UNIVERSIDAD AMAZÓNICA DE PANDO

ÁREA DE CIENCIAS Y TECNOLOGÍA

Carrera de Ingeniería Informática

PROYECTO DE GRADO

"SISTEMA DE VIGILANCIA Y MONITOREO DE LAS AULAS AUDIOVISUALES DEL BLOQUE "G" DEL CAMPUS UNIVERSITARIO DE LA UNIVERSIDAD AMAZONICA DE PANDO UTILIZANDO CAMARAS IP"

PROYECTO DE GRADO PRESENTADO PARA OBTAR AL TÍTULO ACADÉMICO DE LICENCIADO EN INGENIERÍA DE SISTEMAS INFORMATICOS

Postulante : Univ. James Joffre Zeballos Ordoñez

Tutor : Ing. Juan Carlos Gallardo Jiménez

Asesor : Mcs.Ing. Christhian Miauchi Nataly

Cobija - Pando – Bolivia

Gestión. 2016

INDICE

INDICE II

INDICE III

INDICE DE FIGURA

INDICE DE FOTOS

INDICE DE IMAGENES DE INTALACION SOFTWARE

INDICE DE IMÁGENES DE ADMINISTRACION DE RENDIMIENTO

INDICE DE IMÁGENES DE ADMINISTRACION DE FALLA

INDICE DE IMÁGENES DE ADMINISTRACION DE SEGURIDAD

INDICE IV

CAPITULO I

INTRODUCCION

1.1. ANTECEDENTES

La Universidad Amazónica de Pando (U.A.P.), Teniendo en cuenta que es una de las Universidades más jóvenes del Sistema Universitario, tiende a crecer y desarrollarse más, incrementándose nuevas carreras de acuerdo a demandas y por ende el incremento del estamento estudiantil, para este propósito y por la tendencia tecnológica se tiene aulas con equipamiento Audiovisuales muy costosos, como también, una gran cantidad de diferentes activos que son vulnerables a daños y robos. VER [ANEXO A]

La Universidad Amazónica de Pando como entidad pública, se encuentra en la necesidad de proporcionar seguridad a los bienes del Estado, puesto que la falta de seguridad en sus ambientes se ha convertido en un creciente y sentido problema con el cual viene lidiando sin poder hasta la fecha lograr el tan anhelado objetivo de tener que brindar una adecuada seguridad.

La falta de seguridad convierte a la Universidad Amazónica de Pando y a todos quienes la conforman, en sujetos vulnerables ante la inseguridad, es por este motivo que el empleo de las nuevas tecnologías puede brindar una alternativa para solucionar la problemática planteada anteriormente, pues al establecer un adecuado sistema de seguridad mediante "la implementación de cámaras de monitoreo en los Aulas Audio Visuales del Bloque "G". De esta forma se apoyara a disminuir el daño y pérdidas de los diferentes bienes y otros objetos personales que se encuentran en la Universidad Amazónica de Pando.

El presente Proyecto tiene como finalidad, la implementación de un sistema de vigilancia y monitoreo de las aulas Audiovisuales del Bloque "G" del Campus Universitario de la Universidad Amazónica de Pando utilizando cámara IP y grabador de vídeo en red (Network Video Recorder, NVR), que permita la vigilancia de cada una de las aulas audiovisuales resguardando los diferentes activos que se encuentran en estas aulas Audiovisuales.

1.2. DESCRIPCIÓN DEL PROBLEMA

A medida que transcurren los años se evidencia la creación de nuevas carreras dentro de la Universidad Amazónica de Pando, ocasionando también el incremento de la población estudiantil. Este incremento hace que sea difícil la vigilancia y monitoreo de las diferentes aulas que se encuentran en el Campus Universitario en especial aquellas que cuentan con equipos audiovisuales muy costosos, los mismos que se convierten en centros de vulnerabilidad sujetos a sufrir daños, pérdidas de bienes y otros objetos, por actos delincuenciales.

Así mismo se tiene denuncias de robos dentro de las aulas, y destrozos de los muebles no pudiendo identificar a los autores.

Estas causas anteriormente mencionadas conducen al planteamiento del siguiente problema principal:

“Ineficiencia en la vigilancia, monitoreo y administración de las aulas audiovisuales del bloque “G” de la Universidad Amazónica de Pando”

A raíz de los problemas ya mencionados anteriormente, trae consigo una serie de efectos como daño a los equipos audiovisuales, sustracción de accesorios computacionales, destrozo de activos que se encuentran en las aulas del Bloque “G” provocando un enorme daño económico a la Universidad Amazónica de Pando.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

“Implementar un sistema de vigilancia y monitoreo para mejorar las administración y resguardar los activos que se encuentran en las aulas Audiovisuales del Bloque “G” de la Universidad Amazónica de Pando utilizando cámara IP y grabador de vídeo en red (Network Video Recorder), NVR.

1.3.2. OBJETIVOS ESPECIFICOS

- Realizar un diagnóstico de la situación actual de las Aulas del bloque “G” del Campus Universitario con relación a la seguridad.
- Realizar el diseño de la red de vigilancia y monitoreo para las Aulas audiovisuales del bloque “G”
- Instalar las cámaras IP de acuerdo al diseño de la red de monitoreo.
- Realizar las pruebas del sistema de vigilancia y monitoreo de las aulas audiovisuales del bloque “G”

1.4. JUSTIFICACIÓN

1.4.1. JUSTIFICACIÓN ECONOMICA

Con la implementación de este sistema de vigilancia y monitoreo se podrá reducir el índice de robo y el mal uso que se le da a los activos que se encuentran en las aulas audiovisuales del bloque “G”, reduciendo de gran manera los daños económicos que se produce a la Universidad Amazónica de Pando.

1.4.2. JUSTIFICACIÓN SOCIAL

El sistema de vigilancia y monitoreo será de mucha importancia para las autoridades de la Universidad Amazónica de Pando, ya que a través de este sistema se identificara los actos delincuenciales que se produzcan en estas instalaciones, así mismo se tendrá una mejor administración y resguardo de los activos que se encuentran en la Aulas Audiovisuales del bloque “G”.

1.4.3. JUSTIFICACIÓN TÉCNICA

Las Cámaras IP, son cámaras de vídeo de gran calidad que tienen incluido un ordenador a través del que se conectan directamente a Internet y la red que tenga la institución la cual podrá tener información en toda la red del Campus Universitario y así preservar los bienes que hay en las diferente Aulas Audio Visuales del Bloque “G”.

1.5. ALCANCES

Con la implementación de un sistema de vigilancia y monitores con cámaras IP, por medio de una red, se podrá observar y tener una mejor administración y control sobre las diferentes Aulas Audio Visuales del Bloque “G”.

- El Sistemas de vigilancia y monitores con cámaras IP brindara información visual en tiempo real de las aulas audiovisuales del bloque “G”.
- El Sistemas de vigilancia y monitores con cámaras IP alertar sobre robos
- El Sistemas de vigilancia y monitores con cámaras IP facilitara la investigación en caso de robo
- El Sistema de vigilancia y monitores con cámaras IP se utilizara con fines de resguardar los activos del aula audiovisual.
- El Sistema de vigilancia y monitores con cámaras IP no tendrá como fin designara aulas
- El Sistema de vigilancia y monitores con cámaras IP no tendrá como fin controlar la asistencia de los docentes

1.6. METODOLOGÍA

Para el desarrollo de este proyecto, se utilizó la metodología Modelo Funcional para la administración de Redes, mediante el cual se realizara un análisis detallado del cómo y que se necesita para su implementación desde los análisis previos hasta las pruebas del mismo.

La ventaja de esta metodología, es que divide en 5 áreas funcionales que son: Configuración, rendimientos, fallas, contabilidad y seguridad, donde se define las funciones de cada una de ellas. Para el desarrollo del proyecto se adecuara cuatro procesos.

1.6.1. Administración de configuración

A continuación se describen las actividades ubicadas dentro del proceso de la administración de la configuración. Estas actividades son la planeación y diseño de la red; la instalación y administración del software; administración de hardware, y el

aprovisionamiento. Por último se mencionan los procedimientos y políticas que pueden ser de ayuda para el desarrollo de esta área.

1.6.2. Administración de rendimiento

Tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo al comportamiento encontrado

1.6.3. Administración de falla

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para reestablecer la situación o minimizar el impacto de la falla

1.6.4. Administración de la seguridad

Su objetivo es ofrecer servicios de seguridad a cada uno de los elementos de la red así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques, así como para la respuesta ante incidentes de seguridad.

1.7. RESULTADOS OBTENIDOS

Al termino del Proyecto el Sistema de Vigilancia y Monitoreo de la aula audiovisuales del bloque “G” del Campus Universitario de la U.A.P, cabe la necesidad de brindar información veraz y oportuna en un tiempo eficiente de manera que se establece como parte esencial para la investigación en caso de robo y mejor administración de los ambientes para el procesos Académico - Administrativo fortaleciendo así en el cuidado de los activos de esta Superior Casa de Estudios.

1.8. ORGANIZACIÓN DEL DOCUMENTO

El presente trabajo se organiza los siguientes capítulos.

CAPÍTULO I, se refiere a los antecedentes, el problema, la solución propuesta, los objetivos y la metodología adoptada para el cumplimiento de los objetivos.

CAPÍTULO II, presenta el marco teórico y conceptual del trabajo, hace referencia a la metodología, herramientas y técnicas aplicadas para el desarrollo del proyecto de grado.

CAPÍTULO III, presenta la ingeniería del proyecto, el desarrollo del proyecto, y la implementación del sistema.

CAPÍTULO IV, presenta las conclusiones y recomendaciones del proyecto

En el presente capítulo se da a conocer toda la información necesaria y relacionada con el sistema de vigilancia y monitorea con cámaras IP, primeramente se da referencia de la Universidad Amazónica de Pando; posteriormente se detalla la parte legal, y a continuación se hace referencia a toda las bases teóricas que sustenta el presente Proyecto.

El sistema está orientado tanto a los usuarios, como a las tecnologías elegidas para su implementación, es por ello que en este capítulo se desarrollan términos que ayuden a comprender métodos, técnicas para la implementación de este proyecto.

CAPITULO II

REFERENCIA INSTITUCIONAL
REFERENCIA LEGAL
REFERENCIA TEÓRICA

2.1. REFERENCIA INSTITUCIONAL

La Universidad Amazónica de Pando, es una Institución Pública y Autónoma de Educación Superior, que forma profesionales idóneos, con excelencia académica, pensamiento crítico y compromiso social, que desarrolle la investigación científica y tecnología, promoviendo la interacción social, en un contexto de diversidad social e interculturalidad, para contribuir al desarrollo integral de nuestra amazonia. (U.A.P. 2013)

MISION

Institución Pública (Domótica Viva s.l., 2002) y Autónoma de Educación Superior, que forma profesionales idóneos, con excelencia académica, pensamiento crítico y compromiso social, que desarrolle la investigación científica y tecnología, promoviendo la interacción social, en un contexto de diversidad social e interculturalidad, para contribuir al desarrollo integral de nuestra amazonia.

VISIÓN INSTITUCIONAL

En el año 2017 la Universidad Amazónica de Pando será una Universidad Autónoma, transparente, desconcentrada, incluyente, con libertad de pensamientos, comprometida con su población, que brinde profesionales de excelencia académica, investigación científica y tecnología pertinente hacia su entorno; enfocada en una gestión moderna y flexible basada en resultados, con todos sus programas acreditados, orientados al bienestar de la comunidad universitaria para contribuir al desarrollo integral de nuestra amazonia.

ASPECTOS ORGANIZACIONALES Y FUNCIONALES DE LA UAP

La estructura orgánica de la U.A.P. cuenta con dos niveles: De decisiones y asesoría y el nivel operativo. VER [ANEXO B]

2.2. REFERENCIA LEGAL

La Universidad Amazónica de Pando, fue creada mediante Decreto Supremo N° 20511 del 21 de septiembre de 1984 y sancionada mediante Ley de la Nación N° 653 de 18 de octubre de 1984.

El Estatuto Orgánico de la UAP fue aprobado en la VI Conferencia Nacional de Universidades en octubre de 1997 y por el Congreso Nacional de Universidades el mes de mayo de 1999, ambos eventos realizados en la ciudad de Trinidad Capital del Departamento del Beni.

Las actividades académicas comenzaron oficialmente el 3 de diciembre de 1993, con dos Carreras:

- Licenciatura en Biología
- Licenciatura en Enfermería.

En agosto de 1996 se incorporó la carrera de Informática a nivel de Técnico Superior. Posteriormente, consecuente con la política de diversificación de la oferta curricular, a partir de la gestión académica del 2000 se crearon los siguientes programas académicos:

- Ingeniería Agroforestal, a Nivel de Licenciatura.
- Derecho, con mención en derecho ambiental, a nivel de Licenciatura.
- Construcción Civil, a nivel de Técnico Superior
- Pesca y Acuicultura, también a nivel de Técnico Superior.

2.3. REFERENCIA TEÓRICA

2.3.1. INTRODUCCION

De acuerdo al CAP. IV en su numeral 50 (SISTEMAS DE CÁMARAS DE SEGURIDAD Y MONITOREO ELECTRÓNICO) de la Ley N° 264 del 31 de julio del 2012, LEY DEL SISTEMA NACIONAL DE SEGURIDAD CIUDADANA “PARA UNA VIDA SEGURA”, refiere:

Las empresas prestadoras de servicios públicos, las entidades financieras bancarias, las entidades públicas y los centros de esparcimiento público y privado con acceso masivo de personas, deberán instalar en sus dependencias sistemas de cámaras de seguridad y monitoreo electrónico para garantizar la seguridad de las personas. La contravención a esta normativa será sancionada de acuerdo a su reglamentación. VER [ANEXO, C]

Es en este sentido, que el contenido de este capítulo se enfoca en conceptos esenciales para el funcionamiento de un sistema de vigilancia y monitoreo con cámaras IP, para esto se examinara en primer lugar la evolución que ha tenido en los sistemas de vigilancia y sus componentes en rasgos generales, la historia e importancia de la Internet, tipos de redes ya sean alámbricas o inalámbricas y sus diferentes topologías, así como también los componentes de la red.

2.3.2. DESCRIPCIÓN GENERAL DE UN SISTEMA DE VÍDEO EN RED

El video en red, también denominado video vigilancia basada en IP o vigilancia IP aplicado a la industria de la seguridad, utiliza una red IP alámbrica o inalámbrica como eje principal para la transmisión de video, audio digital y otros datos. Al aplicar la tecnología de alimentación a través de Ethernet (PoE), la red también puede utilizarse para suministrar energía a los productos de video en red. (DOINTECH , 2015)

Un sistema de video en red permite supervisar y grabar video desde cualquier lugar de la red, ya sea, por ejemplo, una red de área local (LAN) o una red de área amplia (WAN) como Internet.

Los componentes básicos de un sistema de video en red son la cámara de red, el codificador de video (empleado para conectar cámaras analógicas a una red IP), la red, el servidor y el almacenamiento, y el software de gestión de video. Como la cámara de red y el codificador de video son equipos basados en ordenadores, poseen capacidades que no pueden compararse a las de una cámara CCTV (circuito cerrado de televisión) analógica. La cámara de red, el codificador de video y el software de gestión de video se consideran las piedras angulares de una solución de vigilancia IP.

Los componentes de la red, el servidor y el almacenamiento son parte del equipo de IT estándar.

La posibilidad de utilizar equipamiento comercial listo para el uso representa una de las principales ventajas del video en red. Otros componentes de un sistema de video en red incluyen accesorios, como soportes, midspans PoE y joysticks. Se tratara más

detenidamente cada componente de video en red en capítulos sucesivos. (DOINTECH , 2015)

2.3.2.1 Ventajas

Un sistema de video vigilancia en red completamente digital ofrece un sinfín de ventajas y funcionalidades avanzadas que no puede ofrecer un sistema de video vigilancia analógica tradicional.

Las ventajas incluyen una alta calidad de imagen, accesibilidad remota, gestión de eventos y capacidades de video inteligente, posibilidades de integración sencilla y mejor escalabilidad, flexibilidad y rentabilidad.

Alta calidad de imagen: en una aplicación de video vigilancia, disponer de una calidad de imagen alta resulta esencial para poder capturar nítidamente un incidente en curso e identificar a las personas u objetos implicados. Con las tecnologías HDTV/megapíxel y de

Barrido progresivo, una cámara de red puede ofrecer una mejor calidad de imagen y una resolución mayor que una cámara analógica. Para obtener más información sobre la calidad de imagen, consulte los capítulos 2, 3 y 6. (AXIS COMMUNICATIONS, 2006-2015)

La calidad de imagen también puede conservarse más fácilmente en un sistema de video en Red que en uno de video vigilancia analógica. Con los sistemas analógicos actuales, que utilizan una grabadora de video digital (DVR) como medio de grabación, se realizan muchas conversiones analógicas a digitales: en primer lugar, las señales analógicas se convierten en digitales en la cámara y, a continuación, de nuevo en analógicas para su transmisión; después, las señales analógicas se digitalizan para grabarse. Las imágenes capturadas se degradan con cada conversión entre los formatos analógico y digital, así como con la distancia de su transmisión por cable. Cuanto mayor sea el recorrido que las señales de video analógicas deben realizar, más débiles se tornan. En un sistema de vigilancia IP completamente digital, las imágenes procedentes de una cámara de red se digitalizan una vez, permaneciendo en formato digital sin sufrir conversiones

innecesarias ni degradación debido a la distancia recorrida en su transmisión por la red.

Accesibilidad remota: es posible configurar las cámaras de red y los codificadores de video y acceder a ellos de forma remota, permitiendo a múltiples usuarios autorizados visualizar el video en directo y grabado en cualquier momento y prácticamente desde cualquier lugar del mundo conectado a red. Esto resulta ventajoso en el caso de que los usuarios desearan que otra empresa, como una empresa de seguridad o las autoridades policiales, también tuviera acceso al video.

Gestión de eventos y vídeo inteligente: a menudo disponemos de demasiado material de Video grabado y de poco tiempo para analizarlo adecuadamente. Los productos de video en Red pueden encargarse de este problema de distintas formas. Las cámaras de red y los codificadores de video, por ejemplo, pueden programarse para enviar videos para su grabación solo cuando se produzca, bien mediante programación o activación, un evento.

Esto reduciría la cantidad de grabaciones sin interés. Las grabaciones de video también pueden etiquetarse con cierta información, denominada metadatos, para facilitar la búsqueda y el análisis de los videos de interés.

Los productos de video en red Axis son compatibles con funcionalidades de video inteligente (por ejemplo, detección de movimiento por video, alarma anti manipulación activa, detección de audio, cable de activación y aplicaciones de terceros como contadores de personas y mapeados de calor). También ofrecen conexiones de E/S (Entrada/Salida) a dispositivos externos, como luces. Estas características permiten a los usuarios definir las condiciones o eventos que activaran las alarmas. Al producirse un evento, los productos pueden responder automáticamente con acciones programadas. Las acciones configurables pueden incluir grabaciones de video de una o más instalaciones, locales y/o externas por seguridad, activar dispositivos externos como alarmas, luces e interruptores de posición de puertas y enviar mensajes de notificación a usuarios. Las funcionalidades de gestión de eventos pueden configurarse empleando las páginas

web del producto de video en red o un programa de software de gestión de video. Para obtener más información sobre la gestión de video, consulte el Capítulo 11.

Integración sencilla y preparada para el futuro: los productos de video en red basados en estándares abiertos pueden integrarse fácilmente en una amplia variedad de sistemas de Gestión de video. El video procedente de una cámara de red también puede integrarse en otros sistemas, como un punto de venta, un control de acceso o un sistema de gestión de edificios. Un sistema analógico, por otra parte, raramente dispone de una interfaz abierta para la integración sencilla con otros sistemas y aplicaciones.

2.3.2.2. Escalabilidad y flexibilidad:

Un sistema de video en red puede crecer conforme a las necesidades del usuario, cámara a cámara, mientras que los sistemas analógicos normalmente solo pueden ampliarse en pasos de cuatro o dieciséis unidades. Los sistemas IP ofrecen un medio para que los productos de video en red y otros tipos de aplicaciones compartan la misma red alámbrica o inalámbrica para comunicar datos. El video, audio, comandos PTZ y de E/S, alimentación y otros datos pueden transmitirse a través del mismo cable, pudiendo añadir cualquier número de productos de video en red al sistema sin modificaciones significativas ni costosas para la infraestructura de red. Esto no sucede con un sistema analógico.

En un sistema de video analógico, cada cámara debe estar conectada directamente y mediante un cable específico (normalmente coaxial) a un puesto de visualización/grabación.

También podrían requerirse cables individuales para el movimiento horizontal/vertical y zoom y para el audio.

También podrían requerirse cables individuales para el movimiento horizontal/vertical y zoom y para el audio. Los productos de video en red también pueden situarse y conectarse a la red desde prácticamente cualquier lugar y el sistema puede ser tan abierto o cerrado como se desee. Dado que un sistema de video en red está basado en protocolos y un equipamiento IT estándar, puede

beneficiarse de estas tecnologías a medida que el sistema se amplia. Por ejemplo, el video puede almacenarse en servidores redundantes ubicados en localizaciones independientes para aumentar la fiabilidad, pudiendo utilizarse herramientas para el mantenimiento del sistema, la administración de la red y para compartir la carga automáticamente, lo que resulta imposible en el caso del video analógico.

Rentabilidad de la inversión: un sistema de vigilancia IP normalmente tiene un coste total de propiedad inferior al de un sistema analógico CCTV tradicional. Una infraestructura de red IP a menudo ya se ha implementado y se utiliza para otras aplicaciones dentro la organización, por lo que una aplicación de video en red puede aprovecharse de la infraestructura existente. Las opciones inalámbricas y redes IP también constituyen alternativas mucho menos costosas que el cableado de fibra óptica o coaxial tradicional empleado por un sistema analógico CCTV. Además, las transmisiones de video digital pueden enviarse a todo el mundo mediante diversas infraestructuras interpretativas. Los costes de gestión y equipamiento también son inferiores, ya que el almacenamiento y las aplicaciones secundarias se ejecutan en servidores basados en sistemas abiertos y estándares de la industria, no en hardware de propiedad exclusiva como un DVR, en el caso de un sistema analógico CCTV.

Un sistema de video en red también puede ofrecer otras perspectivas para mejorar un negocio.

Por ejemplo, en aplicaciones para el comercio minorista, la implementación del análisis de video en red puede ayudar a mejorar la afluencia de clientes y a mejorar las ventas.

Además, los productos de video en red son compatibles con tecnologías de Alimentación a través de Ethernet (PoE). La tecnología PoE permite a los dispositivos conectados a red recibir alimentación de un midspan o conmutador habilitado para dicha tecnología a través del mismo cable Ethernet que transmite los datos (video). Por lo tanto, no es necesario disponer de una toma de pared junto

a la localización de la cámara. La tecnología PoE ofrece un notable ahorro en costes de instalación y puede aumentar la fiabilidad del sistema.

2.3.2.3. Comunicación segura:

Los productos de video en red, así como las transmisiones de video, pueden asegurarse de varios modos. Incluyen la autentificación mediante nombre de usuario y contraseña, filtro de direcciones IP, autentificación mediante IEEE 802.1X y encriptado de datos utilizando HTTPS (SSL/TLS) o VPN. En una cámara analógica no existe capacidad de encriptación ni posibilidades de autentificación. Cualquiera puede interceptar el video o sustituir la señal procedente de una cámara analógica por otra señal de video. Los productos de video en red también disponen de flexibilidad para ofrecer varios niveles de acceso de usuario.

Las instalaciones de video analógico existentes, sin embargo, pueden migrar a un sistema de video en red y aprovechar algunas de las ventajas digitales con ayuda de los codificadores de video y dispositivos como adaptadores de Ethernet sobre cable coaxial, que hacen uso de cables coaxiales heredados.

2.3.2.4 Aplicaciones

El video en red puede emplearse en un número de aplicaciones casi ilimitado. La mayoría de sus usos pertenecen al ámbito de la seguridad y vigilancia o la supervisión remota de personas, lugares, propiedades y operaciones. El video en red se emplea cada vez más en la mejora de la eficiencia comercial, a medida que aumenta el número de aplicaciones de video inteligente. A continuación, se exponen algunas posibilidades de aplicación habituales en sectores industriales clave.

- **Comercio minorista.-** Los sistemas de video en red de las tiendas minoristas pueden reducir notablemente los casos de hurto, mejorar la seguridad del personal y optimizar la gestión de la tienda. Una importante ventaja que ofrece el video en red es su posibilidad de integración en un sistema EAS (Vigilancia electrónica de artículos) o en un sistema POS (Punto de venta) del

establecimiento, con el objetivo de facilitar imagen y grabación de actividades relacionadas con pérdidas. El sistema puede permitir la detección rápida de incidentes potenciales, así como cualquier falsa alarma. El video en red permite un alto nivel de interoperabilidad y la rentabilidad más inmediata.

El video en red, junto con las aplicaciones de video inteligente, puede ayudar a identificar las áreas más concurridas de un establecimiento, ofreciendo una grabación de la actividad del consumidor y del comportamiento de compra que ayudaran a optimizar el diseño de una tienda o mostrador. También puede contabilizar el número de personas que entran y salen de un establecimiento para ayudar, por ejemplo, en temas relativos a la planificación del personal y reflejar cuando es necesario abrir más cajas para absorber grandes colas.

- **Transporte.-** El video en red ayuda a proteger a los pasajeros, al personal y las mercancías en cualquier sistema de transporte. En lo referente al transporte público, todas las cámaras de seguridad de estaciones, terminales, autobuses, trenes y túneles pueden conectarse a un centro de seguridad. Cuando se produce un incidente, los operadores de seguridad pueden visionar el video en directo procedente de las cámaras relevantes para decidir rápidamente la acción adecuada a tomar. En los aeropuertos, el video en red también se está convirtiendo en una herramienta empleada para aumentar la eficacia de una amplia variedad de servicios en áreas como estacionamientos, comercios, facturación, servicios de restauración y control de Seguridad.

  Los puertos y las terminales logísticas se benefician de las capacidades de detección integradas del video en red, que pueden alertar automáticamente al personal de seguridad de la violación de un perímetro. El video en red también puede utilizarse para supervisar las condiciones de tráfico, reducir la congestión y permitir una respuesta rápida ante accidentes. Una amplia variedad de cámaras de red Axis soportan exigentes condiciones interiores y exteriores. Para vehículos de pasajeros, como autobuses y trenes, Axis ofrece cámaras de red que pueden soportar diversas temperaturas, niveles de humedad, polvo, vibraciones y actos de vandalismo.

- **Actividades bancarias y financieras.-** Los bancos utilizan el video vigilancia desde hace mucho tiempo y, aunque la mayoría de las instalaciones siguen siendo analógicas, el video en red se emplea en instalaciones nuevas y rehabilitadas. Esto permite a un banco supervisar eficazmente sus oficinas centrales, sus sucursales y los cajeros automáticos desde una localización central.

  El sistema puede estar equipado con capacidades inteligentes que envían automáticamente alertas ante intentos de fraude en cajeros automáticos, como clonación de tarjetas o bloqueos de tarjetas o efectivo. Todo el video puede grabarse con calidad HDTV, ofreciendo imágenes nítidas de personas y objetos que faciliten las investigaciones e identificaciones positivas.

- **Vigilancia urbana.-** El video en red es una de las herramientas más útiles en la lucha contra el crimen y para la protección ciudadana. Puede utilizarse tanto para detectar como para disuadir. El uso de redes inalámbricas ha permitido un desarrollo efectivo del video en red en todo el entorno urbano. Los costes de instalación pueden reducirse enormemente gracias a cámaras de red que ofrecen características de instalación rápida y fiable, incluyendo la posibilidad de enfoque y configuración remotos a través de la red. Las capacidades de vigilancia remota del video en red han permitido a la policía responder rápidamente a crímenes que se cometen en directo.

- **Educación.-** Desde guarderías a universidades, los sistemas de video en red ayudan a disuadir actos vandálicos y a mejorar la seguridad del personal y los estudiantes. Permiten la supervisión eficaz de todas las instalaciones interiores y exteriores y ofrecen imágenes de alta calidad que facilitan una identificación positiva de personas y objetos. Además, las cámaras en red pueden generar alarmas automáticas. Por ejemplo, si una cámara se manipula, o si se producen ruidos o movimientos en un edificio en horario de cierre, pueden enviarse

imágenes en tiempo real al personal de seguridad. El video en red también puede utilizarse para el aprendizaje a distancia, por ejemplo, para estudiantes que no puedan asistir a clase.

El sistema puede conectarse fácilmente a la infraestructura de una red existente, manteniendo así unos costes bajos de instalación y mantenimiento.

- **Seguridad ciudadana.-** El video en red puede emplearse para asuntos relacionados con el cumplimiento de la ley, militares y control fronterizo. Es también un método eficiente de asegurar toda clase de edificios públicos, desde museos y bibliotecas hasta juzgados y prisiones. Las cámaras situadas en las salidas y entradas de los edificios pueden grabar a las personas que entran y salen las 24 horas del día. Pueden emplearse para prevenir actos vandálicos y para mejorar la seguridad del personal y de los visitantes.
- **Asistencia sanitaria.-** El video en red permite mejorar la seguridad global y del personal, pacientes y visitantes en hospitales e instalaciones de asistencia sanitaria.

  En caso de alarma, el personal de seguridad autorizada y del hospital puede acceder al video en directo de áreas críticas, como salas de urgencias, departamentos psiquiátricos y salas de suministros médicos para obtener una visión rápida de la situación. El video en red también permite una monitorización del paciente de alta calidad, asistencia medica remota por parte de especialistas y aprendizaje a distancia.

- **Industrial.-** El video en red no es solo una herramienta eficiente para asegurar perímetros y locales, también se emplea en la supervisión y mejora de la eficacia de líneas y procedimientos de fabricación y sistemas logísticos. En áreas peligrosas o salas blancas, la supervisión remota reduce los tiempos para la solución de problemas y respuesta. En industrias con varias instalaciones de producción, el video en red puede reducir notablemente los desplazamientos necesarios por motivos de asistencia técnica.

- **Infraestructuras críticas.-** Tanto si se trata de una planta solar, como de una subestación eléctrica o de una instalación de gestión de residuos, el video en red puede ayudar a garantizar una actividad diaria segura, protegida e ininterrumpida. Los datos de producción procedentes de instalaciones remotas pueden mejorarse gracias a la información visual.

  Los sistemas de vigilancia ofrecen nuevas posibilidades de seguridad y comercial par a todos los sectores de la industria. (AXIS COMMUNICATIONS, 2006-2015)

2.3.3. CÁMARA DE RED O CÁMARA IP

Las cámaras IP, son vídeo cámaras de vigilancia que tienen la particularidad de enviar las señales de video (y en muchos casos audio), pudiendo estar conectadas directamente a un Reuter ADSL, o bien a un concentrador de una Red Local, para poder visualizar en directo las imágenes bien dentro de una red local (LAN), o a través de cualquier equipo conectado a Internet (WAN) pudiendo estar situado en cualquier parte del mundo.

A la vez, las cámaras IP permiten el envío de alarmas por medio de Email, la grabación de secuencias de imágenes, o de fotogramas, en formato digital en equipos informáticos situados tanto dentro de una LAN como de la WAN, permitiendo de esta forma verificar posteriormente lo que ha sucedido en el lugar o lugares vigilados.

2.3.3.1 Instalación de las cámaras IP

Las cámaras IP, son vídeo-cámaras de vigilancia que tienen la particularidad de enviar las señales de video (y en muchos casos audio), pudiendo estar conectadas directamente a un Router ADSL, o bien a un concentrador de una Red Local, para poder visualizar en directo las imágenes bien dentro de una red local (LAN), o a través de cualquier equipo conectado a Internet (WAN) pudiendo estar situado en cualquier parte del mundo.

2.3.3.2. Constitución de las cámaras IP

Las cámaras IP internamente están constituidas por la “cámara” de Vídeo propiamente dicha (Lentes, sensor de imagen, procesador digital de señal), por un

“motor” de compresión de imagen (Chip encargado de comprimir al máximo la información contenida en las imágenes) y por un “ordenador” en miniatura (CPU, FLASH, DRAM, y módulo ETHERNET/ WIFI) encargado en exclusiva de gestionar procesos propios, tales como la compresión de las imágenes, el envío de imágenes, la gestión de alarmas y avisos, la gestión de las autorizaciones para visualizar imágenes, ... en definitiva las cámaras IP son unos equipos totalmente autónomos, lo que permite conectarlo en el caso más sencillo directamente a un Reuter ADSL, y a la red eléctrica y de esta forma estar enviando imágenes del emplazamiento donde este situada.

También es posible conectar las cámaras IP como un equipo más dentro de una Red Local, y debido a que generalmente las redes locales tienen conexión a Internet, saliendo de esta forma las imágenes al exterior de la misma manera que lo hace el resto de la información de la Red. (Seguridad via ip, 2014)

2.3.3.3. Aplicación de las cámaras IP

Algunas de las aplicaciones más frecuentes de las cámaras IP son la vigilancia de:

- **Viviendas,** permitiendo visionar la propia vivienda desde la oficina, desde un hotel, cuando estamos de vacaciones.
- **Negocios,** permitiendo controlar por ejemplo varias sucursales de una cadena de tiendas, gasolineras.
- **Instalaciones industriales,** almacenes, zonas de aparcamiento, Muelles de descarga, accesos, incluso determinados procesos de maquinaria o medidores.
- **Hostelería, Restauración,** Instalaciones deportivas.
- **Lugares Turísticos,** cada día es más frecuente que Organismos oficiales, como Comunidades Autónomas, Ayuntamientos, promocionen sus zonas turísticas, o lugares emblemáticos de las ciudades, instalaciones deportivas, implementado en sus páginas Web las imágenes procedentes de Cámaras IP estratégicamente situadas en esos lugares (Seguridad via ip, 2014).

2.3.3.4. Ventajas de las cámaras IP frente a los sistemas de Circuito Cerrado de Televisión (CCTV) Tradicionales

Las Cámaras IP poseen muchas ventajas frente a los sistemas tradicionales de vigilancia mediante Circuito Cerrado de TV (CCTV), las fundamentales son:

- **Acceso Remoto:** La observación y grabación de los eventos no tiene por qué realizarse "in situ" como requieren los sistemas CCTV.
- **Costo reducido:** La instalación es mucho más flexible ya que se basa en la infraestructura de la Red Local existente o nueva, o también en la conexión directa a un Router, bien por cable o de forma inalámbrica (Wireless LAN). Se elimina el costo de los sistemas de grabación digital de los CCTV, ya que las grabaciones se realizan en el disco duro de un PC de la propia red local o en un PC remoto.
- **Flexibilidad frente a la ampliación del sistema:** Los sistemas tradicionales CCTV generalmente requieren duplicar los sistemas de monitorización cuando se amplía el sistema, los sistemas de Cámaras IP permiten su ampliación sin necesidad de invertir en nuevos sistemas de monitorización.

2.3.3.5. Transformación de los sistemas de vigilancia CCTV a un sistema de Cámaras IP

Es posible convertir un Sistema de Vigilancia CCTV en Cámaras IP, mediante los Servidores de Vídeo IP.

Un Servidor de Vídeo es una de las partes integradas en el interior de una Cámara de Red.

El Servidor de Vídeo internamente está constituido por uno o varios "conversores" Analógico Digitales (Chip que pasa la señal de vídeo analógica de las cámaras a formato digital), "motor" de compresión de imagen (Chip encargado de comprimir al máximo la información contenida en las imágenes), y por un "ordenador" en miniatura (CPU, FLASH, DRAM, y módulo ETHERNET) encargado en exclusiva de gestionar procesos propios, tales como la compresión de las imágenes, el envío de imágenes, la gestión de alarmas y avisos, la gestión de las autorizaciones para

visualizar imágenes, en definitiva es un equipo totalmente autónomo, lo que permite conectarlo, en el caso más sencillo directamente a un Reuter ADSL, y a la red eléctrica y de esta forma poder enviar imágenes del sistema tradicional de CCTV. (Domótica Viva s.l., 2002)

2.3.3.6. Control de movimientos de las cámaras IP como en los sistemas de CCTV tradicionales

Es posible controlar las cámaras como en los Sistema de Vigilancia CCTV tradicionales.

Dentro de la gama de Cámaras IP existe una gran variedad en función de la aplicación que le vaya a dar, en general existen cámaras Fijas y Cámaras con movimiento. Las Cámaras "Pan-Tilt" (P/T) así llamadas por disponer de posibilidad de movimiento Horizontal y Vertical, permiten crear un sistema de vigilancia con gran cobertura y gran flexibilidad, ya que en muchas ocasiones pueden sustituir a varias cámaras fijas.

La visualización de las cámaras con movimiento y el manejo de las mismas se pueden realizar a distancia mediante el Internet Explorer, simplemente tecleando la dirección IP privada o pública de la cámara en función de que se visualice desde la LAN o la WAN. Inmediatamente será solicitado introducir el Nombre de Usuario y Contraseña, y esto dará paso a la visualización de las imágenes. En la pantalla de visualización estarán presentes las herramientas de software que permiten girar la cámara, llevarla a la posición preestablecida etc. (Domótica Viva s.l., 2002)

2.3.3.7. Conexión de sensores externos de alarma a las Cámaras IP

Es posible conectar sensores de alarma externos a las Cámaras IP, todas las Cámaras y Servidores de Vídeo disponen de entradas para conectar opcionalmente Sensores Externos complementarios a los sistemas que incluyen de fábrica, por ejemplo detectores PIR convencionales para poder cubrir la detección de movimiento que pudiera provenir de ángulos no cubiertos por la cámara.

En general las Cámaras IP así como los servidores de Vídeo disponen un complejo sistema de detección de movimiento mediante el análisis instantáneo y continuado de las variaciones que se producen en los fotogramas de vídeo que registra el sensor óptico. Este sistema permite graduar el nivel de detección de movimiento en la escena, y por ejemplo poder discriminar si en la escena ha entrado un "coche" o un "peatón", incluso en algunos modelos es posible generar distintas áreas dentro de la escena, y cada una con distinta sensibilidad al movimiento. (Domótica Viva s.l., 2002)

2.3.3.8. Dispositivos de forma remota desde las Cámaras IP

Según (Domótica Viva s.l., 2002) es posible la conexión de un relé que maneje por ejemplo el encendido de luces, o por ejemplo la apertura de una puerta. Las Cámaras IP y Servidores de Vídeo disponen de una salida Abierto Cerrado, que se controla desde el software de visualización.

2.3.3.9. Ubicación de las cámaras IP

Las Cámaras IP, y en general todas las cámaras de TV. Están diseñadas para su uso en interiores, en condiciones normales de polvo y humedad y temperatura.

Para la utilización de las Cámaras IP o de las cámaras de TV en exteriores o en interiores donde las condiciones de trabajo sean extremas, es necesario utilizar Carcasas de Protección adecuadas a la utilización que se le vaya a dar. Existe gran variedad de carcasas, están las con Ventilación, con Calefacción, Metálicas, de Plástico,... cada aplicación aconsejará la elección del modelo adecuado. (Domótica Viva s.l., 2002)

2.3.3.10. Protección de las cámaras IP

Las Cámaras de Red y los Servidores de Video disponen en su software interno de apartados de seguridad que permiten en general establecer diferentes niveles de seguridad en el acceso a las mismas. Los Niveles son:

- **Administrador:** Acceso mediante Nombre de usuario y Contraseña a la configuración total de la cámara.

- **Usuario:** Acceso mediante Nombre de usuario y Contraseña a la visualización de las imágenes y manejo del relé de salida.
- **Demo: Acceso** libre a la visualización sin necesidad de identificación. (Domótica Viva s.l., 2002)

2.3.3.11. Transmisión de Audio desde Cámaras IP

En general la mayoría de las Cámaras IP disponen de micrófonos de alta sensibilidad incorporados en la propia cámara, con objeto de poder transmitir audio mediante el protocolo de conexión UDP. (Domótica Viva s.l., 2002)

2.3.3.12. Sistemas de compresión de vídeo que utilizan las Cámaras IP

El sistema de Compresión de Imagen que utilizan las Cámaras IP tiene como objetivo hacer que la información obtenida del sensor de imagen, que es muy voluminosa, y que si no se tratara adecuadamente haría imposible su envío por los cables de la red Local, ocupe lo menos posible, sin que por ello las imágenes enviadas sufran deterioro en la calidad o en la visualización.

En definitiva los sistemas de compresión de imagen tienen como objetivo ajustar la información que se produce a los anchos de banda de los sistemas de transmisión de la información como por ejemplo el ADSL

Los estándares de compresión actuales son el MJPEG y MPG4, este último es el más reciente y potente. (Domótica Viva s.l., 2002)

2.3.3.13. Visualización de las Cámaras IP

Para la visualización de las Cámaras IP lo único que se necesita es que en el sistema operativo del PC se encuentre instalado el Microsoft Internet Explorer, mediante el mismo se tendrá acceso a la dirección propia de la Cámara de Red, que mostrará las imágenes de lo que en ese momento este sucediendo.

Esto resulta extremadamente útil, ya que permitirá poder visualizar la cámara desde cualquier ordenador, en cualquier parte del mundo, sin necesidad de haber instalado un software específico.

Aunque las imágenes Motion JPEG generadas por un sistema de vigilancia IP son nativas para la mayoría de los navegadores web estándar, el verdadero valor de los productos de Vigilancia IP se aprecia mejor cuando se utiliza software de grabación y monitorización profesional, lo que convierte al servidor de PC's de una red en un grabador de vídeo en red (Network Video Recorder, NVR).

2.3.3.14. Configuración remota de las cámaras IP

Las Cámaras IP y los Servidores de Vídeo solamente necesitan conectarse directamente a un PC mediante un cable de red "cruzado" cuando se instalan por primera vez.

Una vez instalada, cualquier modificación de la configuración, de los ajustes de calidad de imagen, de las contraseñas de acceso, se realizará de forma remota desde cualquier punto del mundo, bastará con conectarse a la cámara en modo "Administrador" a través de la Red de Internet. (Domótica Viva s.l., 2002)

2.3.3.15. Normas y Estándares del Codificador para compresión de video.

H.261 es el codificador estándar para la compresión de vídeo. Es el primer miembro de la familia H.26x de normas de codificación de vídeo y fue el primer códec de vídeo que fue útil en términos prácticos. H.261 fue diseñado originalmente para la transmisión sobre RDSI líneas en las que las velocidades de datos son múltiplos de 64 kbit/s. El algoritmo de codificación fue diseñado para ser capaz de operar a velocidades de bits de vídeo entre 40 kbit/s y 2 Mbit/s. De hecho, todas las normas posteriores internacionales de codificación de vídeo (MPEG-1 Parte 2, H.262 / MPEG-2 Parte 2, H.263, MPEG-4 Parte 2, H.264 / MPEG-4 Parte 10, y HEVC) se han basado estrechamente en el diseño H.261. Además, los métodos utilizados por el comité de desarrollo de H.261 para desarrollar conjuntamente el estándar ha mantenido el proceso operativo básico para los trabajos de normalización posterior en el campo. Fue desarrollado por el CCITT Especialistas del XV Grupo de Estudio sobre Codificación para Telefonía Visual (que más tarde se convirtió en parte de la UIT-T SG16). (tecnology, 2011 - 2016)

2.3.4. INTERNET

2.3.4.1. Origen y evolución

La red de computadoras Internet nació en 1969. Fue creada por un grupo de investigadores del Departamento de Defensa de los EE.UU. para establecer un sistema de comunicación con otras agencias del gobierno. La idea era desarrollar un sistema que respondiera a la pregunta: ¿cómo se podrían comunicar las autoridades después de una guerra nuclear? La solución era crear una red que no dependiera de un organismo central, sino que estuviera integrada por puntos de enlace de igual rango y con la misma capacidad de originar, transmitir y recibir mensajes. En caso de que alguno de estos nodos recibiera un ataque o dejara de funcionar, el resto de la red seguiría operando y los mensajes llegarían a su destino final.

Así, en 1969 la Agencia para Proyectos de Investigación Avanzada (ARPA1), una dependencia del Pentágono, decidió incursionar en la creación de una red de computadoras que permitiera el intercambio de información telefónica y que cumpliera con los requerimientos antes mencionados. A esta red se la llamó Arpanet y fue desarrollada gracias al apoyo del MIT (Massachussets Institute of Technology) y la UCLA (Universidad de California Los Ángeles).

La aparición de este nuevo sistema de comunicación trajo un problema: ¿cómo enlazar computadoras distintas, como la IBM y las no compatibles a esta? Ante esa interrogante se crearon los protocolos, un conjunto de reglas que permite el intercambio de datos entre dos computadoras. “El protocolo original se conocía como NCF (Network Control Protocol), que fue cambiado por un nuevo estándar más sofisticado llamado TCP/IP, publicado en 1974 por Vint Cert y Bob Kahn. TCP (Transmission Control Protocol) convierte mensajes en cadenas de paquetes en el nodo de origen y los ensambla de nuevo en el punto de destino.

IP (Internet Protocol) maneja el direccionamiento y permite que los paquetes sean ruteados, a través de diferentes nodos, hasta diferentes redes con varios estándares como Ethernet2, FDDI3 y X.2545. Gracias a estos protocolos,

computadoras con diferentes sistemas operativos pueden entrar en contacto para intercambiar investigaciones, enviar correos electrónicos, suscribirse a listas de interés, conversar en tiempo real, etc.

En el año 1983, Arpanet se divide en una red militar llamada Milinet e Internet propiamente dicho. La primera se desenvuelve en el ámbito militar y la segunda es de carácter público.

Al inicio, Internet es administrado por la National Science Foundation (NSF), encargada de organizar los dominios (o direcciones de Internet para las diferentes redes conectadas) según sus ubicaciones geográficas y el tipo de actividades que realizan (ver cuadro 1.1). De esta manera, en una dirección de Internet será sencillo reconocer el país y el tipo de actividad que la origina.

Cuadro 1.1	
gov :	Government
gob :	Gobierno
mil :	Militares
edu :	Educacionales
com :	Comerciales
org :	Organizaciones
net :	Enlace entre redes

En 1986, la National Science Foundation inició en Estados Unidos el desarrollo de la red NSFNET para facilitar el acceso de toda la comunidad científica ame ricana a cinco grandes centros de supercomputación. Esta red privada se convirtió en la espina dorsal de Internet.

En 1989, un equipo de investigación en Suiza, perteneciente al CERN6 (Centro Europeo de Investigación de Partículas), desarrolló una serie de protocolos para transferir hipertexto7 vía Internet. Hasta finales de los años de la década de 1980, Internet fue utilizado principalmente por investigadores y académicos

estadounidenses; pero en la década siguiente, desde que empezó a popularizarse, creció a un ritmo desenfrenado.

A principios de 1990, un grupo de personas perteneciente al National Center for Supercomputing Applications (NCSA) mejoró esos nuevos protocolos y desarrolló el NCSA Mosaic, el primer navegador que convertía el uso de Internet en algo fácil. Fue entonces cuando comenzó el boom de la World Wide Web (WWW) que atrajo a miles de personas hacia Internet.

Internet es una red de ordenadores conectados en todo el mundo que ofrece diversos servicios a sus usuarios, como pueden ser el correo electrónico, el chat o la web. Todos los servicios que ofrece Internet son llevados a cabo por miles de ordenadores que están permanentemente encendidos y conectados a la red, esperando que los usuarios les soliciten los servicios y sirviéndolos una vez son solicitados. Estos ordenadores son los servidores, los hay que ofrecen correo electrónico, otros hacen posible nuestras conversaciones por chat, otros la transferencia de ficheros o la visita a las páginas web y así hasta completar la lista de servicios de Internet.

Desde un punto de vista más amplio la "Internet" constituye un fenómeno sociocultural de importancia creciente, una nueva manera de entender las comunicaciones que están transformando el mundo, gracias a los millones de individuos que acceden a la mayor fuente de información que jamás haya existido y que provocan un inmenso y continuo trasvase de conocimientos entre ellos.

Existen cuatro características que definen a la "Internet":

1. Grande: la mayor red de computadoras del mundo

2. Cambiante: se adapta continuamente a las nuevas necesidades y circunstancias

3. Diversa: da cabida a todo tipo de equipos, fabricantes, redes, tecnologías, medios físicos de transmisión, usuarios, etc...

4. Descentralizada: no existe un controlador oficial sino más bien está controlada por los miles de administradores de pequeñas redes que hay en todo el mundo. Por lo tanto, queda garantizado el talante democrático e independencia de la red frente a grupos de presión (políticos, económicos o religiosos). (Marquez, 2014)

2.3.5. REDES DE COMPUTADORAS

Una red de computadoras (también llamada red de ordenadores o red informática) es un conjunto equipos (computadoras y dispositivos), conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, para compartir información (archivos), recursos (discos, impresoras, programas, etc.) y servicios (acceso a una base de datos, internet, correo electrónico, chat, juegos, etc.). A cada una de las computadoras conectadas a la red se le denomina un nodo.

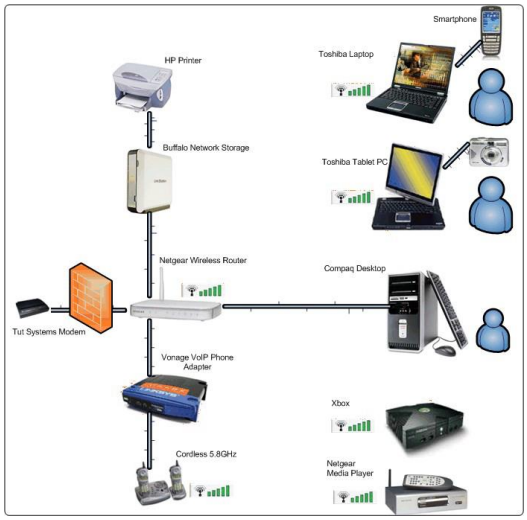


IMAGEN 1 : REDES DE COMPUTADORAS
FUENTE: MARQUEZ, 2014

2.3.5.1. Clasificación de la Red

Las redes de computadoras se clasifican de la siguiente manera:

- Según su cobertura se clasifican en: PAN, LAN, MAN, WAN
- Según su topología se clasifican en: ESTRELLA, ANILLO, BUS, HIBRIDAS.
- Según su relación funcional DE CLASIFICAN EN: CLIENTE SERVIDOR, IGUAL A IGUAL.

2.3.5.2. Según su cobertura

2.3.5.2.1. PAN **(red de área Personal):**

Es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora (teléfonos incluyendo las ayudantes digitales personales) cerca de una persona. El alcance de una PAN es de algunos metros. Se pueden conectar con cables alos USB y FireWire de la computadora. Una red personal sin hilos del área (WPAN) se puede también hacer posible con tecnologías de red tales como IrDA y Bluetooth.

2.3.5.2.2. LAN (red de área local):

Una red que se limita a un área tal como un cuarto, un solo edificio o una nave. Una LAN grande se divide generalmente en segmentos lógicos más pequeños llamados grupos de trabajo.

2.3.5.2.3. MAN (red de área metropolitana):

Una red que conecta las redes de dos o más locales pero no se extiende más allá de los límites de la una ciudad.

2.3.5.2.4. WAN (red de área mundial):

Es una red que cubre un área geográfica amplia y en gran parte de su estructura utiliza instalaciones de transmisión telefónicas.

IMAGEN 2 : WAN (RED DE AREA MUNDIAL)

FUENTE: MARQUEZ, 2014

2.3.5.3. Según su topología:

La topología o forma lógica de una red se define como la forma de tender el cable a estaciones de trabajo individuales.

2.3.5.3.1. Topología Estrella:

La red se une en un único punto; un concentrador de cableado o HUB que a través de él los bloques de información son dirigidos hacia las estaciones. Su ventaja es que el concentrador monitorea el tráfico y evita las colisiones y una conexión interrumpida no afecta al resto de la red. La desventaja es que los mensajes son enviados a todas las estaciones, aunque vaya dirigido a una.

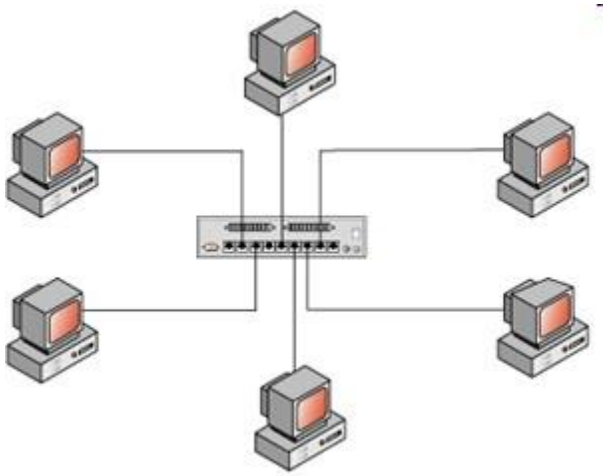


IMAGEN 3: TOPOLIGIA ESTRELLA
FUENTE: MARQUEZ, 2014

2.3.5.3.2. Topología Anillo

Las estaciones están unidas unas con otras formando un círculo por medio de un cable común. Las señales circulan en un solo sentido alrededor del círculo, regenerándose en cada nodo. Cada nodo examina la información que es enviada a través del anillo, si no está dirigida a él la pasa al siguiente nodo. La desventaja es que si se rompe una conexión, se cae la red completa.

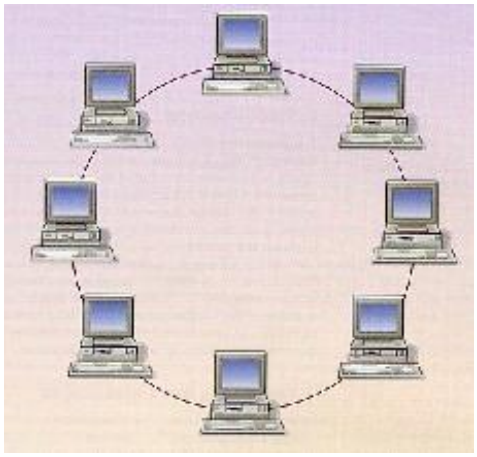


IMAGEN 4: TOPOLOGIA ANILLO
FUENTE: MARQUEZ, 2014

2.3.5.3.3. Topología Bus

Las estaciones están conectadas por un único segmento de cable. A diferencia del anillo, el bus es pasivo, no se produce regeneración de las señales en cada nodo.

Los nodos en una red de "bus" transmiten la información y esperan que ésta no vaya a chocar con otra información transmitida por otro de los nodos. Si esto ocurre, cada nodo espera una pequeña cantidad de tiempo al azar, después intenta retransmitir la información.

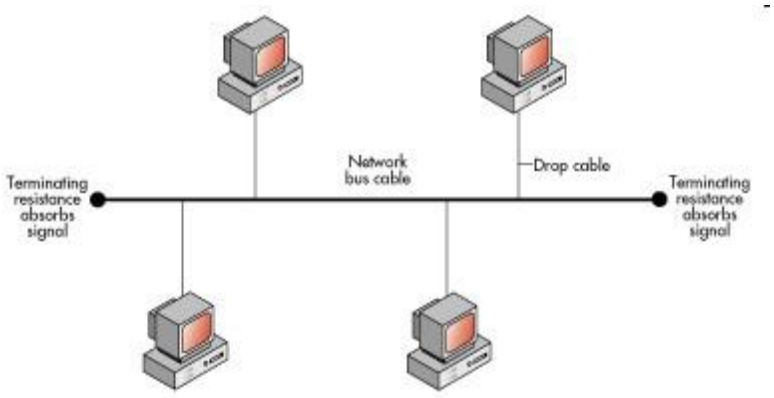


IMAGEN 5: TOPOLOGIA BUS
FUENTE: MARQUEZ, 2014

2.3.5.3.4. Topología Jerárquica

Los nodos están colocados en forma de árbol. Es parecida a una serie de redes en estrella interconectadas, con la diferencia que no tiene un nodo central sino un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos. Es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones porque se comparte el mismo canal de comunicaciones.

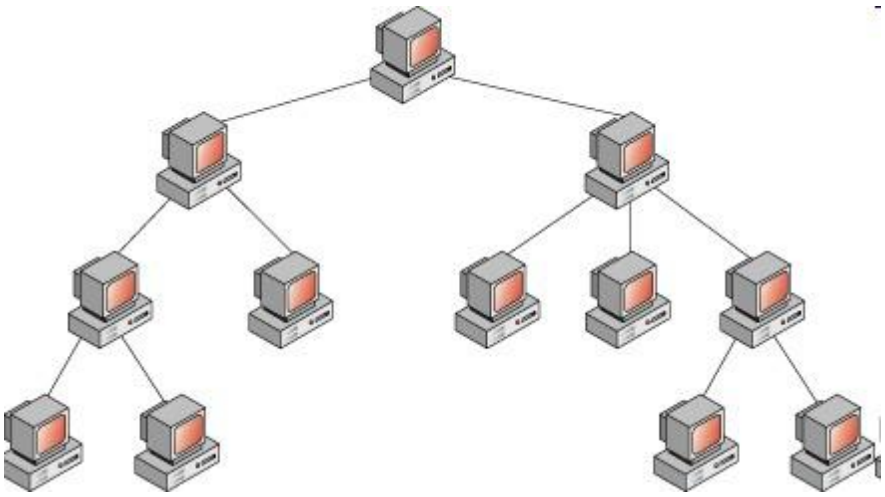


IMAGEN 6: TOPOLIGIA JERARQUICA
FUENTE: MARQUEZ, 2014

2.3.5.3.5. Topología Híbridas

El bus, la estrella y el anillo se combinan algunas veces para formar redes híbridas.

Anillo en estrella: se utiliza con el fin de facilitar la administración de la red. Físicamente, la red es una estrella centralizada en un concentrador, mientras que a nivel lógico, la red es un anillo.

Bus en estrella: el fin es igual a la topología anterior. En este caso la red es un "bus" que se cablea físicamente como una estrella por medio de concentradores.

Estrella jerárquica: esta estructura de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada para formar una red jerárquica.

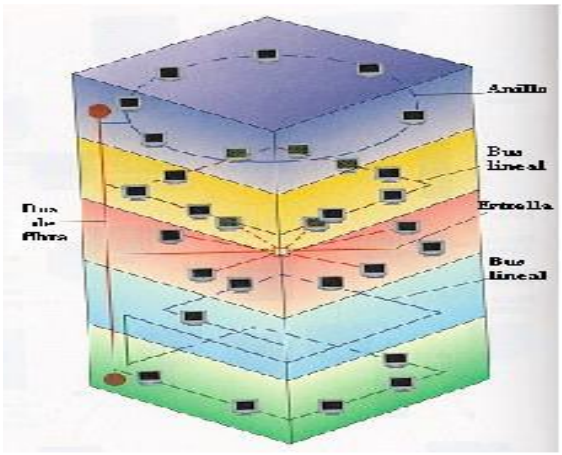


IMAGEN 7: TOPOLOGIA HIBRIDAS
FUENTE: MARQUEZ, 2014

2.3.5.4. Según su relación funcional

2.3.5.4.1. Cliente-Servidor:

En este caso el servidor es una máquina específica que usa un sistema operativo desarrollado especialmente para este tipo de red. Las estaciones de trabajo comparten recursos disponibles a partir de este servidor. La ejecución de las tareas está dividida entre el cliente (o estación) y el servidor. Este tipo

de red proporciona un mejor rendimiento y niveles de seguridad más adecuados para el trabajo profesional en red.

2.3.5.4.2. Par a par:

Punto a punto (P2P) es un tipo de red donde todos los equipos conectados pueden desempeñar el papel de servidor y de estación de trabajo al mismo tiempo. En este caso, si alguien quisiera compartir un recurso podría ofrecerlo a los demás. Este es un tipo de red para trabajos simples, donde el volumen de información intercambiado es pequeño y la seguridad no es un factor crítico.

IMAGEN 8: SEGÚN SU RELACION FUNCIONAL
FUENTE: MARQUEZ, 2014

2.3.6. Componentes Básicos

Dentro los componentes Básicos se tienen los siguientes Computadoras y Periféricos como las placas de comunicación

2.3.6.1. Placas de comunicación

2.3.6.1.1. Placa de red:

Permite la conexión con otras computadoras utilizando un cable y alcanza gran velocidad de transmisión.

2.3.6.1.2. Modem:

Cuando la PC se conecta por medio de la línea telefónica.

2.3.6.2. Cables de conexión

2.3.6.12.1. Coaxial:

Similar al utilizado para la TV por cable. Transmite información a 10 Mbps sobre distancias de casi 600 metros. Ej.: RG58 o banda base (utilizado en redes LAN de pequeña cobertura) y RG59 (utilizado para señales de televisión).

IMAGEN 9: CABLE COAXIAL
FUENTE: MARQUEZ, 2014

2.3.6.2.2. Par trenzado:

Sus alambres conductores están enrollados, logra mayor inmunidad al ruido electromagnético. Velocidad de hasta 1 Mbps a aprox. de 100 metros. Es similar a los que conectan los aparatos telefónicos. Ej.: STP y UTP (se utiliza en redes de computadoras en topología de estrella).

IMAGEN 10: PAR TRENZADO
FUENTE: MARQUEZ, 2014

2.3.6.2.3. Fibra óptica:

En lugar de usar señales eléctricas para transmitir la información usa señales de luz, solucionando el problema de ruido. Ofrece un ancho de banda mucho mayor, por eso transmite a velocidades de cientos de Mbps.

IMAGEN 11: FIBRA OPTICA
FUENTE: MARQUEZ, 2014

2.3.7. Transmisiones Inalámbricas

Es una subred de comunicación con cobertura geográfica limitada, cuyo medio físico de comunicación es el aire.

No pretende reemplazar una red cableada, sólo la complementa en situaciones donde es difícil realizar una conexión o para alcanzar grandes distancias.

Presenta la desventaja de cobertura y velocidad limitada y es una tecnología relativamente nueva. Este tipo de comunicación es hecha por compañías especializadas que además suministran los equipos como antenas, codificadores, etc.

Ejemplos: Radio, Infrarrojos, Microondas, BlueTooth, Satelital.

2.3.7.1 Aplicación:

Para expandir una red, movilidad de equipos, crear una nueva red, instalación de red en áreas poco accesibles para cablear, colocación de LAN temporal, enlace entre edificios, etc.

Ejemplos: Radio, Infrarrojos, Microondas, BlueTooth, Satelital

IMAGEN 12: APLICACIONES
FUENTE: MARQUEZ, 2014

2.3.7.2. Alcance

2.3.7.2.1. Largo alcance:

CDPD (cellular digital data packet) o Módems inalámbricos

SMS (short message service) o Mensajería y correo electrónico (teléfonos celulares)

2.3.7.2.2. Corto alcance:

IEEE 802.11 o Redes Inalámbricas o DSSS

Bluetooth o Redes usuario – usuario o FHSS o Cel – PC; PC – PC; PC – Palmpilot.

2.3.7.3. Área de Cobertura

2.3.7.3.1. Tipo Barreras

Tipo Barreras	Tipo de Barrera (techo,pared, piso)	Confiable (metros)	Probable (metros)
Área Abierta	vista directa	120	200
Área Semiabierta	madera, material sintético	30	50
Área Cerrada	Ladrillo	15	25

2.3.7.4. Equipos de Conexión

Dependiendo de la cantidad de equipos existentes, de la distancia física entre ellos y del tipo de red elegida, puede ser indispensable la adquisición de equipos electrónicos que sirven para para una comunicación eficiente y confiable.

Hubs o Concentradores: son equipos que permiten estructurar el cableado de las redes. El hub da conectividad pero lo que entra por una boca se repite en todas y son las terminales las que tienen que rechazar lo que no es para ellas . Ejemplo se usa para unir los brazos de una red en estrella, siendo su núcleo.

Puentes (Bridges): puede unir segmentos o grupos de trabajo LAN, pero puede dividir una red para aislar el tráfico o los problemas.

Switch: es parecido al hub pero lo que entra por una boca solo sale por la que tiene conectada la terminal destino haciendo que la red tenga menos trafico, se dice que es un hub inteligente porque sabe a quién enviar cada paquete.

2.3.7.4.1. Puentes (Bridges):

Puede unir segmentos o grupos de trabajo LAN, pero puede dividir una red para aislar el tráfico o los problemas.

Es el dispositivo de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.

Interconecta segmentos de red (o divide una red en segmentos) haciendo la transferencia de datos de una red hacia otra con base en la dirección física de destino de cada paquete.

El término bridge, formalmente, responde a un dispositivo que se comporta de acuerdo al estándar IEEE 802.1D.

En definitiva, un bridge conecta segmentos de red formando una sola subred (permite conexión entre equipos sin necesidad de routers). Funciona a través de una tabla de direcciones MAC detectadas en cada segmento al que está conectado. Cuando detecta que un nodo de uno de los segmentos está intentando transmitir datos a un nodo del otro, el bridge copia la trama para la otra subred, teniendo la capacidad de desechar la trama (filtrado) en caso de no tener dicha subred como destino. Para conocer por dónde enviar cada trama que le llega (encaminamiento) incluye un mecanismo de aprendizaje automático (auto aprendizaje) por lo que no necesitan configuración manual.

Clasificación de Puentes de red

Se pueden clasificar los puentes de red, atendiendo dos aspectos: según el tipo de interfaz y según la localización geográfica de las redes de área local (LAN) que se van a interconectar.

Según interfaz

- **Puentes homogéneos**

  Interconecta LAN con el mismo protocolo MAC (el nivel físico puede diferir), es decir, no hay conversión de protocolos a nivel 2, simplemente almacenamiento y reenvío de tramas. Un ejemplo de dispositivo homogéneo es un Switch Ethernet.

- **Puentes heterogéneos**

  El puente dispone de una entidad superior encargada de la transformación de cabeceras entre distintos tipos de interfaces. Recibe tramas por una interfaz (por ejemplo: Wi-Fi) para enviarlas por otra de otro tipo (por ejemplo: Ethernet). Un ejemplo de dispositivo, con las interfaces de ejemplo anteriores, es un punto de acceso en una red wi-fi.

Según localización geográfica

- **Puentes locales**

  Sirven para enlazar directamente dos redes físicamente cercanas.

- **Puentes remotos o de área extensa**

  Se conectan en parejas enlazando dos o más redes locales y formando una red de área extensa (WAN) a través de líneas telefónicas (Stallings, (2005)

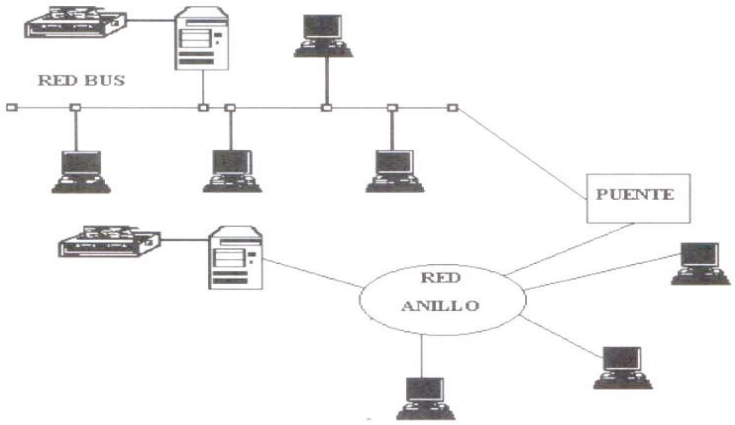


IMAGEN 13: PUENTES (BRIDGES)
FUENTE: STALLINGS, 2005

2.3.7.4.2. Enrutadores (Routers):

Conecta redes o segmentos red con distintos protocolos y arquitecturas. El bridge podría resultar inadecuado para asegurar una comunicación rápida entre todos los segmentos. Una red de esta complejidad necesita un dispositivo que no sólo conozca las direcciones de cada segmento, sino también, que sea capaz de determinar el camino más rápido para el envío de datos y filtrado del tráfico de difusión en el segmento local.

2.3.7.4.3. Repetidores (Repeaters):

Amplían la longitud de la red uniendo dos segmentos y amplificando la señal, pero junto con ella amplifican también el ruido. La red sigue siendo una sola, con lo cual, siguen siendo válidas las limitaciones en cuanto al número de estaciones que pueden compartir el medio.

2.3.7.4.4. Pasarelas (Gateways):

Son equipos para interconectar redes con protocolos y arquitecturas completamente diferentes a todos los niveles de comunicación, al igual que un router, pero se lo emplea como puerta de salida de una red a otra más grande (digamos... Internet)

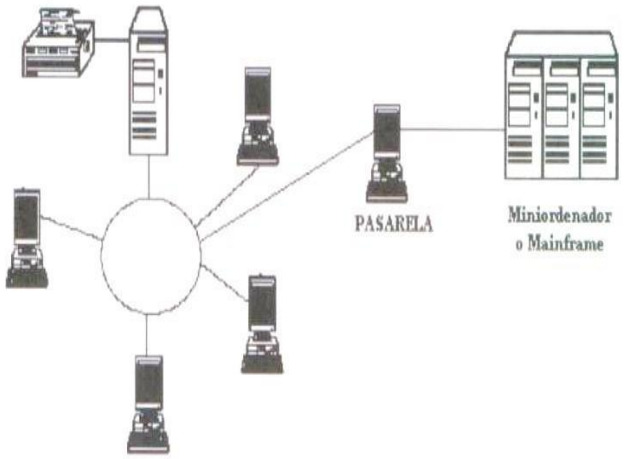


IMAGEN 14: PASARELA (GATEWAYS)
FUENTE: STALLINGS, 2005

2.3.7. 5. ANTENA DE RED INALAMBRICA

La antena es una herramienta que emite la señal. Existen dos familias de antenas, las omnidireccionales y las direccionales.

Las antenas omnidireccionales, recibe su nombre por la capacidad de emitir señales en todas las direcciones.

La antena direccional, es típica para estables enlaces punto a punto o para conectar a un nodo, se caracteriza por su alta ganancia que va desde unos discretos 15dbi, llegando en los modelos superiores hasta los 24 dbi, cuanto más alta es la ganancia de este tipo de antenas, más alta es su direccionalidad, ya que reduce muchísimo el ángulo en el que irradia la señal, llegando a ser tan estrecho como 8 grados de apertura.

2.3.7.6. NVR

Es muy similar a un DVR, la diferencia es que el DVR digitaliza, graba y administra imágenes enviadas desde cámaras de seguridad analógicas, en cambio un NVR, graba y administra imágenes ya digitales las cuales son enviadas desde las cámaras IP a través de una Red.

Con el sistema IP las imágenes llegan procesadas al grabador. Se puede basar en un ordenador o sistema autónomo, se puede usar un cable UTP o incluso Wifi.

Se trata de un videograbador hibrido, ya que combina ambas tecnologías. Se incluye en entornos donde se aprovechan instalaciones analógicas y se recurre a la tecnología IP.

2.3.7.7. SWITCH

Es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la Red, debido al ancho de banda pequeños y embotellamientos.

El switch puede agregar mayor ancho de bandada, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto.

2.3.7.8. TPLINK

Es un adaptador inalámbrico de ala potencia de 300 Mbps que permite a los usuarios activar el PC o portátil con capacidad inalámbrica muy potente para ofrecer mejoras de rendimiento. El adaptador adopta el diseño de alta potencia que ofrece hasta diez veces la gama de adaptadores convencionales.

2.3.7.9. CAMARA IP

Las cámaras IP, son vídeo cámaras de vigilancia que tienen la particularidad de enviar las señales de video (y en muchos casos audio), pudiendo estar conectadas directamente a un Router ADSL, o bien a un concentrador de una Red Local, para poder visualizar en directo las imágenes bien dentro de una red local (LAN), o a través de cualquier equipo conectado a Internet (WAN) pudiendo estar situado en cualquier parte del mundo.

A la vez, las cámaras IP permiten el envío de alarmas por medio de E-mail, la grabación de secuencias de imágenes, o de fotogramas, en formato digital en equipos informáticos situados tanto dentro de una LAN como de la WAN, permitiendo de esta forma verificar posteriormente lo que ha sucedido en el lugar o lugares vigilados.

Las cámaras IP actualmente se pueden instalar en cualquier sitio que disponga de conexión a Internet mediante Router ADSL o XDSL (Con dirección IP fija, aunque algunos modelos también permiten IP dinámica); incluso otros modelos de cámaras ip permiten que esa conexión no sea permanente y que cuando sea necesaria se pueda realizar por medio de un módem convencional a la línea telefónica básica.

2.3.7.10. CABLE UTP CATEGORIA 6ª

El cable UTP categoría 6ª, es un estándar de cable para gigabit, etheternet y otros protocolos de Redes que es retro compatible con los estándares de categoría 5, 5e y categoría 3. La categoría 6ª posee características y especificaciones para evitar la diafonía y el ruido.

El Cable de categoría 6, o Cat 6a (ANSI/TIA/EIA-568-B.2-1) es un estándar de cables para Gigabit Ethernet y otros protocolos de redes que es retrocompatible con los estándares de categoría 5/5e y categoría 3. La categoría 6 posee características y especificaciones para evitar la diafonía (o crosstalk) y el ruido.

El estándar de cable se utiliza para 10BASE-T, 100BASE-TX y 1000BASE-TX (Gigabit Ethernet). Alcanza frecuencias de hasta 250 MHz en cada par y una velocidad de 1 Gbps. La conexión de los pines para el conector RJ45 que en principio tiene mejor inmunidad a interferencia arriba de 100Mbps es el T568A.1 2 3 (Areas, 2009)

2.3.7.11. CONECTOR RJ 45

El conector RJ45 es uno de los conectores principales utilizados con tarjeta de red Ethernet que transmite información a través de cables de par trenzado. Por este motivo, a veces se le denominado puerto Ethernet.

Es utilizada comúnmente con estándares como TIA/EIA-568-B, que define la disposición de los pines (patillaje) o wiring pinout.

2.3.7.12. SOFTWARE CONFIGTOOL

(dahua technology, 2010-2015)El software configtool nos proporciona dahua tiene como características principal las siguientes funciones:

- Ver imagen de la cámara y actualizar la configuración de codificación de color
- Configuración de las cámara IP desde la computadora
- Llevar a cabo actualización masivas de firmware dela cámara y NVR
- Nos permite verificar y/o confirmar la configuración de cada cámara que contiene nuestro equipo, lo que podemos realizar las modificaciones de, video, red, resoluciones, información, etc.

2.3.7.13. SOFTWARE SMARTPSS

Smartpss es un software gratuito de dahua para conectarse a sus equipos desde ordenadores Windows y Mac sirve para conectar a grabadores (High Definition Composite Video Interface HDCVI) Dahua, NVRs Dahua, cámara IP, etc. (dahua technology, 2010-2015)

2.3.8. METODOLOGIA

La metodología utilizada para el desarrollo de este proyecto es, la metodología modelo funcional para la administración de redes, estos modelos detallan las tareas y funciones que deben ser ejecutadas en el proceso de administración de redes.

2.3.8.1. Administración de redes.

El término administración de redes es definido como la suma total de todas las políticas, procedimientos que intervienen en la planeación, configuración, control, monitoreo de los elementos que conforman a una red con el fin de asegurar el eficiente y efectivo empleo de sus recursos. Lo cual se verá reflejado en la calidad de los servicios ofrecidos.

2.3.8.2. Dimensiones de la administración de redes.

Las dimensiones de la administración de red se enfocan de la siguiente manera:

Dimensión Funcional. Se refiere a la asignación de tareas de administración por medio de áreas funcionales.

Dimensión Temporal. Se refiere a dividir el proceso de administración en diferentes fases cíclicas, incluyendo las fases de planeación, implementación y operación.

Dimensión del escenario. Se refiere al resto de los escenarios adicionales al de administración de redes, como son administración de sistemas, administración de aplicaciones, etc.

2.3.8.3. DESARROLLO DE LA METODOLOGÍA

Se sugiere la creación de las siguientes áreas funcionales para ser aplicadas en la administración de redes.

2.3.8.3.1. Administración de la configuración

A continuación se describen las actividades ubicadas dentro del proceso de la administración de la configuración. Estas actividades son la planeación y diseño de la red; la instalación y administración del software; administración de hardware, y el aprovisionamiento. Por último se mencionan los procedimientos y políticas que pueden ser de ayuda para el desarrollo de esta área.

- **Planeación y diseño de la red.** La meta de esta actividad es satisfacer los requerimientos inmediatos y futuros de la red, reflejarlos en su diseño hasta llegar a su implementación.

  El proceso de planeación y diseño de una red contempla varias etapas, algunas son:

a) Reunir las necesidades de la red. Las cuales pueden ser específicas o generales, tecnológicas, cuantitativas, etc. Algunas de las necesidades específicas y de índole tecnológico de una red pueden ser:
   - Multicast,
   - Voz sobre IP (VoIP),
   - Calidad de servicio (QoS), etc.
   - Algunas necesidades cuantitativas pueden ser

- Cantidad de nodos en un edificio
- Cantidad de switches necesarios para cubrir la demanda de nodos.

Este tipo de requerimientos solamente involucran una adecuación en el diseño de la red, no requiere de un rediseño completo, en el caso de alguna necesidad más general puede requerir de un cambio total en la red ya que en estos casos los cambios afectan a gran parte del diseño. Una necesidad general, por ejemplo, se presenta cuando se desea la implementación de nuevas tecnologías de red como el cambiar de ATM a GigabitEthernet, o cambiar los protocolos de ruteo interno.

b) Diseñar la topología de la red
c) Determinar y seleccionar la infraestructura de red basada en los requerimientos técnicos y en la topología propuesta.
d) Diseñar, en el caso de redes grandes, la distribución del tráfico mediante algún mecanismo de ruteo, estático o dinámico.
e) Si el diseño y equipo propuesto satisfacen la necesidades, se debe proceder a planear la implementación, en caso contrario, repetir los pasos anteriores hasta conseguir el resultado esperado.

2.3.8.3.2. Selección de la infraestructura de red.

Esta selección se debe realizar de acuerdo a las necesidades y la topología propuesta. Si se propuso un diseño jerárquico, se deben seleccionar los equipos adecuados para las capas de acceso, distribución y núcleo (core). Además, la infraestructura debe cumplir con la mayoría de las necesidades técnicas de la red. Lo mas recomendable es hacer un plan de pruebas previo al cual deben ser sujetos todos los equipos que pretendan ser adquiridos.

2.3.8.3.3. Instalaciones y Administración del software.

El objetivo de estas actividades es conseguir un manejo adecuado de los recursos de hardware y software dentro de la red.

- **Instalaciones de hardware**

Las tareas de instalación de hardware contemplan, tanto la agregación como la sustitución de equipamiento, y abarcan un dispositivo completo, como un switch o un ruteador; o solo una parte de los mismos, como una tarjeta de red, tarjeta procesadora, un módulo, etc. El proceso de instalación consiste de las siguientes etapas:

Realizar un estudio previo para asegurar que la parte que será instalada es compatible con los componentes ya existentes.

Definir la fecha de ejecución y hacer un estimado sobre el tiempo de duración de cada paso de la instalación.

Notificar anticipadamente a los usuarios sobre algún cambio en la red.

Generalmente, a toda instalación de hardware corresponde una instalación o configuración en la parte de software, entonces es necesario coordinar esta configuración.

Generar un plan alterno por si la instalación provoca problemas de funcionalidad a la red.

Realizar la instalación procurando cumplir con los límites temporales previamente establecidos.

Documentar el cambio para futuras referencias.

- **Administración del software.**

  Es la actividad responsable de la instalación, desinstalación y actualización de una aplicación, sistema operativo o funcionalidad en los dispositivos de la red. Además, de mantener un control sobre los programas que son creados para obtener información específica en los dispositivos.

  Antes de realizar una instalación, se debe tomar en cuenta lo siguiente.

Que las cantidades de memoria y almacenamiento sean suficientes para la nueva entidad de software.

Asegurar que no exista conflicto alguno, entre las versiones actuales y las que se pretenden instalar.

Otra actividad importante es el respaldo frecuente de las configuraciones de los equipos de red ya que son un elemento importante que requieren especial cuidado. Estos respaldos son de mucha utilidad cuando un equipo se daña y tiene que ser reemplazado ya que no es necesario realizar la configuración nuevamente, lo que se hace es cargar la configuración al dispositivo mediante un servidor de FTP.

2.3.8.3.4. Provisionamiento

Esta tarea tiene la función de asegurar la redundancia de los elementos de software y hardware más importantes de la red. Puede llevarse a cabo en diferentes niveles, a nivel de la red global o de un elemento particular de la red. Es la responsable de abastecer los recursos necesarios para que la red funcione, elementos físicos como conectores, cables, multiplexores, tarjetas, módulos, elementos de software como versiones de sistema operativo, parches y aplicaciones. Además de hacer recomendaciones para asegurar que los recursos, tanto de hardware como de software, siempre se encuentren disponibles ante cualquier eventualidad.

Algunos elementos de hardware más importantes como son: tarjetas procesadoras, fuentes de poder, módulos de repuesto, equipos para sustitución y un respaldo de cada uno de ellos.

2.3.8.3.5. Políticas y procedimientos relacionados

En este apartado se recomienda realizar, entre otros, los siguientes procedimientos y políticas.

- Procedimiento de instalación de aplicaciones más utilizadas.
- Políticas de respaldo de configuraciones.

- Procedimiento de instalación de una nueva versión de sistema operativo.

2.3.8.4. Administración del rendimiento

Tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo al comportamiento encontrado.

La administración del rendimiento se divide en 2 etapas: monitoreo y análisis.

2.3.8.4.1. Monitoreo

El monitoreo consiste en observar y recolectar la información referente al comportamiento de la red en aspectos como los siguientes:

a) Utilización de enlaces

Se refiere a las cantidades ancho de banda utilizada por cada uno de los enlaces de área local (Ethernet, Fastethernet, GigabitEthernet, etc), ya sea por elemento o de la red en su conjunto.

b) Caracterización de tráfico.

Es la tarea de detectar los diferentes tipos de tráfico que circulan por la red, con el fin de obtener datos sobre los servicios de red, como http, ftp, que son más utilizados. Además, esto también permite establecer un patrón en cuanto al uso de la red.

c) Porcentaje de transmisión y recepción de información.

Encontrar los elementos de la red que más solicitudes hacen y atienden, como servidores, estaciones de trabajo, dispositivos de interconexión, puertos y servicios.

d) Utilización de procesamiento

Es importante conocer la cantidad de procesador que un servidor está consumiendo para atender una aplicación.

Esta propuesta considera importante un sistema de recolección de datos en un lugar estratégico dentro de la red, el cual puede ser desde una solución comercial como Spectrum o la solución propia de la infraestructura de red, hasta una solución integrada con productos de software libre.

2.3.8.4.2. Análisis.

Una vez recolectada la información mediante la actividad de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a mejorar su desempeño.

En el proceso de análisis se pueden detectar comportamientos relacionados a lo siguiente:

a) Utilización elevada.

Si se detecta que la utilización de un enlace es muy alta, se puede tomar la decisión de incrementar su ancho de banda o de agregar otro enlace para balancear las cargas de tráfico. También, el incremento en la utilización, puede ser el resultado de la saturación por tráfico generado maliciosamente, en este caso de debe contar con un plan de respuesta a incidentes de seguridad.

b) Tráfico inusual.

El haber encontrado, mediante el monitoreo, el patrón de aplicaciones que circulan por la red, ayudará a poder detectar tráfico inusual o fuera del patrón, aportando elementos importantes en la resolución de problemas que afecten el rendimiento de la red.

c) Elementos principales de la red.

Un aspecto importante de conocer cuáles son los elementos que más reciben y transmiten, es el hecho de poder identificar los elementos a los cuales establecer un monitoreo más constante, debido a que seguramente son de importancia. Además, si se detecta un elemento que generalmente no se encuentra dentro del patrón de los equipos con más actividad, puede ayudar a la detección de posibles ataques a la seguridad de dicho equipo.

d) Calidad de servicio.

Otro aspecto, es la Calidad de servicio o QoS, es decir, garantizar, mediante ciertos mecanismos, las condiciones necesarias, como ancho de banda, retardo, a aplicaciones que requieren de un trato especial, como lo son la voz sobre IP (VoIP), el video sobre IP mediante H.323, etc.

e) Control de tráfico.

El tráfico puede ser reenviado o ruteado por otro lado, cuando se detecte saturación por un enlace, o al detectar que se encuentra fuera de servicio, esto se puede hacer de manera automática si es que se cuenta con enlaces redundantes.

Si las acciones tomadas no son suficientes, éstas se deben reforzar para que lo sean, es decir, se debe estar revisando y actualizando constantemente.

2.3.8.4.3. Interacción con otras áreas

La administración del rendimiento se relaciona con la administración de fallas cuando se detectan anomalías en el patrón de tráfico dentro de la red y cuando se detecta saturación en los enlaces. Con la administración de la seguridad, cuando se detecta tráfico que es generado hacia un solo elemento de la red con más frecuencia que la común. Y con la administración de la

configuración, cuando ante una falla o situación que atente contra el rendimiento de la red, se debe realizar alguna modificación en la configuración de algún elemento de la red para solucionarlo.

2.3.8.5. Administración de fallas

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para reestablecer la situación o minimizar el impacto de la falla.

El proceso de la administración de fallas consiste de distintas fases.

- *Monitoreo de alarmas*. Se realiza la notificación de la existencia de una falla y del lugar donde se ha generado. Esto se puede realizar con el auxilio de las herramientas basadas en el protocolo SNMP.
- *Localización de fallas*. Determinar el origen de una falla.
- *Pruebas de diagnóstico*. Diseñar y realizar pruebas que apoyen la localización de una falla.
- *Corrección de fallas*. Tomar las medidas necesarias para corregir el problema, una vez que el origen de la misma ha sido identificado.
- *Administración de reportes.* Registrar y dar seguimiento a todos los reportes generados por los usuarios o por el mismo administrador de la red.

Una falla puede ser notificada por el sistema de alarmas o por un usuario que reporta algún problema.

2.3.8.5.1. Monitoreo de alarmas

Las alarmas son un elemento importante para la detección de problemas en la red. Es por eso que se propone contar con un sistema de alarmas, el cual es una herramienta con la que el administrador se auxilia para conocer que existe un problema en la red. También conocido como sistema de monitoreo, se trata

de un mecanismo que permite notificar que ha ocurrido un problema en la red. Esta propuesta se basa en la utilización de herramientas basadas en el protocolo estándar de monitoreo, SNMP, ya que este protocolo es utilizado por todos los fabricantes de equipos de red.

Cuando una alarma ha sido generada, ésta debe ser detectada casi en el instante de haber sido emitida para poder atender el problema de una forma inmediata, incluso antes de que el usuario del servicio pueda percibirla.

Las alarmas pueden ser caracterizadas desde al menos dos perspectivas, su tipo y su severidad.

Tipo de las alarmas

- *Alarmas en las comunicaciones*. Son las asociadas con el transporte de la información, como las pérdidas de señal.
- *Alarmas de procesos*. Son las asociadas con las fallas en el software o los procesos, como cuando el procesador de un equipo excede su porcentaje normal.
- *Alarmas de equipos.* Como su nombre lo indica, son las asociadas con los equipos. Una falla de una fuente de poder, un puerto, son algunos ejemplos.
- *Alarmas ambientales*. Son las asociadas con las condiciones ambientales en las que un equipo opera. Por ejemplo, alarmas de altas temperaturas.
- *Alarmas en el servicio*. Relacionadas con la degradación del servicio en cuanto a límites predeterminados, como excesos en la utilización del ancho de banda, peticiones abundantes de icmp.

Severidad de las alarmas.

- *Crítica.* Indican que un evento severo ha ocurrido, el cual requiere de atención inmediata. Se les relaciona con fallas que afectan el funcionamiento global de la red. Por ejemplo, cuando un enlace

importante está fuera de servicio, su inmediato restablecimiento es requerido.

- *Mayor*. Indica que un servicio ha sido afectado y se requiere su inmediato restablecimiento. No es tan severo como el crítico, ya que el servicio se sigue ofreciendo aunque su calidad no sea la óptima.
- *Menor*. Indica la existencia de una condición que no afecta el servicio pero que deben ser tomadas las acciones pertinentes para prevenir una situación mayor. Por ejemplo, cuando se alcanza cierto límite en la utilización del enlace, no indica que el servicio sea afectado, pero lo será si se permite que siga avanzando.
- *Indefinida.* Cuando el nivel de severidad no ha sido determinado por alguna razón.

2.3.8.5.2. Localización de fallas.

Este segundo elemento de la administración de fallas es importante para identificar las causas que han originado una falla. La alarma indica el lugar del problema, pero las pruebas de diagnóstico adicionales son las que ayudan a determinar el origen de la misma. Una vez identificado el origen, se tienen que tomar las acciones suficientes para reparar el daño.

- *Pruebas de diagnóstico*

Las pruebas de diagnóstico son medios importantes para determinar el origen de una falla. Algunas de estas pruebas de diagnóstico que se pueden realizar.

- Pruebas de conectividad física.

Son pruebas que se realizan para verificar que los medios de transmisión se encuentran en servicio, si se detecta lo contrario, tal vez el problema es el mismo medio.

- *Pruebas de conectividad lógica.*

Son pruebas que ofrecen una gran variedad, ya que pueden ser punto a punto, o salto por salto. Las pruebas punto a punto se realizan entre entidades finales,

y las salto por salto se realizan entre la entidad origen y cada elemento intermedio en la comunicación. Los comandos usualmente utilizados son “ping” y “traceroute”.

- *Pruebas de medición***.**

Esta prueba va de la mano con la anterior, donde, además de revisar la conectividad, se prueban los tiempos de respuesta en ambos sentidos de la comunicación, la pérdida de paquetes, la ruta que sigue la información.

2.3.8.5.3. Corrección de fallas.

Es la etapa donde se recuperan las fallas, las cuales pueden depender de la tecnología de red. En esta propuesta solo se mencionan las prácticas referentes a las fallas al nivel de la red.

- *Entre los mecanismos más recurridos*, y que en una red basada en interruptores son aplicables, se encuentran los siguientes.
- *Reemplazo de recursos dañados*. Hay equipos de red que permiten cambiar módulos en lugar de cambiarlo totalmente.
- *Aislamiento del problema*. Aislar el recurso que se encuentra dañado y que, además, afecta a otros recursos es factible cuando se puede asegurar que el resto de los elementos de la red pueden seguir funcionando.
- *Redundancia.* Si se cuenta con un recurso redundante, el servicio se cambia hacia este elemento.
- *Recarga del sistema*. Muchos sistemas se estabilizan si son reiniciados.
- *Instalación de software*. Sea una nueva versión de sistema operativo, una actualización, un parche que solucione un problema específico, etc.
- *Cambios en la configuración*. También es algo muy usual cambiar algún parámetro en la configuración del elemento de la red.

2.3.8.6. Administración de reportes

Es la etapa de documentación de las fallas. Cuando un problema es detectado o reportado, se le debe asignar un número de reporte para su debido seguimiento, desde ese momento un reporte queda abierto hasta que es corregido. Este es un

medio para que los usuarios del servicio puedan conocer el estado actual de la falla que reportaron.

El ciclo de vida de la administración de reportes se divide en cuatro áreas, de acuerdo a la recomendación X.790 de la ITU-T.

Creación de reportes

Un reporte es creado después de haber recibido una notificación sobre la existencia de un problema un problema en la red, ya sea por una alarma, una llamada telefónica de un usuario, por correo electrónico o por otros medios. Cuando se crea un reporte de be contener al menos la siguiente información:

- El nombre de la persona que reportó el problema
- El nombre de la persona que atendió el problema o que creó el reporte del mismo.
- Información técnica para ubicar el área del problema
- Comentarios acerca de la problemática.
- Fecha y hora del reporte

Seguimiento a reportes

La administración de reportes debe permitir al administrador dar seguimiento de cada acción tomada para solucionar el problema, y conocer el estado histórico y actual del reporte. Para cada reporte debe mantenerse un registro de toda la información relacionada al mismo: pruebas de diagnóstico, como fue solucionado el problema, tiempo que llevó la solución, etc, y esta debe poder ser consultada en cualquier momento por el administrador.

Manejo de reportes

El administrador debe ser capaz de tomar ciertas acciones cuando un reporte está en curso, como escalar el reporte, solicitar que sea cancelado un reporte que no ha sido cerrado aún, poder hacer cambios en los atributos del reporte, como lo es

el teléfono de algún contacto, poder solicitar hora y fecha de la creación o finalización de un reporte, etc.

Finalización de reportes

Una vez que el problema reportado ha sido solucionado, el administrador o la gente responsable del sistema de reportes, debe dar por cerrado el reporte. Una práctica importante, es que antes de cerrar un reporte el administrador debe asegurarse que efectivamente el problema reportado ha sido debidamente corregido.

2.3.8.7. Administración de la contabilidad

Es el proceso de recolección de información acerca de los recursos utilizados por los elementos de la red, desde equipos de interconexión hasta usuarios finales. Esto se realiza con el objetivo de realizar los cobros correspondientes a los clientes del servicio mediante tarifas establecidas. Este proceso, también llamado tarificación, es muy común en los proveedores de servicio de Internet o ISP.

2.3.8.8. Administración de la seguridad

Su objetivo es ofrecer servicios de seguridad a cada uno de los elementos de la red así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques, así como para la respuesta ante incidentes de seguridad.

2.3.8.8.1. Prevención de ataques

El objetivo es mantener los recursos de red fuera del alcance de potenciales usuarios maliciosos. Una acción puede ser la implementación de alguna estrategia de control de acceso. Obviamente, los ataques solamente se reducen pero nunca se eliminan del todo.

2.3.8.8.2. Detección de intrusos

El objetivo es detectar el momento en que un ataque se esta llevando a cabo. Hay diferentes maneras en la detección de ataques, tantas como la variedad de ataques mismo. El objetivo de la detección de intrusos se puede lograr mediante un sistema de detección de intrusos que vigile y registre el tráfico

que circula por la red apoyado en un esquema de notificaciones o alarmes que indiquen el momento en que se detecte una situación anormal en la red.

2.3.8.8.3. Respuesta a incidentes

El objetivo es tomar las medidas necesarias para conocer las causas de un compromiso de seguridad en un sistema que es parte de la red, cuando éste hay sido detectado, además de tratar de eliminar dichas causas.

2.3.8.8.4. Políticas de Seguridad

La meta principal de las políticas de seguridad es establecer los requerimientos recomendados para proteger adecuadamente la infraestructura de cómputo y la información ahí contenida. Una política debe especificar los mecanismos por los cuales estos requerimientos deben cumplirse. El grupo encargado de ésta tarea debe desarrollar todas las políticas después de haber hecho un análisis profundo de las necesidades de seguridad.

Entre otras, algunas políticas necesarias son:

- Políticas de uso aceptable
- Políticas de cuentas de usuario
- Políticas de configuración de ruteadores
- Políticas de listas de acceso
- Políticas de acceso remoto.
- Políticas de contraseñas.
- Políticas de respaldos.

2.3.8.8.5. Servicios de seguridad

Los servicios de seguridad definen los objetivos específicos a ser implementados por medio de mecanismos de seguridad. Identifica el “que”.

De acuerdo a la Arquitectura de Seguridad OSI, un servicio de seguridad es una característica que debe tener un sistema para satisfacer una política de seguridad.

La arquitectura de seguridad OSI identifica cinco clases de servicios de seguridad:

- Confidencialidad
- Autenticación
- Integridad
- Control de acceso
- No repudio

Un paso importante es definir cuáles de estos servicios deben ser implementados para satisfacer los requerimientos de las políticas de seguridad.

2.3.8.8.6. Mecanismos de seguridad

Se deben definir las herramientas necesarias para poder implementar los servicios de seguridad dictados por las políticas de seguridad. Algunas herramientas comunes son: herramientas de control de acceso, cortafuegos (firewall), TACACS+ o RADIUS; mecanismos para acceso remoto como Secure shell o IPSec; Mecanismos de integridad como MD5, entre otras.

Todos estos elementos en su conjunto conforman el modelo de seguridad para una red de cómputo.

2.3.8.8.7. Proceso.

Para lograr el objetivo perseguido se deben, al menos, realizar las siguientes acciones:

Elaborar las políticas de seguridad donde se describan las reglas de administración de la infraestructura de red. Y donde además se definan las expectativas de la red en cuanto a su buen uso, y en cuanto a la prevención y respuesta a incidentes de seguridad.

Definir, de acuerdo a las políticas de seguridad, los servicios de necesarios y que pueden ser ofrecidos e implementados en la infraestructura de la red.

Implementar las políticas de seguridad mediante los mecanismos adecuados.

2.3.8.9. CONCLUSIONES

La administración de redes es la suma de todas las actividades de planeación y control, enfocadas a mantener una red eficiente y con altos niveles de disponibilidad. Dentro de estas actividades hay diferentes responsabilidades fundamentales como el monitoreo, la atención a fallas, configuración, la seguridad, entre otras.

Esto nos lleva a reconocer que una red debe contar con un sistema de administración aun cuando se crea que es pequeña, aunque es cierto que entre mayor sea su tamaño mas énfasis se debe poner en esta tarea.

En los puntos anteriores se describió una propuesta de administración para redes de datos. La propuesta se basó en la recomendación de la ITU-T, el modelo TMN y en el modelo OSI-NM de ISO. Se presentó una propuesta global que enfatiza en todos los aspectos relacionados a la buena operación de una red, como lo son el control sobre los sucesos en la red, la visualización de los tipos de tráfico, la detección y atención oportuna de problemas, aspectos de seguridad, etc.

La metodología presentada se basa en un modelo con tareas bien definidas y complementarias. Esta modularidad permite su mejor entendimiento y facilita su implementación y actualización.

2.4. HERRAMIENTAS UTILIZADAS

2.4.1. ANTENA DE RED INALAMBRICA

La antena es una herramienta que emite la señal. Existen dos familias de antenas, las omnidireccionales y las direccionales.

Las antenas omnidireccionales, recibe su nombre por la capacidad de emitir señales en todas las direcciones.

La antena direccional, es típica para estables enlaces punto a punto o para conectar a un nodo, se caracteriza por su alta ganancia que va desde unos discretos 15dbi,

llegando en los modelos superiores hasta los 24 dbi, cuanto más alta es la ganancia de este tipo de antenas, más alta es su direccionalidad, ya que reduce muchísimo el ángulo en el que irradia la señal, llegando a ser tan estrecho como 8 grados de apertura.

2.4.2. NVR

Es muy similar a un DVR, la diferencia es que el DVR digitaliza, graba y administra imágenes enviadas desde cámaras de seguridad analógicas, en cambio un NVR, graba y administra imágenes ya digitales las cuales son enviadas desde las cámaras IP a través de una Red.

Con el sistema IP las imágenes llegan procesadas al grabador. Se puede basar en un ordenador o sistema autónomo, se puede usar un cable UTP o incluso Wifi.

Se trata de un videograbador hibrido, ya que combina ambas tecnologías. Se incluye en entornos donde se aprovechan instalaciones analógicas y se recurre a la tecnología IP.

2.4.3. SWITCH

Es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la Red, debido al ancho de banda pequeños y embotellamientos.

El switch puede agregar mayor ancho de bandada, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto.

2.4.4. TPLINK

Es un adaptador inalámbrico de ala potencia de 300 Mbps que permite a los usuarios activar el PC o portátil con capacidad inalámbrica muy potente para ofrecer mejoras de rendimiento. El adaptador adopta el diseño de alta potencia que ofrece hasta diez veces la gama de adaptadores convencionales.

2.4.5. CAMARA IP

Las cámaras IP, son vídeo cámaras de vigilancia que tienen la particularidad de enviar las señales de video (y en muchos casos audio), pudiendo estar conectadas directamente a un Router ADSL, o bien a un concentrador de una Red Local, para

poder visualizar en directo las imágenes bien dentro de una red local (LAN), o a través de cualquier equipo conectado a Internet (WAN) pudiendo estar situado en cualquier parte del mundo.

A la vez, las cámaras IP permiten el envío de alarmas por medio de E-mail, la grabación de secuencias de imágenes, o de fotogramas, en formato digital en equipos informáticos situados tanto dentro de una LAN como de la WAN, permitiendo de esta forma verificar posteriormente lo que ha sucedido en el lugar o lugares vigilados.

Las cámaras IP actualmente se pueden instalar en cualquier sitio que disponga de conexión a Internet mediante Router ADSL o XDSL (Con dirección IP fija, aunque algunos modelos también permiten IP dinámica); incluso otros modelos de cámaras ip permiten que esa conexión no sea permanente y que cuando sea necesaria se pueda realizar por medio de un módem convencional a la línea telefónica básica.

2.4.6. CABLE UTP CATEGORIA 6ª

El cable UTP categoría 6ª, es un estándar de cable para gigabit, etheternet y otros protocolos de Redes que es retro compatible con los estándares de categoría 5, 5e y categoría 3. La categoría 6ª posee características y especificaciones para evitar la diafonía y el ruido.

2.4.7. CONECTOR RJ 45

El conector RJ45 es uno de los conectores principales utilizados con tarjeta de red Ethernet que transmite información a través de cables de par trenzado. Por este motivo, a veces se le denominado puerto Ethernet.

2.4.8. CRIMPADORA

Una crimpadora, también conocida como alicates de terminales, pinzas de compresión, tenaza de engastar tenaza de crimpar, o tenaza de crimpado es una herramienta utilizada para corrugar o crimpar dos piezas metálicas o de otros materiales maleables mediante la deformación de una o ambas piezas; esta deformación es lo que las mantiene unidas.

Esta técnica suele usarse para unir terminales con recubrimiento aislante, conectores (F, BNC, RJ11, RJ12, RJ455) y cables (coaxial, y de par trenzado) de telecomunicaciones. También los hay para fibra óptica.

2.4.9. SOFTWARE CONFIGTOOL

(dahua technology, 2010-2015)El software configtool nos proporciona dahua tiene como características principal las siguientes funciones:

Ver imagen de la cámara y actualizar la configuración de codificación de color

Configuración de las cámara IP desde la computadora

Llevar a cabo actualización masivas de firmware dela cámara y NVR

Nos permite verificar y/o confirmar la configuración de cada cámara que contiene nuestro equipo, lo que podemos realizar las modificaciones de, video, red, resoluciones, información, etc.

2.4.10. SOFTWARE SMARTPSS

(dahua technology, 2010-2015)Smartpss es un software gratuito de dahua para conectarse a sus equipos desde ordenadores Windows y Mac sirve para conectar a grabadores (High Definition Composite Video Interface HDCVI) Dahua, NVRs Dahua, cámara IP, etc. (dahua technology, 2010-2015)

El presente capitulo describe de acuerdo a la Metodología, los procesos que se aplican para la implementación del sistema de vigilancia y monitoreo de las aulas audiovisuales del bloque “G” del campus universitario de la Universidad Amazónica de Pando utilizando cámaras IPs.

CAPITULO III

MARCO APLICATIVO

3. MARCO APLICATIVO.

Para llevar a cabo la implementación del sistema de vigilancia y monitoreo de las aulas audiovisuales del bloque “G” del campus universitario de la Universidad Amazónica de Pando utilizando cámaras IPs, se realizó haciendo seguimiento a la Metodología Modelo Funcional para la Administración de Redes, la misma que se describe en el Marco Metodológico.

Cabe recalcar, que de las cinco áreas funcionales que forman parte de la metodología solo se tomó en cuenta cuatro de ellas, las cuales son:

1. **Administración de configuración**
2. **Administración de rendimiento**
3. **Administración de falla**
4. **Administración de seguridad**

3.1. ADMINISTRACIÓN DE LA CONFIGURACIÓN

A continuación se describen las actividades ubicadas dentro del proceso de la administración de la configuración. Estas actividades son: Planeación y diseño de la red, instalación y administración del software, administración de hardware.

3.1.1. Planeación y diseño de la red.

La meta de esta actividad es satisfacer los requerimientos inmediatos y futuros de la red, reflejarlos en su diseño hasta llegar a su implementación.

El proceso de planeación y diseño de una red contempla varias etapas, algunas son: *Reunir las necesidades de la red, Diseñar la topología de la red, Determinar y seleccionar la infraestructura, Diseñar, en el caso de redes grandes*

3.1.1.1. Reunir las necesidades de la red. Las cuales pueden ser específicas o generales, tecnológicas y cuantitativas.

A) Necesidades específicas o Generales:

Para la implementación del sistema de vigilancia y monitoreo se utilizaran los siguientes equipos y accesorios tecnológicos, los cuales son:

- Cámaras IP Modelo dh-ipc-hdw1220sn-0360b.

- NVR dahua modelo dhi-nrv4216

- Antena de red inalambrica NanoStation M5 Ubiquiti 5GHz Indoor/ Outodoor airmax 16dbi

- Switch D-LINK des-1016d

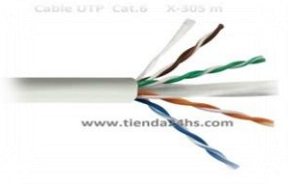
- CPU delux intel core(TM)i5-4460 CPU @ 3.20GHz .3.20 GHz memoria de 4.00GB sistemas operativo windows 7 ultimate de 64 bit

- TV irt led 2496 cmbblue tv led 24p

- Monitor samsung s19c150

- Conectores RJ45

- Cable utp categoría 6ª



B) Necesidades tecnológicas cuantitativas

Para la implementación del sistema de vigilancia y monitoreo se requerirá lo siguiente:

- 14 Camaras IP Modelp dh-ipc-hdw1220sn-0360b.
- 1 NVR dahua modelo dhi-nrv4216
- 2 DGS-1016D 16-Port Gigabit Unmanaged Desktop Switch
- 5 Antenas NanoStation M5 Ubiquiti 5GHz Indoor/ Outodoor airmax 16dbi cada 4camaras
    - 500 Metros de cable utp categoría 6ª
    - 40 Conectores RJ45
    - 4 Monitor samsung s19c150
- 4 delux intel core(TM)i5-4460 CPU @ 3.20GHz .3.20 GHz memoria de 4.00GB sistemas operativo windows 7 ultimate de 64 bit.

3.1.1.2. Diseñar la topología de la red:

A) La topología utilizada para la implementación de las cámaras IP en las aulas del bloque "G" es la Topología Estrella**.**

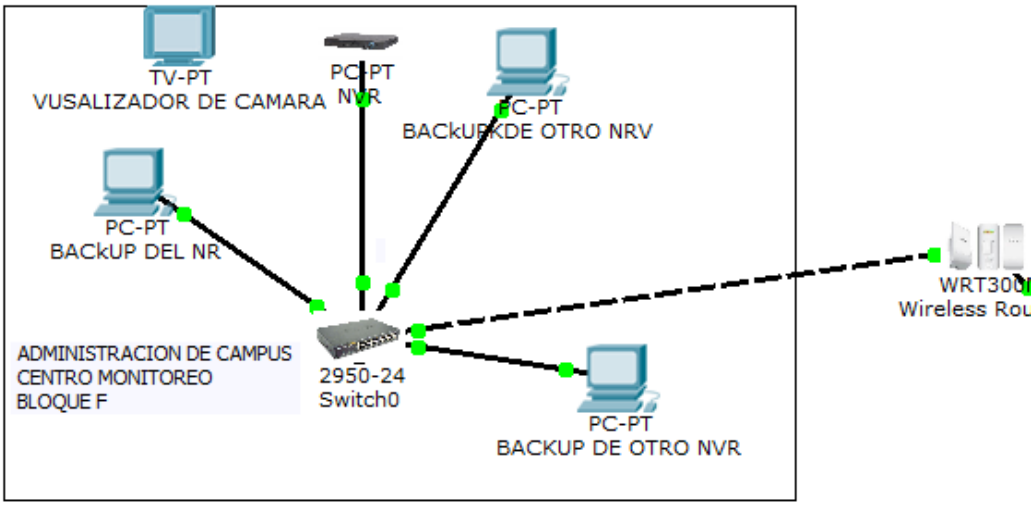


FIGURA Nº 1 : DISEÑO RED DEL CENTRO DE MONITOREO
AUTOR: FUENTE PROPIA

B) La topología utilizada para la comunicación de las computadoras en el centro de vigilancia y monitoreo es la topología estrella.

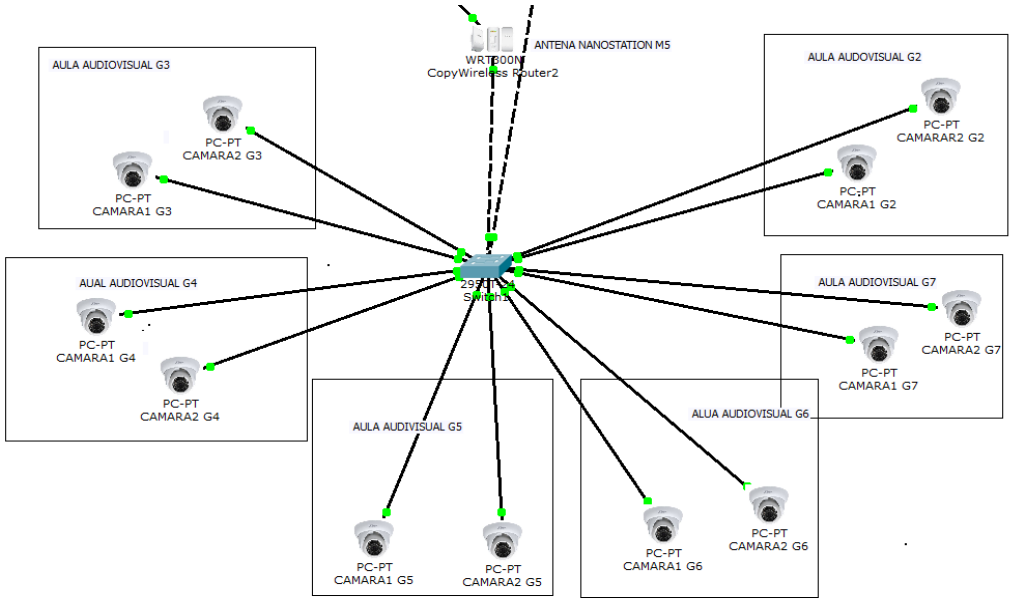


FIGURA Nº 2 : DISEÑO DE RED DEL BLOQUE "G"
AUTOR: FUENTE PROPIA

C) La topología utilizada para la comunicación entre el bloque “G” y el centro de vigilancia y monitoreo es la topología AP – Cliente (BRIDGES)

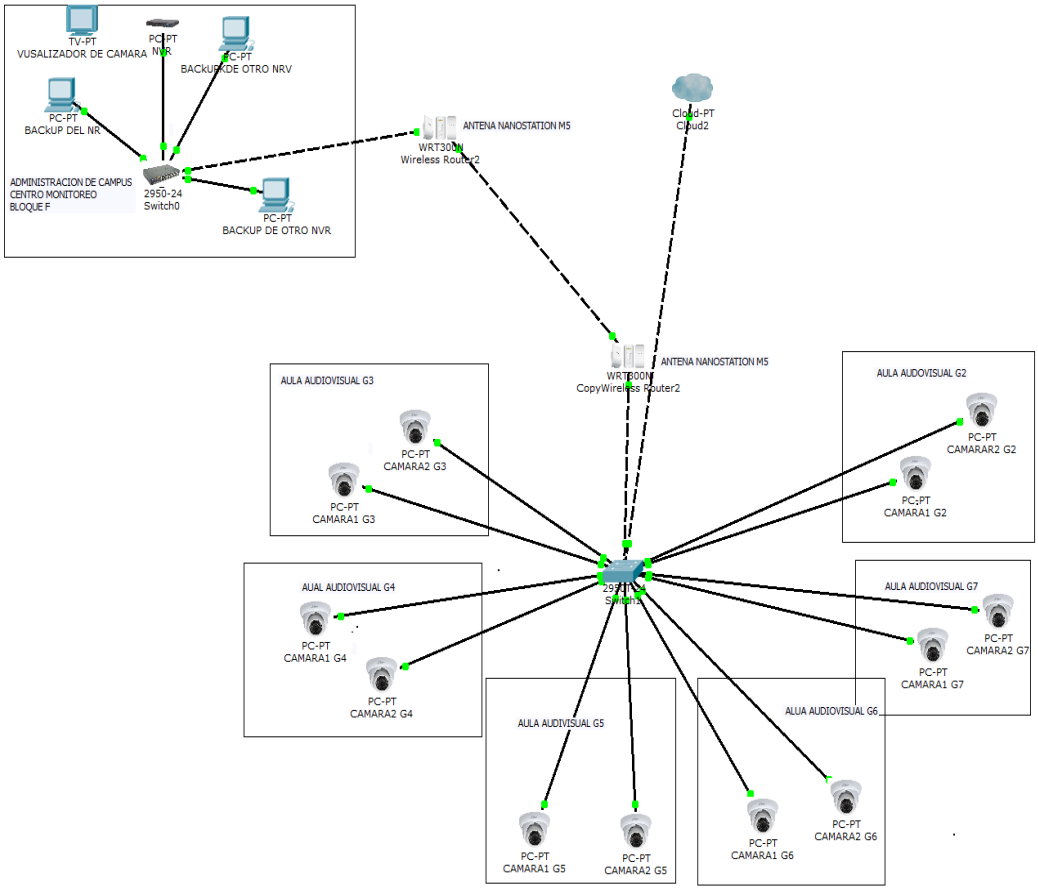


FIGURA Nº 3: DISEÑO DEL SISTEMA DE VIGILANCIA Y MONITOREO
AUTOR: FUENTE PROPIA

3.1.1.3. Determinar y seleccionar la infraestructura:

En esta parte se seleccionara la infraestructura a ser monitorizada donde estarán ubicadas las cámaras IP y también se seleccionara la infraestructura donde será el centro de vigilancia y monitoreo.

- Selección infraestructura a ser monitorizada
- Selección infraestructura centro de vigilancia y monitoreo

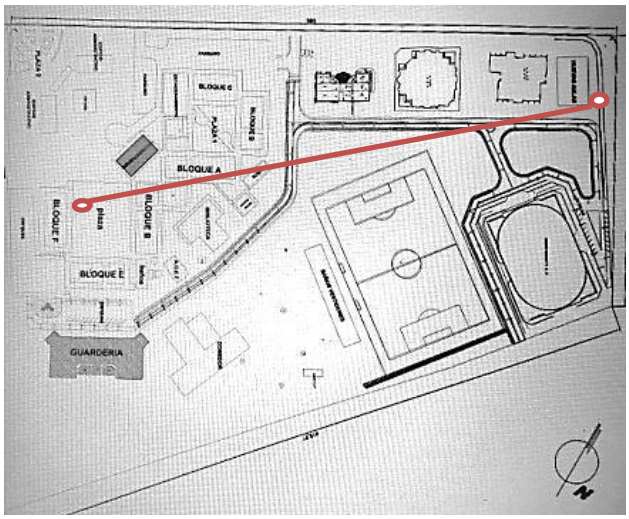


FIGURA Nº 4 : IMAGEN DEL SELECCIÓN DE LA VIGILANCIA Y EL MONITOREO
AUTOR: FUENTE PROPIA

d) **Diseñar:**

En esta parte se hará el diseño de la red entre que se comunica el bloque "G" y el centro de vigilancia y monitoreo, el mismo que es la topología BRIDGE, utilizando antenas de red inalámbrica.

3.1.2. Instalaciones y Administración del software.

El objetivo de estas actividades es conseguir un manejo adecuado de los recursos de hardware y software dentro de la red.

3.1.2.1 Instalaciones de hardware

En esta parte se contempla toda la parte hardware que se utilizó para la implementación del sistema de vigilancia y monitoreo de las aulas del bloque "G", la misma que se divide en dos y esta son las siguientes:

a) Aulas del Bloque "G": En estas aulas se instaló los siguientes equipos hardware:

- Cámaras IP Modelo dh-ipc-hdw1220sn-0360b.
- Switches D-LINK des-1016d
- Cableado UTP categoría 6ª

- Acometida de energía eléctrica
- Antena de red inalámbrica NanosTation M5 Ubiquuiti 5GHz Indor/ Outodoor armax 16dbi

Toda la implementación de la parte hardware se hizo de acuerdo al diseño de la red.

FOTOS Nº 1: INSTALACIÓN DE LA CHAMARA IP EN EL BLOQUE "G"
FUENTE: ELABORACIÓN PROPIA

b) Centro de Vigilancia y Monitoreo: En el Centro de Monitoreo se Instaló los siguientes equipos hardware.

- NVR marca dahua modelo dhi-nrv4216
- CPU delux Intel core (TM)i5-4460 de 3.20 GHz, memoria de 4.00 GB, sistema operativo Windows 7 de 64 bit.
- Monitor Samsung s19 c150.
- Tv irt led 2496 cmbblue tv led 24 p

- Antena de red inalámbrica NanosTation M5 Ubiquuiti 5GHz Indor/ Outodoor armax 16dbi

- Cableado UTP categoría 6ª
- Acometida de energía eléctrica
- Toda la implementación de la parte hardware se hizo de acuerdo al diseño de la red.

FOTOS Nº 2: CENTRO DE MONITOREO
FUENTE: ELABORACIÓN PROPIA

3.1.2.2. Administración del Software.

3.1.2.2.1. Instalación de la cámara IP:

a) El primer paso es colocar CD de instalación que viene en cada cámara IP Modelo dh-ipc-hdw1220sn-0360b software

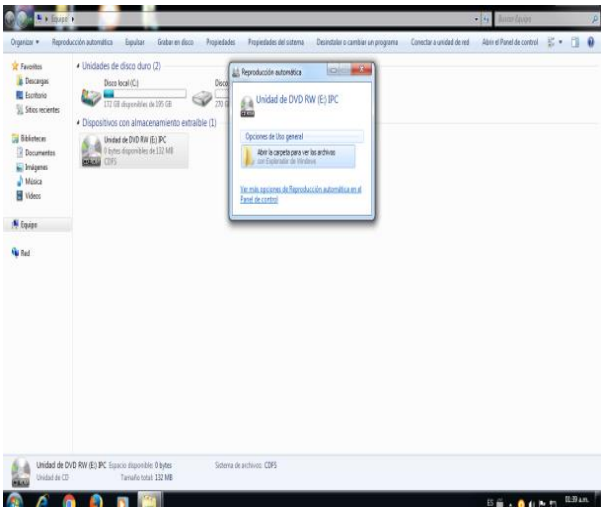


IMAGEN Nº 1: INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

b) Al abrir el CD seleccionamos la carpeta donde está el software configtool:

- Abrir carpeta tool y encontraremos un comprimido con el nombre carpeta dh-configtool_eng_v2.00.0.R.140410.rar lo abrimos o descomprimimos
    - Al abrir o desprimir el archivo dh-configtool_eng_v2.00.0.R.140410.rar apacera el ejecutable .exe con el mismo nombre.

IMAGEN Nº 2 : INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

c) El instalador aparecerá como una ventana con su presentación de una computadora y una lupa en la parte inferior izquierda esta los botones NEXT y CANCEL da clic en NEXT.

IMAGEN Nº 3: INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

d) En esta ventana parecerá todo los términos que tiene el software de instalación dh-configtool_eng_v2.00.0.R.140410.

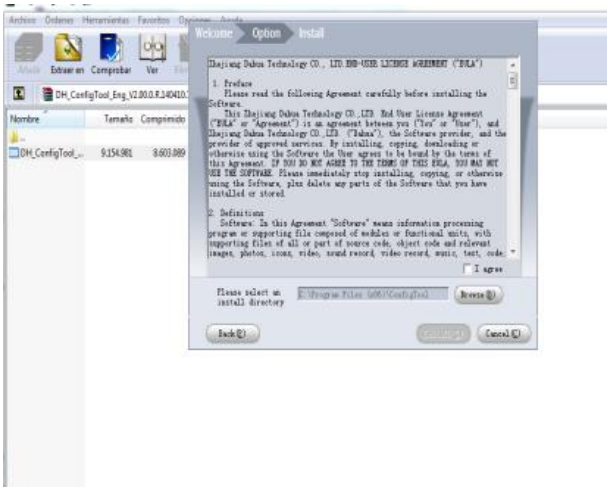


IMAGEN Nº 4: INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

e) Dar tickear la casilla I agree los términos de instalación y dar siguiente a la instalación dh-configtool_eng_v2.00.0.R.140410.

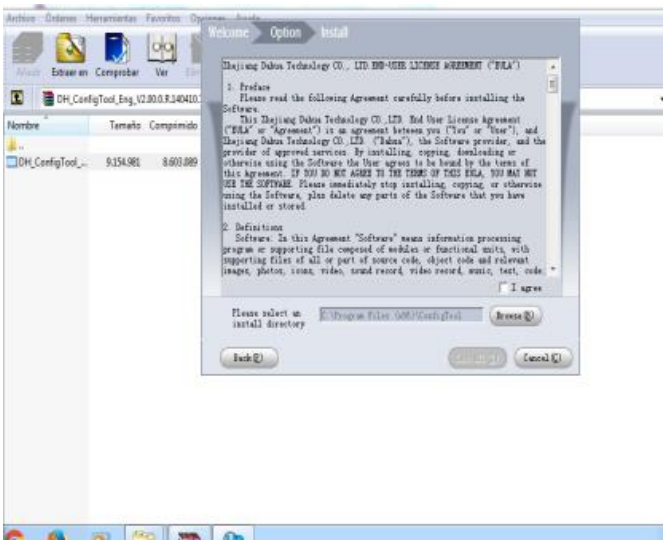


IMAGEN Nº 5: INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

f) Ser cargara la instalación de software dh-configtool_eng_v2.00.0.R.140410.

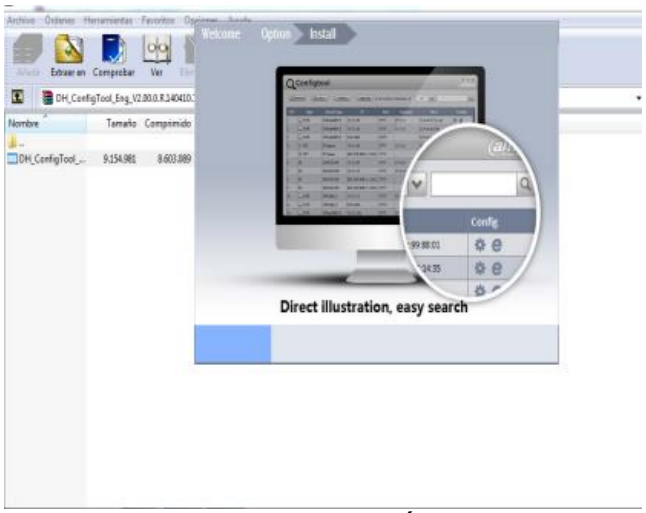


IMAGEN Nº 6: INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

g) Aparcera un mensaje de instalación completa del software dh-configtool_eng_v2.00.0.R.140410el cual muestra un signo de bien al terminar.

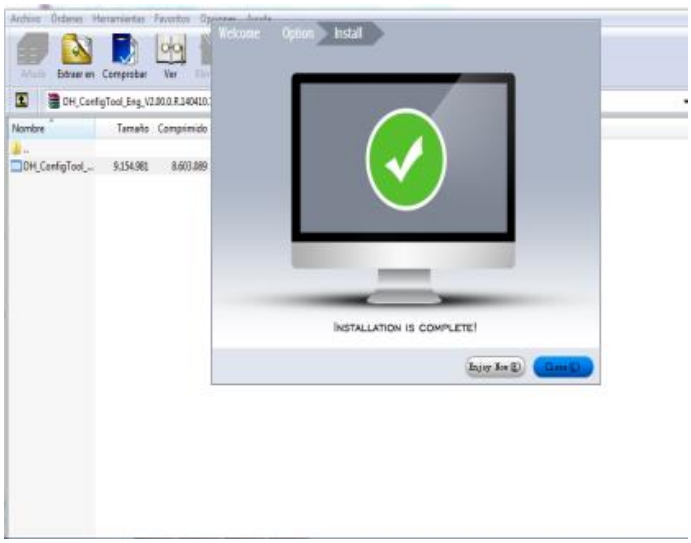


IMAGEN Nº 7: INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

h) Como finalización de la instalación de la herramienta de configuración de cámara ip, dar en el botón cerrar del software dh-configtool_eng_v2.00.0.R.140410.

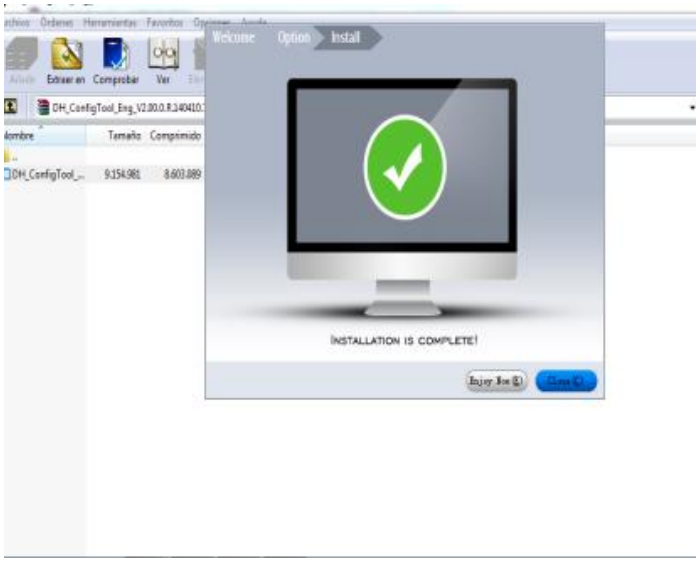


IMAGEN Nº 8: INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

i) Una vez instalado del software dh-configtool_eng_v2.00.0.R.140410 aparcera en el escritorio de la computadora un icono de una lupa mostrado la sigla IP abrir haciendo doble click el icono.

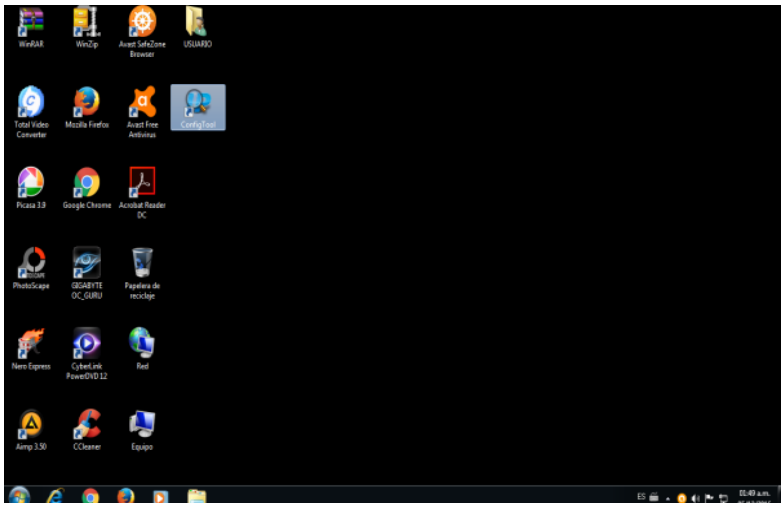


IMAGEN Nº 9 INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

3.1.2.1.3. CONFIGURACION DE LAS CAMARA IP EN EL SOFTWARE DH-CONFIGTOOL_ENG_V2.00.0.R.140410

10.- Al iniciar el software aparecerá en la pantalla automáticamente las cámaras IP y NRV que están conectadas a la red local o dispositivo directamente.

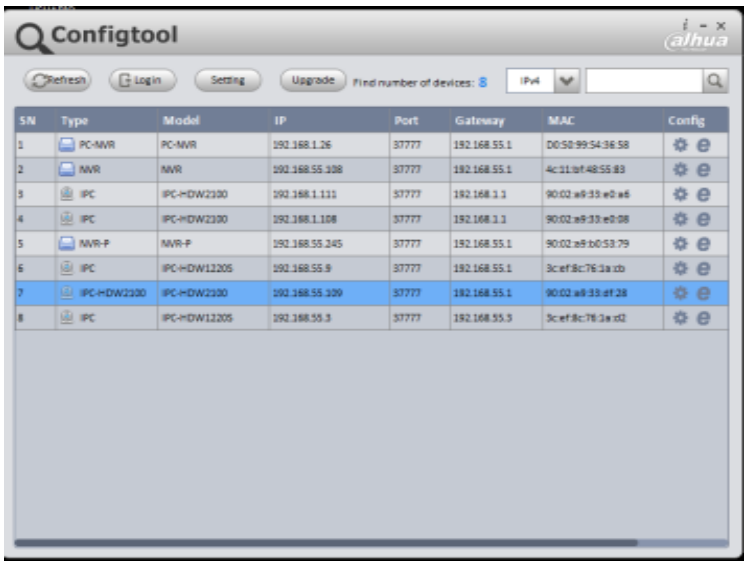


IMAGEN Nº 10: INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

11.- En este paso seleccionaremos las cámaras ip con el modelo dahua IPC-HDW-1220S para proceder a la configuración de la misma.

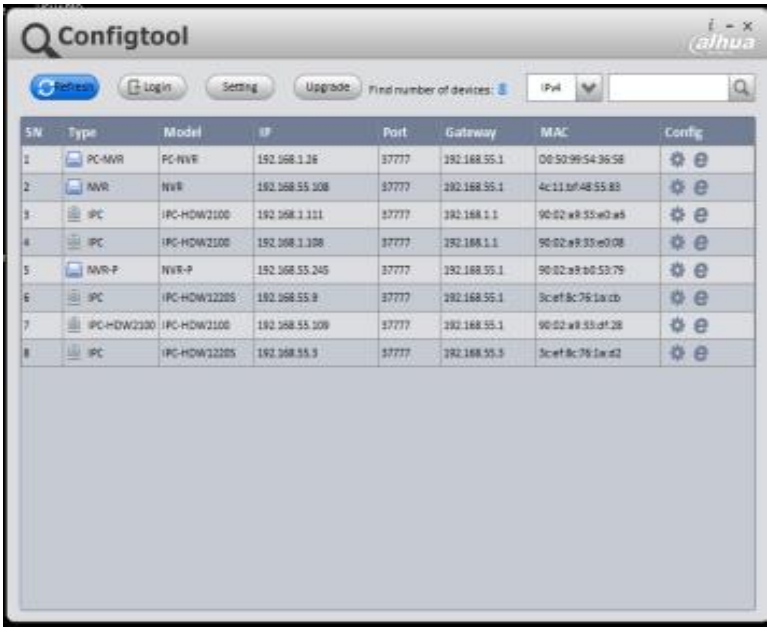


IMAGEN Nº 11: INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

12.- Seleccionar el icono de configuración el cual nos abrirá la ventana de configuración de cámara ip dahua IPC-HDW-1220S.

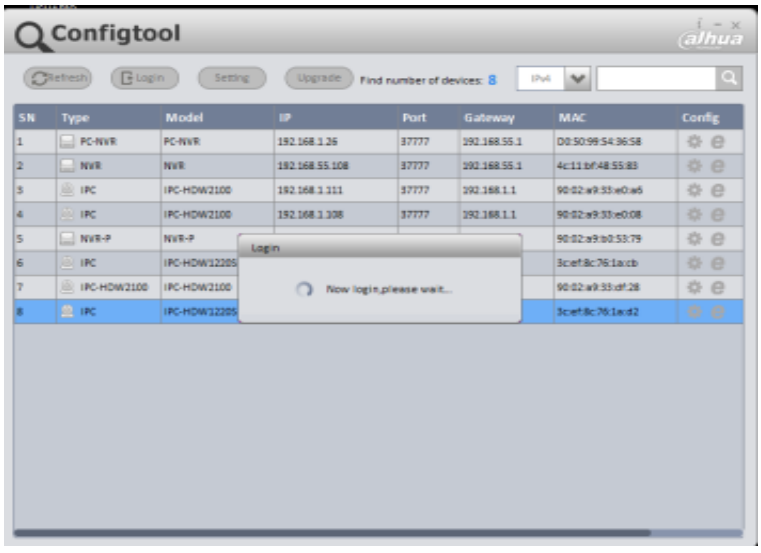


IMAGEN Nº 12: INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

13.- En esta ventana nos muestra el acceso login para la configuración de la cámara ip dahua IPC-HDW-1220S

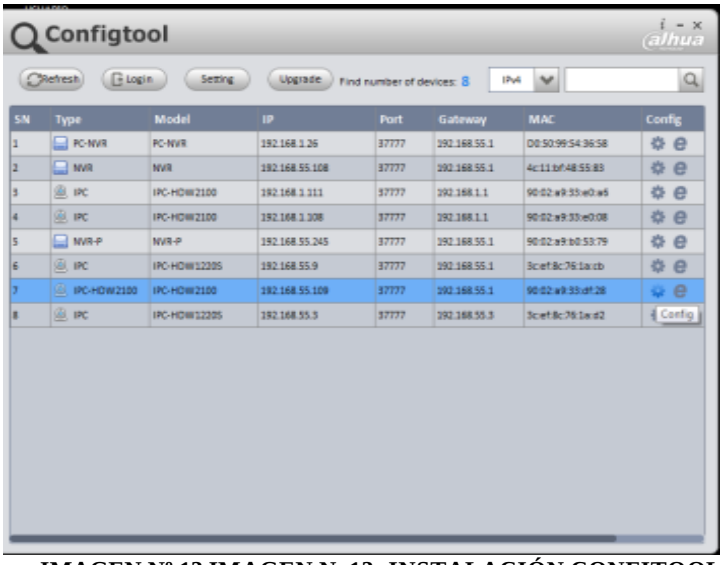


IMAGEN Nº 13 IMAGEN Nº 13: INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

14.- Aparecerá en la pantalla la ventana de configuración de *l*a cámara ip dahua IPC-HDW-1220S nos muestra que la cámara esta activa y su diferente pestaña, opciones de imagen

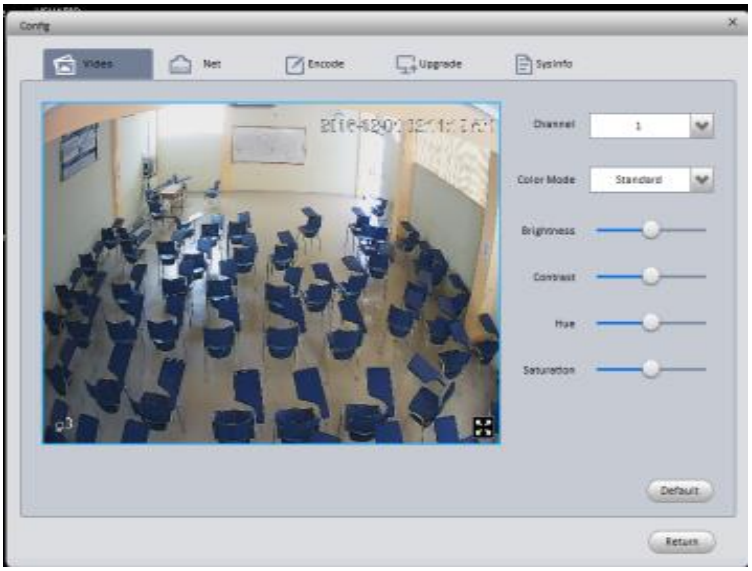


IMAGEN Nº 14 : INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

15.- Entramos dando click en la pestaña de configuración net de la cámara ip dahua IPC-HDW-1220S, donde nos muestra la opciones para cambiar la dirección ip, mascara, puerta de enlace, puertos como ser TCP, HTTP, UDP.

.

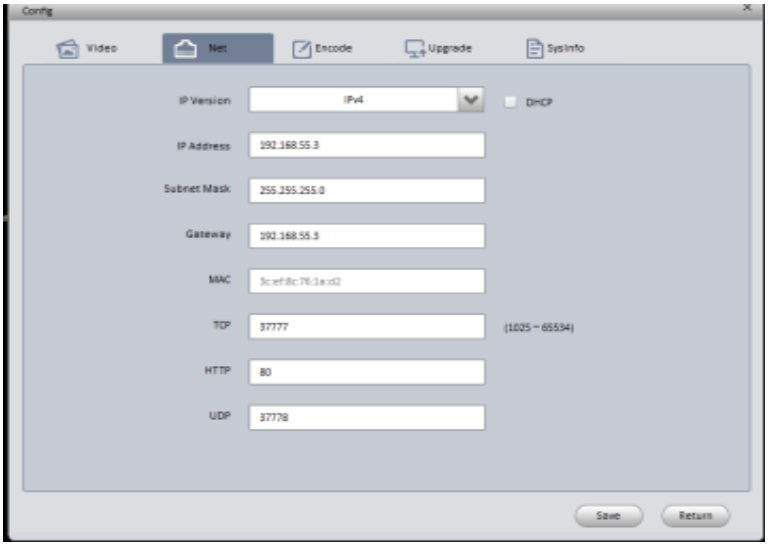


IMAGEN Nº 15: INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

16.- Cambiaremos los Protocolos a la red local que tenemos:

- IP Address : 192.168.55.3:4:7:9
- Subnet Mask: 255.255.255.0
- Gateway : 192.168.55.1

Las demás opciones por defecto para conectarse la red local en la cámara ip dahua IPC-HDW-1220S

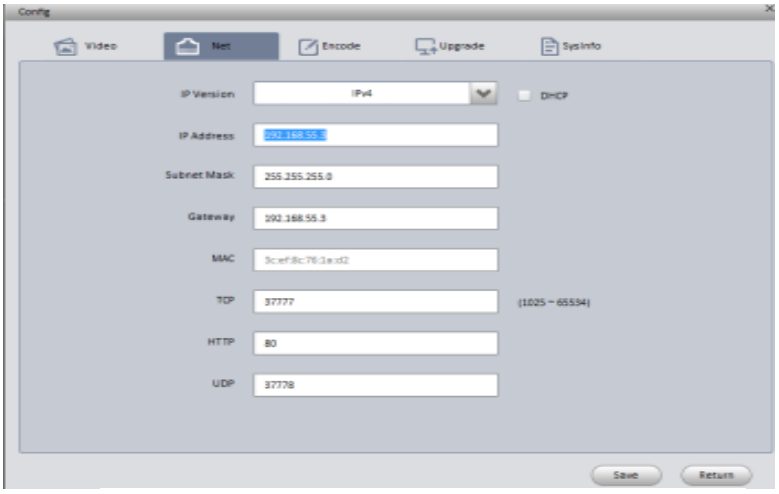


IMAGEN Nº 16: INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

17.- Dar click en guardar los cambios y ahora podremos acceder desde cualquier dispositivo que esté conectado a la red local.

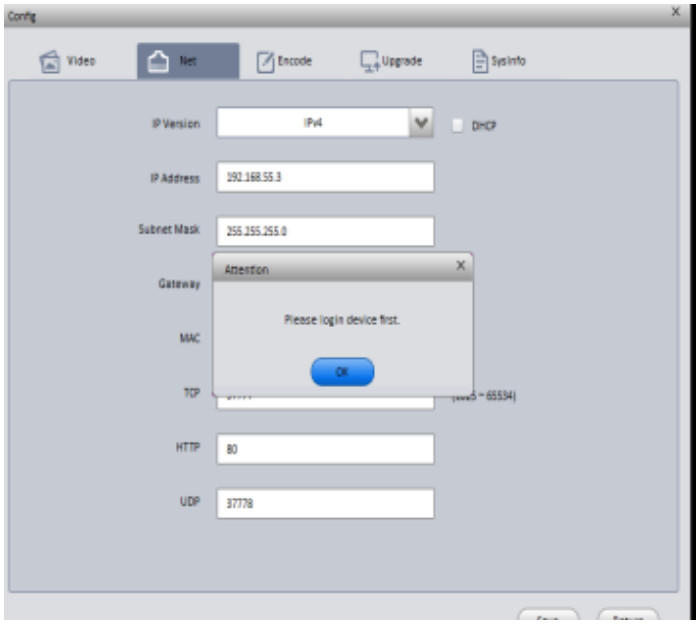


IMAGEN Nº 17: INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

18.-Para poder verificar la conexión abriremos un navegador que sea de preferencia Mozilla o Explorer pondremos en la barra de dirección ip que se colocó a la cámara ip dahua IPC-HDW-1220S.

IMAGEN Nº 18: INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

19.- Una vez introducido la dirección ip se cargara su página de ingreso de la cámara ip dahua IPC-HDW-1220S , pedirá el usuario y la contraseña la que viene por default “admin”, “admin”.

IMAGEN Nº 19: INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

20.- Un vez introducido el usuario y la contraseña nos pedirá instalar el pluing- in para visualizar el video de la cámara ip dahua IPC-HDW-1220S

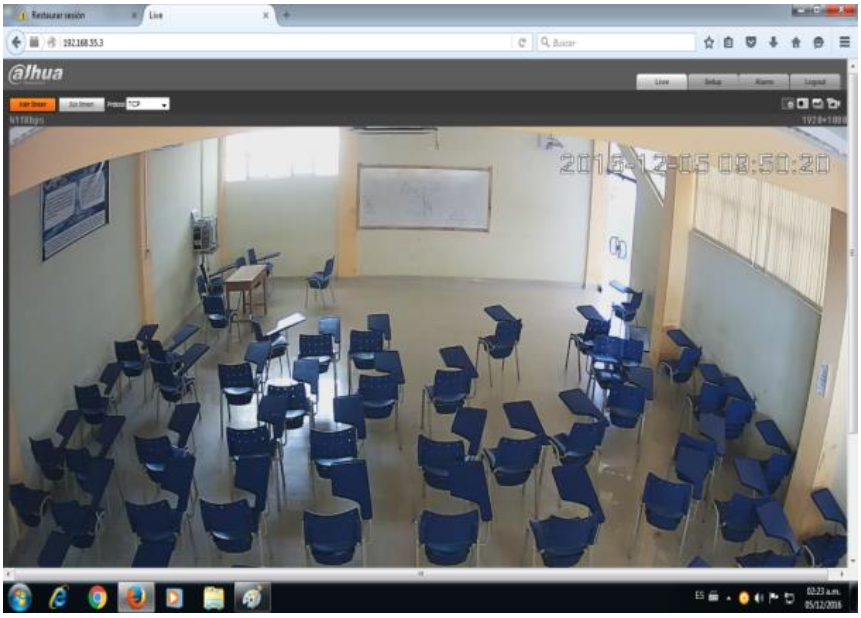


IMAGEN Nº 20: INSTALACIÓN CONFITOOL
FUENTE: ELABORACIÓN PROPIA

3.1.2.1.4. INTALACION DE SOFTWARE DE VISUALIZACION Y GRABACIÓN EN LA PC., SMARTPSS

1.- Colocar el cd para abrir el comprimido el software dh-smartpss_eng_V1.11.1.R.20140910

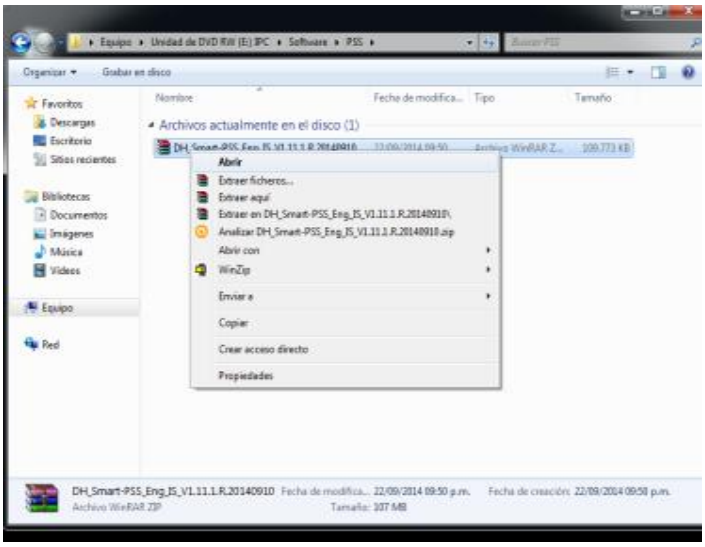


IMAGEN Nº1. 1: INSTALACIÓN SMARTPSS
FUENTE: ELABORACIÓN PROPIA

2.- Una vez abierto cd abrimos las carpetas con el nombre: IPC, Software y PSS, dar doble click para descomprimir el software dh-smartpss_eng_V1.11.1.R.20140910.rar

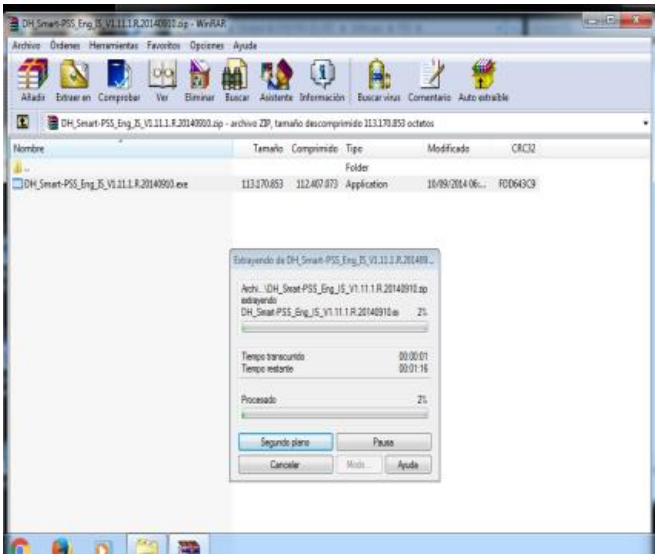


IMAGEN Nº1. 2 : INSTALACIÓN SMARTPSS
FUENTE: ELABORACIÓN PROPIA

3.- Aparecerá la pantalla de presentación del software dh-smartpss_eng_V1.11.1.R.20140910, dar siguiente.

IMAGEN Nº1. 3: INSTALACIÓN SMARTPSS
FUENTE: ELABORACIÓN PROPIA

4.-Hacemos click en la casilla de aceptar los términos del software dh-smartpss_eng_V1.11.1.R.20140910, y damos siguiente.

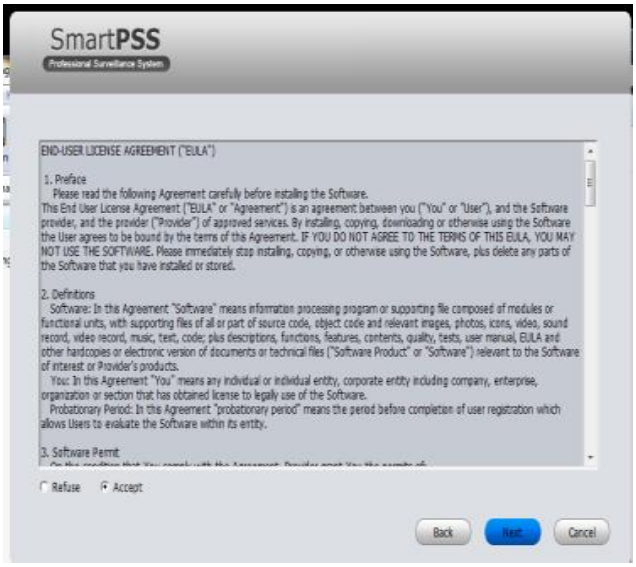
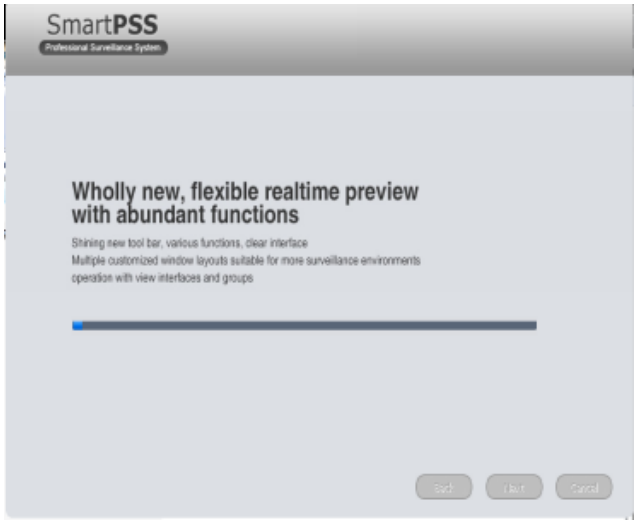


IMAGEN Nº1. 4: INSTALACIÓN SMARTPSS
FUENTE: ELABORACIÓN PROPIA

5.- Esta pantalla daremos siguiente y dejaremos todo por default

IMAGEN Nº1. 5 : INSTALACIÓN SMARTPSS
FUENTE: ELABORACIÓN PROPIA

6.- Cargando la instalación el software dh-smartpss_eng_V1.11.1.R.20140910



.

IMAGEN Nº1. 6: INSTALACIÓN SMARTPSS
FUENTE: ELABORACIÓN PROPIA

7.- pantalla de finalización del software dh-smartpss_eng_V1.11.1.R.20140910

IMAGEN Nº1. 7: INSTALACIÓN SMARTPSS
FUENTE: ELABORACIÓN PROPIA

3.1.2.1.5. CONFIGURACION DE LA CAMARA IP EL EN SOFTWARE DE VISUALIACION Y GRABACION DH-SMARTPSS_ENG_V1.11.1.R.20140910

8.- Una vez instalado el software lo abrimos haciendo doble click en el icono smartpss que está en el escritorio de la computadora

IMAGEN Nº1. 8: CONFIGURACION SMARTPSS
FUENTE: ELABORACIÓN PROPIA

9.- introducir la contraseña por default “admin” del software dh-smartpss_eng_V1.11.1.R.20140910

IMAGEN N°1. 9: CONFIGURACION SMARTPSS
FUENTE: ELABORACIÓN PROPIA

10.- Una vez abierto DEVICES nos aparecerá la ventana para realizar la búsqueda de los dispositivos, esta puede ser en automático o para agregarlo manualmente.

Para esto presionamos el botón refresh y nos mostrará los equipos detectados en la red, una vez que lo encontramos lo seleccionamos con un checkmark (√), y presionamos el botón Add, después de esto aparecerá un cuadro de diálogo para confirmar que lo agregaremos.

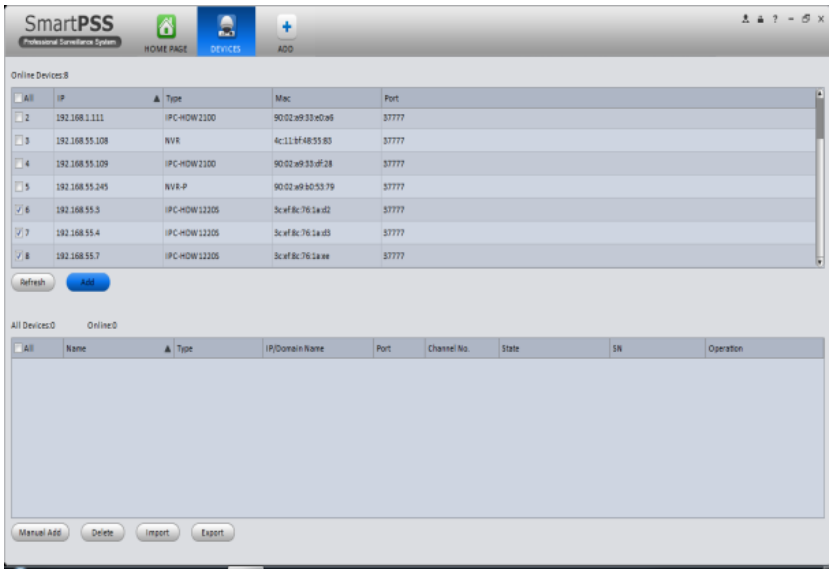


IMAGEN N°1. 10: CONFIGURACION SMARTPSS
FUENTE: ELABORACIÓN PROPIA

11.- Seleccionas las cámaras ip dahua IPC-HDW-1220S y adicionas

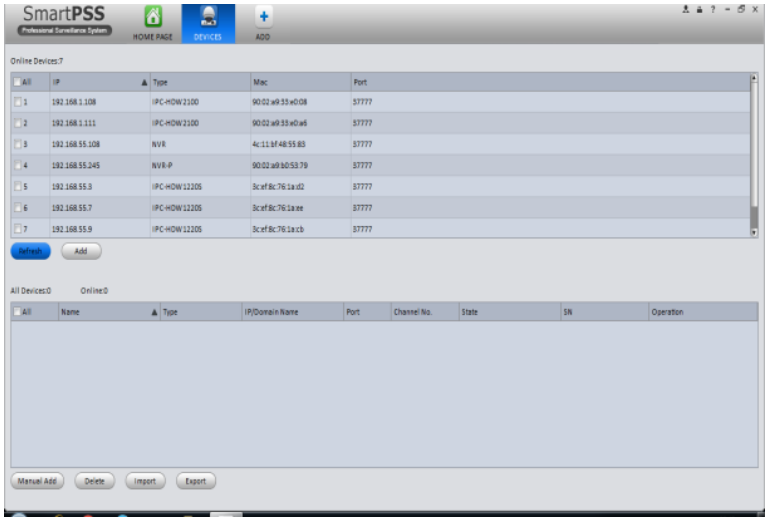


IMAGEN Nº1. 11: CONFIGURACION SMARTPSS
FUENTE: ELABORACIÓN PROPIA

12.- verificación de la conexión de las cámaras ip dahua IPC-HDW-1220S en el software dh-smartpss_eng_V1.11.1.R.20140910

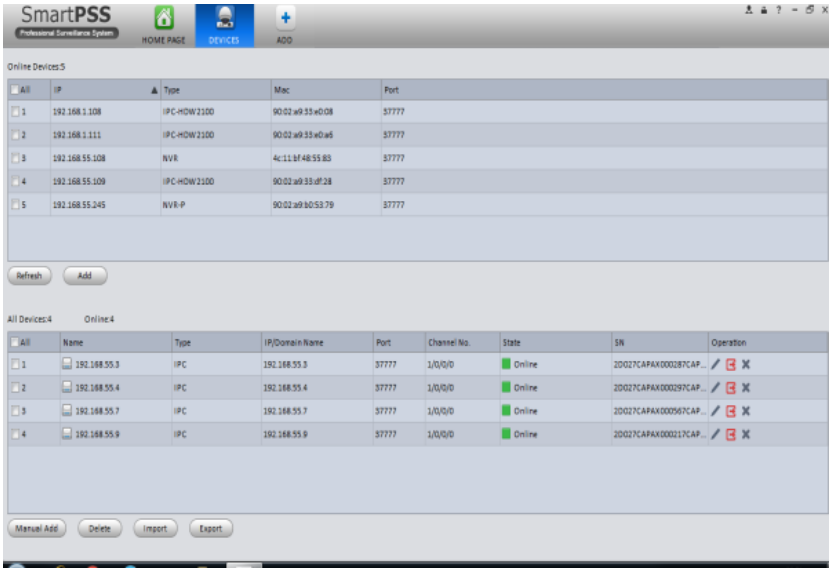


IMAGEN Nº1. 12: CONFIGURACION SMARTPSS
FUENTE: ELABORACIÓN PROPIA

13.- hacer click en la pastaña homepage del software dh-smartpss_eng_V1.11.1.R.20140910

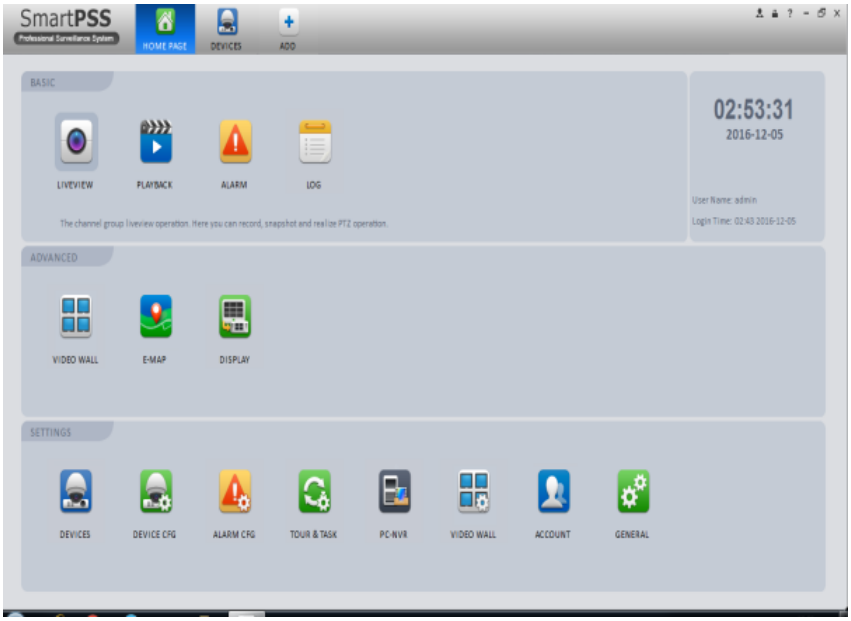


IMAGEN Nº1. 13 CONFIGURACION SMARTPSS
FUENTE: ELABORACIÓN PROPIA

14.-hacer click en el icono liveview del software dh-smartpss_eng_V1.11.1.R.20140910

IMAGEN Nº1. 14: CONFIGURACION SMARTPSS
FUENTE: ELABORACIÓN PROPIA

15.- selecciona la carpeta que dice default group del software dh-smartpss_eng_V1.11.1.R.20140910

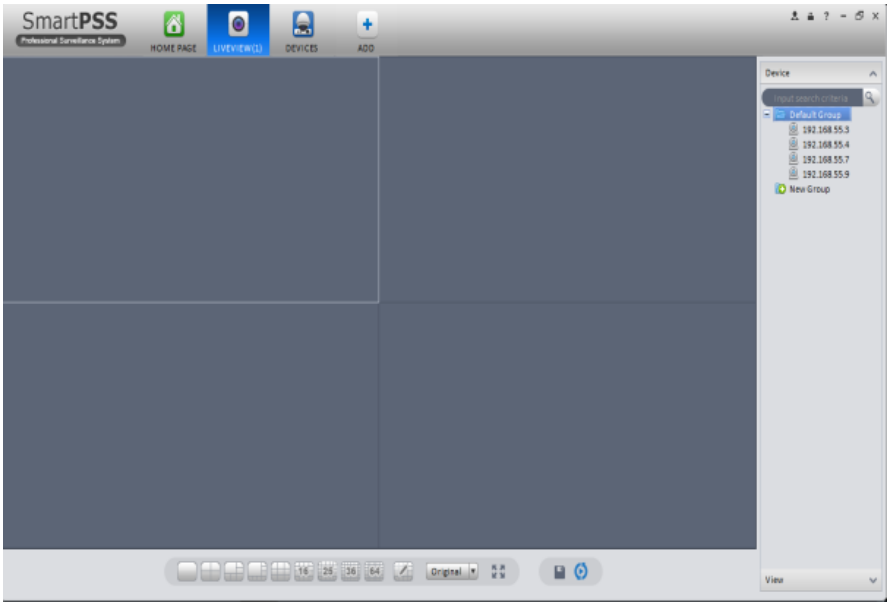


IMAGEN Nº1. 15 CONFIGURACION SMARTPSS
FUENTE: ELABORACIÓN PROPIA

16.- hacer doble click en la cámara ip dahua IPC-HDW-1220S

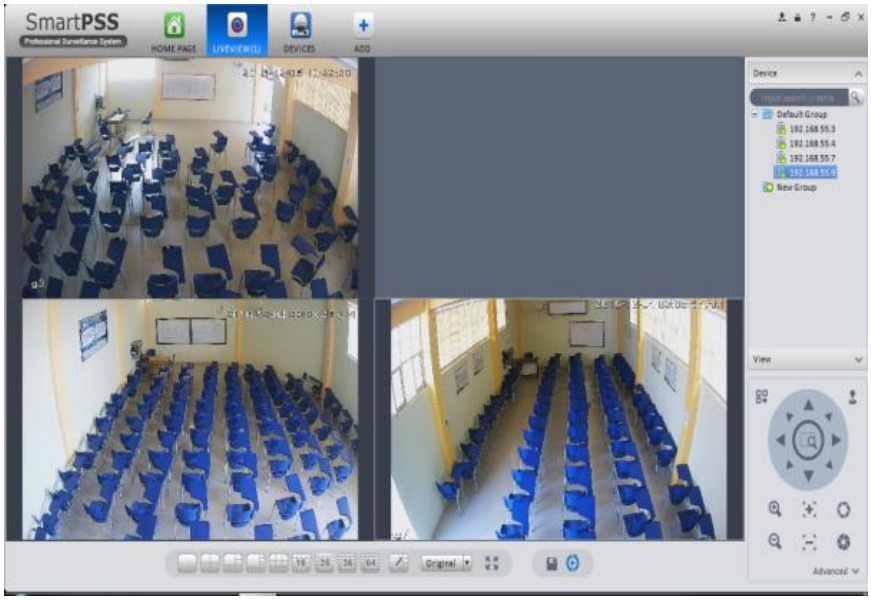


IMAGEN Nº1. 16 : CONFIGURACION SMARTPSS
FUENTE: ELABORACIÓN PROPIA

17.- pantalla donde muestra las cámara ip dahua IPC-HDW-1220S

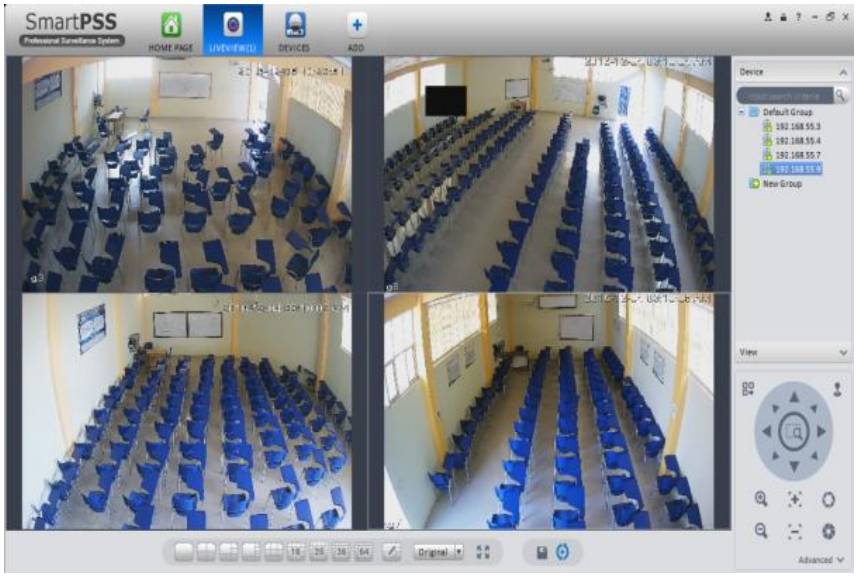


IMAGEN Nº1. 17: CONFIGURACION SMARTPSS
FUENTE: ELABORACIÓN PROPIA

3.2 ADMINISTRACIÓN DEL RENDIMIENTO

Tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo al comportamiento encontrado.

La administración del rendimiento se divide en 2 etapas: monitoreo y análisis.

3.2.1. Monitoreo

El monitoreo consiste en observar y recolectar la información referente al comportamiento de la red en aspectos como los siguientes:

a) **Utilización de enlaces**

Se refiere a las cantidades ancho de banda utilizada por cada uno de los enlaces de área local, ya sea por elemento o de la red en su conjunto.

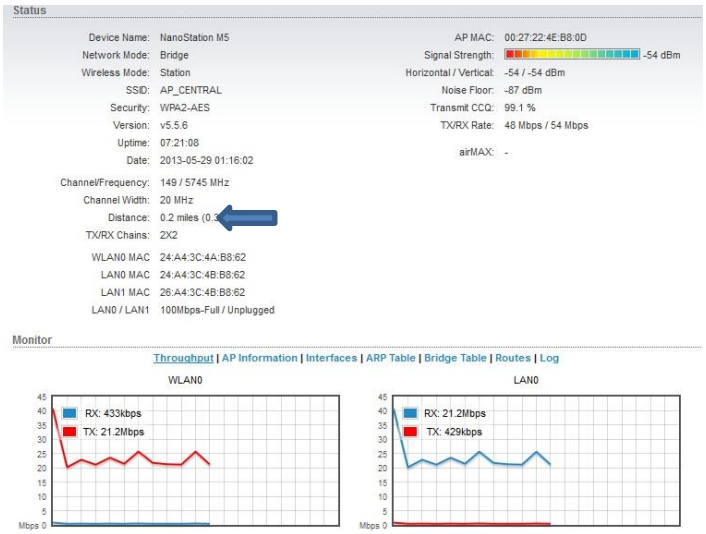
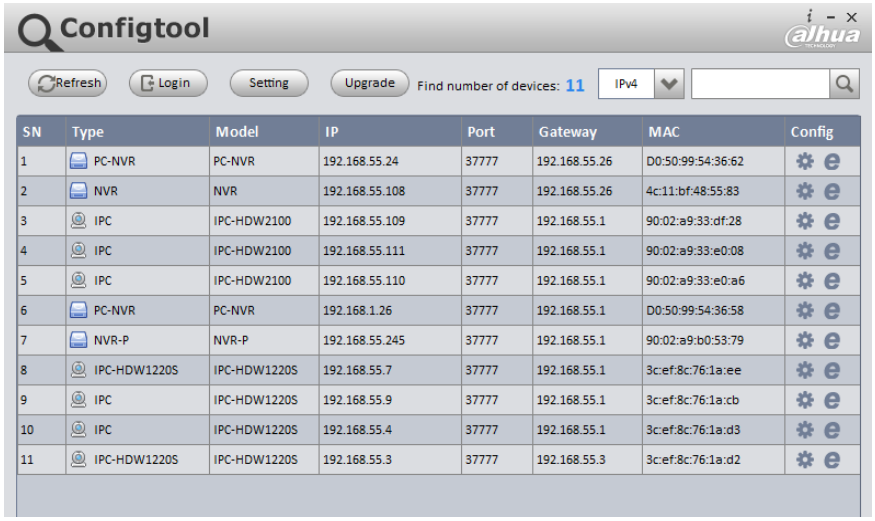


IMAGEN Nº A 1: ENLACE AL CENTRO DE MONITOREO
FUENTE: ELABORACIÓN PROPIA

b) Caracterización de tráfico.

Es la tarea de detectar los diferentes tipos de tráfico que circulan por la red, con el fin de obtener datos sobre los servicios de red, como http, ftp, que son más utilizados. Además, esto también permite establecer un patrón en cuanto al uso de la red.



SN	Type	Model	IP	Port	Gateway	MAC	Config
1	PC-NVR	PC-NVR	192.168.55.24	37777	192.168.55.26	D0:50:99:54:36:62	
2	NVR	NVR	192.168.55.108	37777	192.168.55.26	4c:11:bf:48:55:83	
3	IPC	IPC-HDW2100	192.168.55.109	37777	192.168.55.1	90:02:a9:33:df:28	
4	IPC	IPC-HDW2100	192.168.55.111	37777	192.168.55.1	90:02:a9:33:e0:08	
5	IPC	IPC-HDW2100	192.168.55.110	37777	192.168.55.1	90:02:a9:33:e0:a6	
6	PC-NVR	PC-NVR	192.168.1.26	37777	192.168.55.1	D0:50:99:54:36:58	
7	NVR-P	NVR-P	192.168.55.245	37777	192.168.55.1	90:02:a9:b0:53:79	
8	IPC-HDW1220S	IPC-HDW1220S	192.168.55.7	37777	192.168.55.1	3c:ef:8c:76:1a:ee	
9	IPC	IPC-HDW1220S	192.168.55.9	37777	192.168.55.1	3c:ef:8c:76:1a:cb	
10	IPC	IPC-HDW1220S	192.168.55.4	37777	192.168.55.1	3c:ef:8c:76:1a:d3	
11	IPC-HDW1220S	IPC-HDW1220S	192.168.55.3	37777	192.168.55.3	3c:ef:8c:76:1a:d2	

IMAGEN Nº A 2: TRÁFICO QUE CIRCULA EN LA RED DEL CENTRO DE MONITOREO
FUENTE: ELABORACIÓN PROPIA

c) **Porcentaje de transmisión y recepción de información**.

Encontrar los elementos de la red que más solicitudes hacen y atienden, como servidores, estaciones de trabajo, dispositivos de interconexión, puertos y servicios.

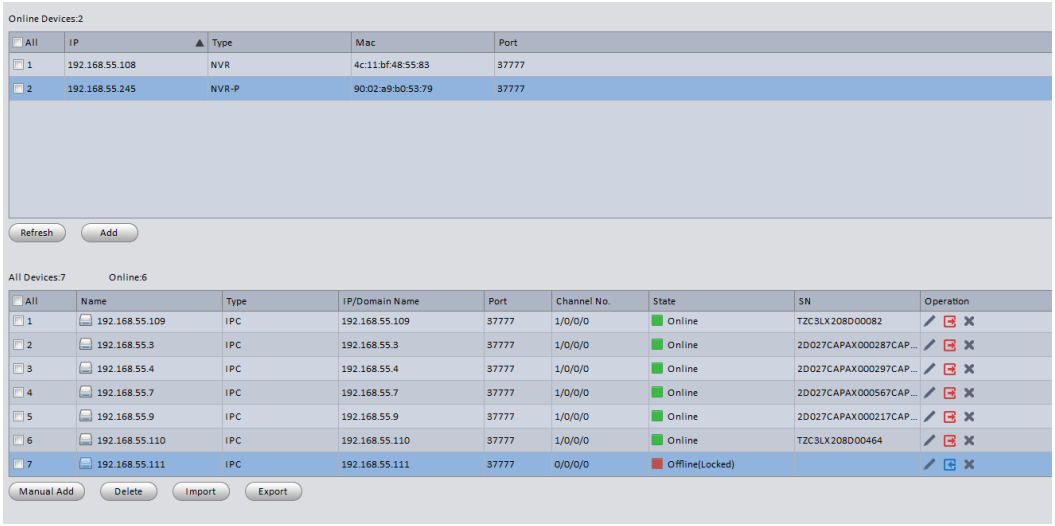


IMAGEN Nº A 3: PORCENTAJE DE ELEMENTOS ENCONTRADO EN LA RED DEL CENTRO DE MONITOREO
FUENTE: ELABORACIÓN PROPIA

3.3. ADMINISTRACIÓN DE FALLAS

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para restablecer la situación o minimizar el impacto de la falla.
El proceso de la administración de fallas consiste de distintas fases.

a) Monitoreo de alarmas. Se realiza la notificación de la existencia de una falla y del lugar donde se ha generado. Esto se puede realizar con el auxilio de las herramientas basadas en el protocolo SNMP.

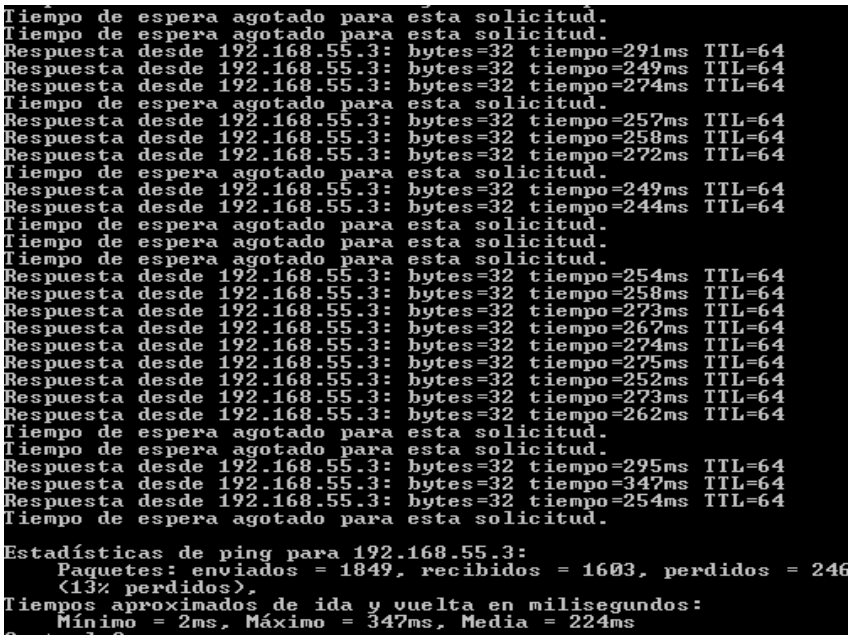


IMAGEN Nº B 1: FALLA EXISTENTE EN LA RED DEL CENTRO DE MONITOREO
FUENTE: ELABORACIÓN PROPIA

b) Localización de fallas. Determinar el origen de una falla.

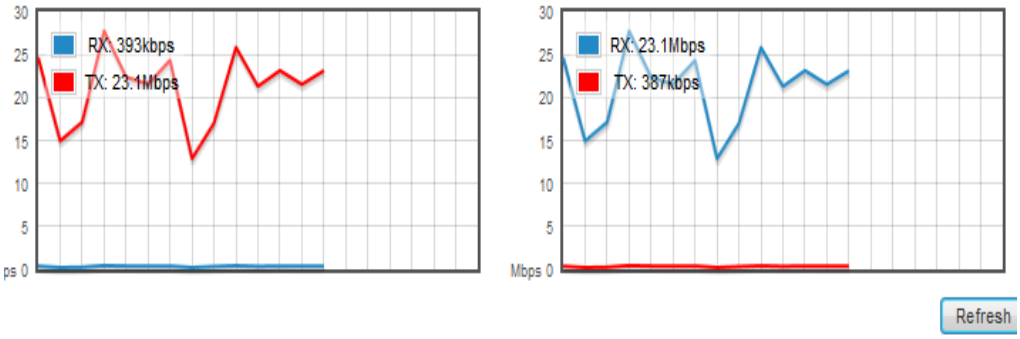


IMAGEN Nº B 2: FALLA ENCONTRADA EN LA RED DEL CENTRO DE MONITOREO
FUENTE: ELABORACIÓN PROPIA

3.4. ADMINISTRACIÓN DE LA SEGURIDAD

Su objetivo es ofrecer servicios de seguridad a cada uno de los elementos de la red así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques, así como para la respuesta ante incidentes de seguridad.

a) Prevención de ataques

El objetivo es mantener los recursos de red fuera del alcance de potenciales usuarios maliciosos. Una acción puede ser la implementación de alguna estrategia de control de acceso. Obviamente, los ataques solamente se reducen pero nunca se eliminan del todo.

- **Seguridad de las cámaras IP**

  Para brindar seguridad a cada una de las cámaras IP se le asigna una contraseña

IMAGEN Nº C 1: SEGURIDAD EN LA CAMARA IP
FUENTE: ELABORACIÓN PROPIA

- **Seguridad de la antena de red inalámbrica**

  Para brindar seguridad a cada una de las antenas se le asigna una contraseña

IMAGEN Nº C 2: SEGURIDAD EN LA ANTENAS
FUENTE: ELABORACIÓN PROPIA

- **Seguridad de la red inalámbrica de enlace**

  Para brindar seguridad al enlace de la red inalámbrica entre el centro de monitoreo y el bloque “G” se le asigna una contraseña

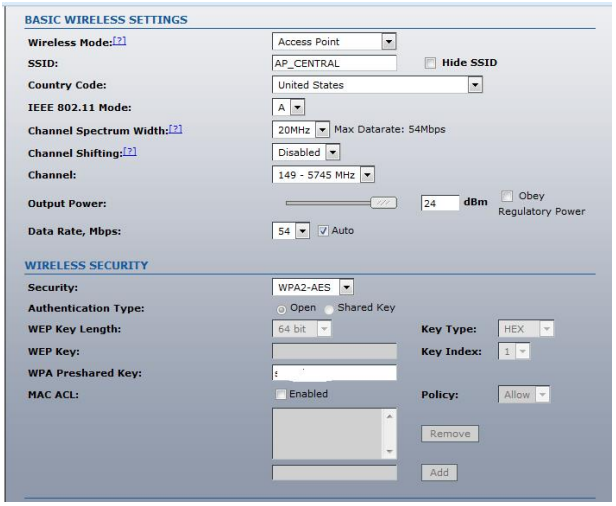


IMAGEN Nº C 3: SEGURIDAD EN LOS ENLACE DE LA ANTENAS
FUENTE: ELABORACIÓN PROPIA

- **Seguridad del dispositivo NVR**

  Para brindar seguridad al dispositivo NVR se le asigna una contraseña

IMAGEN Nº C 4: SEGURIDAD EN LOS ENLACE DE LA ANTENAS
FUENTE: ELABORACIÓN PROPIA

CAPITULO IV
CONCLUSIONES
Y RECOMENDACIONES

4.1. CONCLUSIONES

Al concluir el desarrollo del Sistema de Vigilancia y Monitoreo de las aulas audiovisuales del bloque "G" del campus universitario de la Universidad Amazónica de Pando, se consiguió demostrar que es de gran importancia para la seguridad y el resguardo de todos los bienes de la institución.

Con el sistema implementado y en funcionamiento, se ven los siguientes resultados:

- ✓ Se realizó un diagnóstico de la situación actual de las Aulas del bloque "G" del Campus Universitario con relación a la seguridad.
- ✓ Se realizó el diseño de la red de vigilancia y monitoreo para las Aulas audiovisuales del bloque "G"
- ✓ Se instaló las cámaras IP de acuerdo al diseño de la red de monitoreo.
- ✓ Se realizó las pruebas del sistema de vigilancia y monitoreo de las aulas audiovisuales del bloque "G"

Por lo cual se tiene ahora:

"Mayor eficiencia en la vigilancia, monitoreo y administración de las aulas audiovisuales del bloque "G"".

- ✓ Monitoreo constante de las aulas audiovisuales del bloque "G".
- ✓ Alerta temprana y en tiempo real sobre sospecha de robo o el uso indebido de los activos de la institución.
- ✓ El sistema brindará información visual en tiempo real de las aulas audiovisuales del bloque "G".
- ✓ El sistema facilitará la investigación en caso de robo o mal uso de los activos

Finalmente se tiene un sistema, que facilita la toma de decisiones de manera oportuna, reduciendo en gran manera los daños económicos que se producen en la U.A.P.

4.2. RECOMENDACIONES

Al culminar este proyecto se plantea las siguientes recomendaciones:

- Continuar con la implementación a medida.
- Permitir el flujo de otro tipo de información en el sistema.
- Implementar una red con fibra óptica para una mejor transmisión de información visual.
- Implementar un Sistema de Seguridad del Centro de Monitoreo.

5.1. BIBLIOGRAFIA

AXIS COMMUNICATIONS. (2006-2015). *Guía técnica para vídeo en red.* Recuperado el 36 de 11 de 2016, de Guía técnica Axis para vídeo en red: http://www.axis.com/files/brochure/bc_techguide_60873_es_1501_lo.pdf

dahua technology. (2010-2015). *dahuasecurity*. Obtenido de www1.dahuasecurity.com/es/

DOINTECH , S. (2015). Video Vigilancia IP: Sistemas de Seguridad con Cámaras IP. Bogotá a, Colombi. Obtenido de http://www.dointech.com.co/video-vigilancia-ip.html

Domótica Viva s.l. (2002). *Domótica Viva s.l.* Obtenido de www.domoticaviva.com

Marquez, O. (2014). *Breve historia y momentos claves en la evolución del comercio electrónico.* Barcelona.

Seguridad via ip. (2014). *Seguridad via ip.* Recuperado el 4 de 11 de 2016, de www.seguridadviaip.com.ar

Stallings, W. ((2005). *Comunicaciones y Redes de Computadores.* Recuperado el 10 de 12 de 2016, de Prentice Hall.: www.Prenticehall.org