidades de gestión de vídeo preinstaladas. En este sentido, un NVR es parecido a un DVR. (Algunos DVR, también llamados DVR híbridos, también incluyen una función NVR, es decir, la capacidad también de grabar vídeo basado en red.)

Un hardware de NVR normalmente está patentado y diseñado específicamente para gestión de vídeo. Está dedicado a sus tareas específicas de grabación, análisis y reproducción de vídeo en red y normalmente no permite que ninguna otra aplicación se conecte a éste. El sistema operativo puede ser Windows, UNIX/Linux o patentado.

Un NVR está diseñado para ofrecer un rendimiento óptimo para un conjunto de cámaras y normalmente es menos escalable que un sistema basado en servidor de PC. Esto permite que la unidad resulte más adecuada para sistemas más pequeños donde el número de cámaras se encuentra dentro de los límites de la capacidad de diseño de un NVR. Normalmente, un NVR es más fácil de instalar que un sistema basado en una plataforma de servidor de PC. (axis)

### 8.4. Plataformas de software

Se pueden utilizar plataformas de software diferentes para gestionar video. Implican el uso de interfaz Web incorporada, existente en muchos productos de video en red, o el uso de un programa de software de gestión de video independiente que es una interfaz basada en Windows o en Web.

### *8.4.1. Software basado en cliente de Windows*

Cuando se llega a programas de software independientes para gestión de video, los programas basados en cliente de Windows son los más populares. Los programas de software basados en Web también están disponibles.

Con un programa basado en cliente de Windows, primero se debe instalar el software de gestión de video en el servidor de grabación. Después, se puede instalar un programa de software de cliente de visualización en el mismo servidor de grabación o en cualquier PC, ya sea localmente en la misma red donde se encuentra el servidor de grabación o remotamente en una estación de visualización ubicada en una red independiente. En algunos casos, la aplicación cliente también permite a los usuarios cambiar entre diferentes servidores que tengan el software de gestión de video instalado y, de este modo, hacer posible la gestión de video en un sistema grande o en muchos sitios remotos.

### *8.4.2. Software basado en Web*

Primero se debe instalar un programa de software de gestión de video basado en Web en un servidor de PC que sirva tanto de servidor Web como de grabación. Esto permite a los usuarios de cualquier parte de la red y con cualquier tipo de ordenador conectado a la red pueda acceder al servidor de gestión de video y, así, a los productos de video en red que gestiona, simplemente utilizando un navegador Web.

#### 8.4.2.1. Zoneminder

Es una alternativa de código abierto a las aplicaciones de monitorización de cámaras que está a la altura de cualquier otro software de video vigilancia profesional que permite a los usuarios controlar sus cámaras de forma totalmente gratuita a través de una interfaz web intuitiva. Proporciona una solución integral de video vigilancia, permitiendo capturar, analizar, grabar y monitorizar desde cualquier tipo de cámara: CCTV, cámaras IP o webcams.

Con ZoneMinder se puede programar horarios de funcionamiento de las cámaras y su modo de actuación (grabación continua de vídeo o fotografías en secuencia) , para cada cámara se puede definir una zona de exclusión sobre la que si se detectase alguna alteración en la imagen capturada, el sistema generaría una alarma , ya sea a través de un correo electrónico o con una llamada VoIP utilizando un servidor como Asterisk, el tratamiento de la alarma es configurable, por ejemplo, fuera de horario de oficina. (linux-party)

#### 8.4.2.2. Kmotion

Motion es una aplicación por línea de comandos que crea un servidor web con flujo de vídeo en streaming obteniendo la señal tanto de una cámara local, de USB por ejemplo,

como de una cámara de red. Incluso se puede controlar la cámara de red si tiene esta opción (zoom, movimiento, etc..) y está dentro del catálogo de drivers con los que trabaja la aplicación. Todas las opciones como calidad de capturas, FPS, detección de movimiento (eventos), lanzamiento de scripts al inicio y final de los eventos, velocidad de capturas en función de si se detecta movimiento o no, etc. se configuran mediante archivos de configuración. (kmotion)

El proyecto Kmotion ofrece un front-end para Motion que le da mucha más eficacia y espectacularidad. Con él es posible configurar más cómodamente casi todo y se ejecuta sobre un servidor apache. Además, crea una base de datos de eventos grabados teniendo acceso a ellos para ir directamente a ver lo que más nos interesa.

#### 8.4.2.3. iSpy

Es un software de código abierto para las aplicaciones de monitorización de cámaras de seguridad web que está a la altura de cualquier otro software de videovigilancia profesional. (dosbit)

iSpy permite a los usuarios controlar sus cámaras de seguridad de forma totalmente gratuita mediante una interfaz intuitiva. Con iSpy es posible**:** escuchar y grabar micrófonos remotos en tiempo real; vincular cámaras y micrófonos para grabar audio y vídeo de manera sincronizada; monitorizar el número de cámaras que se desee; detectar, grabar y seguir el movimiento; grabar vídeo y audio a demanda programando horarios; detectar la presencia de merodeadores; sistema de detección facial con reconocimiento; detección y grabación automática del audio**;** grabar automáticamente a un servidor FTP; reconocimiento de objetos comunes como matrículas; y otras muchas funciones.

Con iSpy se pueden programar y ejecutar prácticamente las mismas funciones que con un programa de videovigilancia de pago, pero se trata de una alternativa muy interesante porque es mucho más económica.

iSpy es un software de código abierto válido tanto para usuarios domésticos que únicamente necesiten una o pocas cámaras de vigilancia como para negocios que necesiten un sistema de vigilancia a pequeña escala para ser controlado localmente. Se trata de un programa informático totalmente gratuito que se puede descargar sin coste alguno desde su página web.

# Diseño metodológico

## 1. Tipo de Investigación

El presente trabajo se trata de una investigación centrada en encontrar mecanismos o estrategias que permitan alcanzar con los objetivos propuesto, por tal razón el tipo de investigación es: Investigación aplicada.

## 2. Etapas de la investigación

### 2.1. Etapa I. Recopilación de datos.

En esta etapa se realizó una investigación acerca de los distintos sistemas de video vigilancia IP, tecnologías y herramientas vinculadas con el fin de recolectar información necesaria para la implementación de este. Adicionalmente se recopiló información sobre el sistema de vídeo vigilancia IP instalado, para esto se efectuó una entrevista al encargado del mantenimiento y gestión de dicho sistema, donde deja claro que este sistema no está en funcionamiento por daños de hardware en el servidor, además brindó información sobre las cámaras IP y acerca del equipo servidor.

### 2.2. Etapa II. Selección de herramientas.

Luego de haber realizado un análisis de las tecnologías y herramientas disponibles e investigadas, se ha encontrado ventajas en cada una de ellas. Sin embargo, fue necesario realizar una evaluación de algunos aspectos y requerimientos que se deben tomar en cuenta para la elección de las herramientas que mejor se adecúen a las necesidades del sistema.

**Sistema de gestión de video:** Mediante la comparación de las característica entre los diversos software de video vigilancia IP y pruebas de estos en un sistema virtualizado, se determinó que la mejor opción es zoneminder, el cual permite el uso de distintas formas para monitorizar y grabación de video, sobre todo por que cubre gran parte de las necesidades del nuevo sistema.

**Acceso remoto:** Para facilitar el acceso remoto con interfaz gráfica se seleccionó un software llamado Anydesktop, el cual está basado de un servidor

VNC este es un software sencillo que es capaz de alcanzar con las expectativas de cualquier administrador de sistemas informáticos y para el acceso remoto a través de un terminal la mejor opción es hacer uso de SSH que gracias a si seguridad en la transmisión de datos da confianza para la implementación de este.

**Seguridad Informática:** Se implementaron distintos mecanismo de seguridad para proteger la información almacenada en el servidor. Para evitar la efectividad en ataques de inicio de sesión con fuerza bruta mediante el uso de bots o software automatizados se habilito Google reCaptcha. Al activar el módulo SSL y generar certificados para el servidor apache2 permite que la información que se intercambia entre el cliente y el servidor vaya cifrada, de esta forma, los datos son ilegible ante la captura de tráfico de red con programas como wireshark. Alejarse del equipo servidor sin bloquear el acceso al sistema de monitoreo zoneminder es dejar una puerta abierta a cualquiera que desee ver o alterar el entorno de trabajo de este, limitar el tiempo de caducidad de la sesión activa es una de las medidas más eficaces que se pudo implementar. Se configuró un firewall con IPtables para el cierre de puertos que no fueron utilizados.

**Sistema de almacenamiento:** El Dpto. de computación de la UNAN-León brindo dos unidades de discos duros de 500 Gb c/u dedicados al uso de almacenamiento en el servidor, la primara tarea a realizar fue unificar las dos unidades para crear un volumen lógico de 1000 Gb luego de esto se procedió a crear dos particiones, uno de 80 Gb para el sistema operativo y 920 Gb para el alojamiento de las grabaciones de las cámaras, estas tareas se realizaron haciendo uso de LVM (Logical volumen manager), una de las principales razones por la que se eligió esta tecnología es que permite expandir, disminuir, agregar o quitar unidades de disco duro si necesidad de apagar el equipo servidor.

**Equipo servidor:** Debido a que el antiguo servidor estaba en mal estado se realizaron las solicitudes necesarias, dirigidas a la autoridades del Dpto. de computación, para la adquisición de un nuevo equipo servidor destinado al alojamiento tanto del sistemas de gestión de vídeo como las grabaciones obtenidas por las cámaras. Luego se procedió a realizar pruebas en el servidor con el fin de garantizar el buen funcionamiento de este y la correcta monitorización de los videos obtenidos atreves de las cámaras IP.

## 2.3. Etapa III. Trabajo final.

En esta etapa se realizó la elaboración y prueba de las mejoras tanto software como hardware para la reinstalación del sistema de video vigilancia delos laboratorios y la redacción del informe final junto con la elaboración de la presentación del presente trabajo.

**Hardware**: se proporcionó un servidor con dos discos duros de 500GB cada uno el cual fue un aumento de espacio con respecto al antiguo servidor.

**Software**: primeramente, se instaló el sistema operativo debían más específicamente la versión 9.1, después un servidor web el cual se utilizó apache donde se instaló el software web libre zoneminder para el monitoreo de las cámaras IP de los laboratorios.

Seguido de la instalación del zoneminder se realizaron las configuraciones referentes a mejoras aplicadas en el sistema cada una de estas configuraciones las explicaremos en el siguiente acápite:

### *2.3.1. Desarrollo.*

**Inicio de sesión con SSL.**

Las siglas SSL responden a los términos en inglés (Secure Socket Layer), el cual es un protocolo de seguridad que hace que sus datos viajen de manera íntegra y segura, es decir, la transmisión de los datos entre un servidor y usuario web, y en retroalimentación, es totalmente cifrada o encriptado.

Se utilizaron certificados autogenerados SSL para mejorar la seguridad de los datos intercambiados entre el cliente y el servidor web apache2. Creando los certificados en open SSL para después agregarlos al servidor. Para ello se elaboró un video guía que describe el mecanismo utilizado para la implementación de inicio de sesión con SSL dentro del presente trabajo monográfico, el video puede ser consultado en: https://www.youtube.com/watch?v=j5jUlSApOZc

**Gestión de datos mediante LVM.**

En esta sección se creó un volumen lógico con un sistema de archivos Ext4 para guardar datos y poder aumentar la capacidad del servidor. Logical Volume Management (en adelante LVM, siglas en inglés) hace uso de la función device-mapper del kernel de Linux para proporcionar un sistema de particiones independientes de la estructura subyacente del disco. Con LVM es posible crear un espacio de almacenamiento abstracto así como distintas “particiones virtuales”, por lo que es más fácil de agrandar/encoger particiones (siempre sujeto a posibles limitaciones propias del

sistema de archivos).

Se realizó una partición en disco para ser utilizado por LVM, después se creó un volumen lógico; una vez creado, se agregó a un grupo de volumen lógico, luego creamos un sistema de archivos de volumen lógicos el cual se agregaran al fichero /etc/fstab el cual nos permitirá guardar eventos nuevos de zoneminder sin borrar los antiguos.

Para ello se elaboró un video guía que describe el mecanismo utilizado para la implementación de Inicio de Gestión de datos mediante LVM, el video puede ser consultado en: https://www.youtube.com/watch?v=88LV89maSls

**Inicio de sesión mediante desafío-respuesta con Google reCAPTCHA.**

reCAPTCHA es una extensión de la prueba Captcha que se utiliza para reconocer texto presente en imágenes. Emplea por tanto la prueba desafío-respuesta utilizada en computación para determinar cuándo el usuario es o no humano para, a su vez, mejorar la digitalización de textos. reCAPTCHA se basa en el hecho de que para un ser humano puede ser simple determinar el texto presente en una imagen, pero para una máquina esta tarea resulta en ocasiones demasiado compleja.

Se utilizó en el loggin de zoneminder para evitar entradas realizadas mediante ataques de fuerza bruta a zoneminder, primero se creó el reCAPTCHA en la página de google de esta y después solo se agregaron: la llave secreta y de sitio, en las opciones de zoneminder.

Para ello se elaboró un video guía que describe el mecanismo utilizado para la implementación de Inicio de sesión mediante desafío-respuesta con Google reCAPTCHA, el video puede ser consultado en: https://www.youtube.com/watch?v=ovqPosUFf3o

**Filtrado de eventos.**

Los filtros permiten definir condiciones complejas con acciones asociadas en ZoneMinder. Los ejemplos podrían incluir:

- Borrar los datos cuando el disco duro del servidor llegue al 95%.
- Guardar eventos que tienen más de 7 días de antigüedad.
- Envíe un correo electrónico cada vez que ocurra un nuevo evento para un monitor específico.
- Eliminar eventos que tienen más de 7 días de antigüedad.

Zoneminder utiliza la ventana de filtro para crear sus propios filtros o para modificar los existentes. Incluso puede guardar sus filtros favoritos para reutilizarlos en una fecha

futura. El filtrado en sí es bastante simple; primero elige la cantidad de expresiones que desea que contenga su filtro.

Para ello se elaboró un video guía que describe el mecanismo utilizado para la implementación de filtrado de eventos dentro del presente trabajo monográfico, el video puede ser consultado en: https://www.youtube.com/watch?v=yFAPxmvt4P0

**Caducidad de sesión de usuario.**

Las sesiones de los usuarios que gestionan o trabajan con el zoneminder desde la web deben tener un tiempo de caducidad, esto permite que si el usuario se va a comer a su casa y deja la sesión iniciada la interfaz de acceso web dure cierto tiempo sin actividad y después de ello, obligue al usuario a autenticarse nuevamente.

Se configuro el fichero php-ini en el servidor apache2 para modificarle el tiempo de caducidad de sesión en el servidor.

Para ello se elaboró un video guía que describe el mecanismo utilizado para la implementación de Caducidad de sesión de usuario dentro del presente trabajo de monografía, el video puede ser consultado en: https://www.youtube.com/watch?v=_c3a8Pg7mwk

**Seguridad - Iptables.**

Iptables es una herramienta avanzada de filtrado de paquetes en Linux. Es una herramienta muy establecida, ya que hay millones de sitios en todo el mundo que funcionan y utilizan iptables de forma continua.

De lo que se encarga iptables, dicho de una forma sencilla, es de analizar cada uno de los paquetes del tráfico de red entra en una máquina y decidir, en función de un conjunto de reglas, qué hacer con ese paquete, siempre desde un punto de vista amplio, ya que iptables permite hacer muchas cosas diferentes con el tráfico de red.

Se elaboró un script con las reglas de iptables para detener los paquetes inválidos y que llegan desde direcciones enmascaradas, intenta además detener el escaneo de puertos bloqueando por un tiempo determinado la dirección IP desde donde se origina. Otra de las mejores prácticas que se siguen aquí es la de descartar las conexiones a todos los puertos de comunicación y solo crear reglas con los puertos que realmente se van a necesitar.

```
---

#!/bin/bash

### BEGIN INIT INFO
# Provides:          iptablesd
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: Firewall iptables service.
### END INIT INFO

INTERFAZ="enp2s0"
FW="/sbin/iptables"

#---CONFIGURACIÓN DE IPTABLES---

test -f $FW || exit 0

case "$1" in
start)
  echo "start --> Aplicando reglas para iptables..."

  # Borrar la configuración actual
  echo "  Borrando la configuración actual para iptables"
  iptables -F
  iptables -t filter -F
  iptables -t nat -F
  iptables -t mangle -F
  iptables -X
  iptables -t filter -X
  iptables -t nat -X
  iptables -t mangle -X
  iptables -Z

  # Definir las políticas por defecto
  echo "  Definiendo las políticas por defecto"
  echo "  Todos los puertos y servicios cerrados"
  iptables -P INPUT DROP
  iptables -P OUTPUT DROP
  iptables -P FORWARD DROP
  # iptables -t nat -P PREROUTING DROP
  # iptables -t nat -P POSTROUTING DROP

  # Permitir acceso desde la propia máquina (Interfaz de loopback)
  echo "  Habilitado el acceso desde la propia máquina a través de la interfaz de
loopback"
```

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A INPUT -m state --state NEW -i lo -j ACCEPT

# Permitimos las redirecciones de HTTPS y HTTP
echo "  Permitidas las redirecciones de HTTPS y HTTP"
# HTTPS
iptables -A FORWARD -i $INTERFAZ -p tcp --dport 443 -j ACCEPT # HTTPS [WEB
SEGURO TCP]
# HTTP
iptables -A FORWARD -i $INTERFAZ -p tcp --dport 80 -j ACCEPT # HTTP [WEB TCP]

# Evitamos paquetes TCP que sean nuevos y no tengan flag de SYN
iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP

# Todo lo que sea ICMP se descarta
iptables -A INPUT -p ICMP -j DROP
iptables -A OUTPUT -p ICMP -j DROP

#-----------SERVICIOS ABIERTOS AL TRÁFICO ENTRANTE----------------------------

# Permitir acceso al puerto 80 TCP y UDP (HTTP)
echo "  INPUT --> Puerto TCP 80[HTTP] abierto"
iptables -A INPUT -m state --state NEW -i $INTERFAZ -p tcp --dport 80 -j ACCEPT

# Permitir acceso al puerto 443 TCP y UDP (HTTPS)
echo "  INPUT --> Puerto TCP 443[HTTPS] abierto"
iptables -A INPUT -m state --state NEW -i $INTERFAZ -p tcp --dport 443 -j ACCEPT

# Permitimos acceso al puerto 2822 TCP y UDP (SSH)
echo "  INPUT --> Puerto TCP 2822[SSH] abierto"
iptables -A INPUT -m state --state NEW -i $INTERFAZ -p tcp --dport 2822 -j ACCEPT

# Evitamos ataques syn-flood a solo 4 paquetes por sergundo, los demas se descartan
iptables -A INPUT -p tcp --syn -m limit --limit 1/s --limit-burst 4 -j DROP

#-------------------------------------------------------------------------

#----------------------TRÁFICO SALIENTE PERMITIDO----------------------------

# Permitimos acceso al puerto 67 TCP y UDP (DHCP)
echo "  OUTPUT --> Puerto UDP 67[DHCP] abierto"
iptables -A OUTPUT -m state --state NEW -o $INTERFAZ -p udp --dport 67 -j ACCEPT

# Permitimos acceso al puerto 68 TCP y UDP (DHCP)
echo "  OUTPUT --> Puerto UDP 68[DHCP] abierto"
```

```
  iptables -A OUTPUT -m state --state NEW -o $INTERFAZ -p udp --dport 68 -j ACCEPT

  # Acceso al puerto 53 TCP y UDP (DNS)
  echo "  OUTPUT --> Puerto UDP 53[DNS] abierto"
  iptables -A OUTPUT -m state --state NEW -o $INTERFAZ -p udp --dport 53 -j ACCEPT

  # Acceso al puerto 80 TCP y UDP (HTTP)
  echo "  OUTPUT --> Puerto TCP 80[HTTP] abierto"
  iptables -A OUTPUT -m state --state NEW -o $INTERFAZ -p tcp --dport 80 -j ACCEPT

  # Acceso al puerto 443 TCP y UDP (HTTPS)
  echo "  OUTPUT --> Puerto TCP 443[HTTPS] abierto"
  iptables -A OUTPUT -m state --state NEW -o $INTERFAZ -p tcp --dport 443 -j
ACCEPT

  #--------------------------------------------------------------------------

  # Dado que el servidor tiene: HTTP[80], HTTPS[443] y SSH[2822]
  # abiertos hacia le exterior logeamos [logs] todos los accesos o intentos de acceso a
dichos servicios
  iptables -A INPUT -p tcp --dport 80 -j LOG --log-prefix "LOGS_SERVICES"
  iptables -A INPUT -p tcp --dport 443 -j LOG --log-prefix "LOGS_SERVICES"
  iptables -A INPUT -p tcp --dport 2822 -j LOG --log-prefix "LOGS_SERVICES"

  # Permitimos las conexiones establecidas y relacionadas
  echo "  Permitidas las conexiones establecidas y relacionadas"
  iptables -A INPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
  iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

  # Terminado
  echo "OK. Reglas para iptables aplicadas..."
  ;;

stop)
  echo "stop --> Borrando reglas para iptables..."

  # Borrar la configuración actual
  echo "  Borrando la configuración actual"
  iptables -F
  iptables -t filter -F
  iptables -t nat -F
  iptables -t mangle -F
  iptables -X
  iptables -t filter -X
  iptables -t nat -X
  iptables -t mangle -X
```

```
  iptables -Z

  # Configuración por defecto
  echo "  Estableciendo la configuración por defecto"
  echo "  Todos los puertos y servicios abiertos"
  iptables -P INPUT ACCEPT
  iptables -P OUTPUT ACCEPT
  iptables -P FORWARD ACCEPT
  iptables -t nat -P PREROUTING ACCEPT
  iptables -t nat -P POSTROUTING ACCEPT

  # Terminado
  echo "OK. Restaurada la configuración por defecto para iptables..."
  ;;

restart)
  echo "Reiniciando iptables..."
  $0 stop
  $0 start
  ;;

status)
  echo "status --> Verificando estado de iptables..."
  echo ""
  echo "*** Tabla filter ***"
  iptables -t filter -nvL
  echo "********************"
  echo ""
  echo "*** Tabla nat ***"
  iptables -t nat -nvL
  echo "******************"
  echo ""
  echo "*** Tabla mangle ***"
  iptables -t mangle -nvL
  echo "********************"
  ;;

*)
  echo "Uso: /etc/init.d/$0 {start|stop|restart|status}"
  exit 1
  ;;
esac
exit 0
```

**Presupuesto de implementación**

Anteriormente, mostramos todos los detalles con respecto a la implementación de la reactivación del sistema de video vigilancia en los laboratorios de computación.
A partir de eso podría surgir la pregunta ***¿Cuál sería el costo para poder llevar a cabo la reactivación del sistema de video vigilancia en los laboratorios de computación de la UNAN-León?***. Para responder a esta pregunta presentamos un aproximado de lo que costaría dicha reactivación.

| Detalle | Precio |
|---|---|
| **Costo de la cámara** | 120$ |
| **Cable UTP** | 0.75 $ x Metro |
| **Mano de obra** | 25 $ x Punto(cámara instalada) |
| **Pc DELL vostro 220** | 160$ |
| **2 Discos duros 500 Gb** | 65 $ c/u |
| **Memoria RAM 2Gb** | Incluida en el servidor |
| **Procesador core duo** | Incluida en el servidor |

**TABLA 8 PRESUPUESTO**

# Conclusiones

En el presente trabajo realizado del sistema de video vigilancia IP instalado en algunos de los laboratorios del Dpto. de Computación de la UNAN-León, se ha determinado la necesidad de la reactivación del dicho sistema, dado que a la fecha de realización del presente trabajo, el sistema no está funcionando correctamente, lo cual significa una pérdida y deterioro de los equipos con los que cuenta el Dpto. ya que los equipos instalados están en un continuo deterioro por las malas condiciones externas en las que se encuentran.

Dada la situación actual del sistema instalado se han realizado pruebas con el software libre Zoneminder en el sistema operativo Debian específicamente en su versión 9.1, el cual incluye una gran cantidad de opciones las cuales permiten el manejo de las cámaras IP instaladas y con facilidad de monitoreo, opciones de escalabilidad lo que cual facilita el aumento de número de cámaras, además opciones de seguridad para protección del sistema las cuales permiten tener un sistema más seguro.

En las pruebas realizadas con el zoneminder se pudo comprobar que es una muy buena solución para la reactivación del sistema de video vigilancia instalado ya que se adapta a los recursos con que cuenta el Dpto., siendo un software que no requiere de grandes especificaciones en los recursos del servidor y que permite incorporar las cámaras con las que cuenta el Dpto.

# Recomendaciones

Con el fin de facilitar la continuidad al proyecto y contribuir con la mejora de este se plantean las siguientes recomendaciones:

- La administración de la información de video almacenada debe ser manejada con total seriedad, con fines de seguridad y no como una forma de inmiscuirse en las actividades diarias de otras personas.

- La ubicación de las cámaras debe tener en cuenta ciertos criterios para que el sistema sea realmente efectivo por tal razón se recomienda realizar un estudio enfocado a esta problemática. (Véase la sección  Ubicación y cantidad cámaras IP.

- El almacenamiento de los videos capturado en las cámaras está en su totalidad centralizado, en caso de daños en la unidad de disco rígido toda esta información se perderá permanentemente. El almacenamiento distribuido o en la nube permitiría solventar parte de esta problemática.

- Realizar periódicamente un mantenimiento preventivo a las cámaras IP y al equipo servidor para que estos tengan un óptimo funcionamiento y evitar el deterioro de las mismas.

# Referencias bibliográficas

(s.f.). Obtenido de academic: http://www.esacademic.com/dic.nsf/eswiki/944432

(s.f.). Obtenido de deskshare: https://www.deskshare.com/lang/sp/resources/articles/wcm_SecurityCamera.aspx

(s.f.). Obtenido de comocomprarcctv: https://comocomprarcctv.wordpress.com/2016/10/14/3-elementos-claves-en-cctv/

(s.f.). Obtenido de rnds: http://www.rnds.com.ar/articulos/059/Cap_06.pdf

(s.f.). Obtenido de telecomabc: http://www.telecomabc.com/m/mpeg-4.html

(s.f.). Obtenido de tecnoseguro: https://www.tecnoseguro.com/faqs/cctv/que-es-poe

(s.f.). Obtenido de rhyshaden: http://www.rhyshaden.com/eth_poe.htm

(s.f.). Obtenido de cisco: https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/alolh/sp/svc_4.html

(s.f.). Obtenido de cisco: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

(s.f.). Obtenido de ITE: http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/cortafuegos_iptables.html

(s.f.). Obtenido de mit: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html

(s.f.). Obtenido de microsoft: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2000/bb742566(v=technet.10)

(s.f.). Obtenido de axis: https://www.axis.com/es/learning/web-articles/technical-guide-to-network-video/video-management-systems

(s.f.). Obtenido de linux-party: http://www.linux-party.com/57-seguridad/6308-videovigilancia-con-software-libre-y-linux

(s.f.). Obtenido de kmotion: https//www.kmotion.com

(s.f.). Obtenido de dosbit: http://www.dosbit.com/general/software-libre/ispy-un-software-para-las-camaras-de-vigilancia

Anastopoulou Nicky, L. J.-M. (2012). Obtenido de Slideshare: https://www.slideshare.net/nikianastopoulou/the-art-gallery-problem-eng-50272411

Ariganello, E. (s.f.). *Guía de estudio para la certificación CCNA Routing y Switching.*

AXIS. (4 de Octubre de 2018). *AXIS communications*. Obtenido de Axis communications: https://www.axis.com/es/learning/web-articles/technical-guide-to-network-video/bandwidth-considerations

Communication, A. (s.f.). Obtenido de Axis: https://www.axis.com/es/learning/web-articles/technical-guide-to-network-video/comparing-standards

Communications, A. (s.f.). Obtenido de onvisionsystems: http://www.onvisionsystems.com/destacado/tipos-de-camaras-de-red/

H. Schulzrinne, A. R. (2014). *RFC 2326. RealTime Streaming Protocol 2.0 (RTSP).*

H. Schulzrinne, S. C. (2003). *RFC 3550. RTP: A TransportProtocol for Real-Time Applications.*

Ibáñez, R. (s.f.). Obtenido de Cultura Científica: https://culturacientifica.com/2014/01/29/teorema-de-la-galeria-de-arte/

*Implementación de un sistema de vigilancia y control de eventos con acceso a través de red, en el área de tesorería en la UNAN – Managua.* (s.f.).

Jaun, A. D. (s.f.). *RTP, RTCP, and RTSP - Internet Protocol for Real-Time.*

Landmann. (s.f.). Obtenido de redhat: https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/6/pdf/logical_volume_manager_administration/Red_Hat_Enterprise_Linux-6-Logical_Volume_Manager_Administration-es-ES.pdf

Thomas Weigand, G. J. (s.f.). Obtenido de ieeexplore: https://ieeexplore.ieee.org/document/4117940/

# Anexos

## 1. Entrevistas

1.1 Entrevista parte 1, realizada el viernes 22 de septiembre de 2017. Ing. Denis Berrios (Sistema de cámaras de Seguridad)

Pedimos su colaboración en el llenado de la siguiente entrevista que aportará mucho a nuestra tesis de fin de carrera. Muchas gracias por sus aportes.

1. ¿Cómo y porqué surgió la idea de instalar las cámaras de video vigilancia en el departamento?
   R: Surgió la idea de las cámaras de video IP vigilancia por las pérdidas de hardware en los laboratorios de computación.

2. ¿Desde qué año está instalado dicho sistema?
   R: 2010

3. ¿De cuánto fue el presupuesto invertido para la instalación y puesta en marcha de dicho sistema?
   R: No recuerdo. Fue adquisición de la UNAN-León la que lo compro.

4. ¿Cuáles son espacios (aulas/laboratorios) que están conectados al sistema de video vigilancia?
   R: 2 cámaras por laboratorio. (Hardware, Alcalá 1 y 2, laboratorio 1)

5. ¿De cuánto es la capacidad de almacenamiento del disco duro del servidor de almacenamiento de videos?
   R: 500 Gb

6. ¿Cuánto tiempo en horas de grabación permite el sistema?
   R: 1 semana

7. ¿El sistema está actualmente en funcionamiento?
   R: Por daño de hardware y falta de recursos para compra no está funcionando.

8. ¿De los espacios (aulas/laboratorios) que estaban conectados originalmente al sistema de video vigilancia cuáles aún continúan en funcionamiento?
   R: Ninguno por la repuesta de la pregunta anterior.

9. ¿Todas las cámaras empleadas son de la misma marca y modelo?, ¿cuáles son las marcas y modelos empleadas?
   R: Sí. D link DCS 2102

10. ¿Las cámaras empleadas graban sólo cuando detectan movimiento o graban siempre?
    R: Se pueden configurar de ambas maneras y estaban grabando de corrido.

11. ¿Las cámaras tienen visión nocturna?
    R: Si tienen IR

12. ¿Cuáles son todos los usos que se le da al sistema de cámaras?
    R: Para proteger la propiedad de la UNAN-León. En su momento encontramos a dos estudiantes sus trayendo hardware sin permiso y fue reportado al decano.

13. ¿El servidor dónde está ubicado?
    R: La computadora de grabación está en mi oficina.

14. ¿Cuál es el sistema operativo del servidor?, ¿Cuáles son las características del servidor (almacenamiento, memoria RAM, Procesador, sistema operativo, entre otros,...)?
    R: No requiere nada extraordinario simplemente entre más espacio es mejor por más tiempo de almacenamiento. Es un computador genérico.

15. ¿Quién o quiénes fueron los encargados de la instalación del sistema y si en la actualidad le dan mantenimiento a este?
    R: En su momento yo lo instale y las cámaras no requieren mantenimiento hardware.

16. ¿Qué software de instalación y configuración posee?
    R: El software que trae las cámaras D-link

17. ¿Cuánto tiempo demoraron para la instalación y puesta en marcha?
    R: 30 minutos a 1 hora

18. ¿Cuál fue el problema que dio origen a la instalación del sistema y si hubo un resultado positivo ante este problema?
    R_ No hubo problema. Sino un pequeño atraso con problema de recursos, es decir, escalera, canaletas, toma de corriente.

19. ¿Usted considera que el sistema está siendo de utilidad actualmente?
    R: Como se contestó en una pregunta anterior no está funcionando por daño de equipo.
    Y si es de utilidad.

¿Qué mejoras considera que serían las adecuadas para que el sistema se reactive?
R: Instalación de DVR local en cada laboratorio con 4 cámaras.

20. ¿Actualmente quién es el encargado de administrar el sistema?

R: Yo

21. ¿Se le realiza mantenimiento y si es así cada cuánto tiempo?
    R: Como de contesto en otra pregunta anterior no necesita mantenimiento hardware en las cámaras.

1.2 Entrevista parte 2, realizada el viernes 12 de octubre de 2017. Ing. Denis Berrios (Sistema de cámaras de Seguridad)

1. ¿Cuáles son las características que posee el equipo que se estaba usado como servidor (memoria RAM, disco duro, sistema operativo, tipo y velocidad de interfaz de red, etc.)?
   R: 256 DDR1 RAM, 500 GB HDD, Windows 7 Pro, Tarjeta de red integrada 10/100, etc?

2. ¿El equipo servidor que estaba trabajando anteriormente tenía instalado algún tipo de seguridad como firewall o similares?
   R: Firewall por defecto que trae el ESET NOD32 de la institución.

3. ¿Qué mecanismo de acceso remoto se utilizaba para ingresar al equipo servidor, a las cámaras IP y a la configuración del sistema de video vigilancia?
   R: Las cámaras traen por defecto un sistema local de configuración que se accede por medio de su dirección IP, en la computadora se hace local, ya que por norma de seguridad no hay que hacer remoto desde exterior del recinto.

4. ¿Además del servicio de alojamiento para el sistema de video vigilancia que otros servicios se estaban brindando en ese equipo servidor?
   R: Solamente es un equipo para guardar los videos.

5. ¿Las cámaras también grababan sonido o solamente video?
   R: Tiene opción de grabar sonido que ya que son modo IP.

6. ¿Qué ancho de banda consumen las cámaras ubicadas en cada laboratorio? *
   R: Entre 256 a 512 kbps

7. Con respecto al uso que se le daba y proporcionaba el sistema servidor antes de que fallase, desde su opinión y punto de vista personal, ¿qué mejoras considera útiles y necesarias para que sean realizadas en el proceso de reactivación?
   R: Tamaño medio del marco: 210 kb
      Promedio de ancho de banda por cámara: 8.4 Mbps
      Almacenamiento estimado: 317.5 GB
      Almacenamiento en días (por cámara): 7 días

8. ¿Cuáles son las subredes, direcciones IP, VLANs y máscaras de red que estaban asignadas al servidor y a cada una de las cámaras IP?
   R: Tendría que hablar con informática de la UNAN-León para poder suministrar

esa información, ya que es un dato de la institución.