



UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:

Ingeniería Electrónica Digital y Telecomunicaciones

TEMA: Diseño e implementación de un sistema de video vigilancia utilizando cámaras IP y tecnología OPEN SOURCE que permite el acceso remoto por web al sistema y el envío de notificaciones vía correo electrónico para el laboratorio de computación de la unidad educativa “ZEUS”

AUTOR/ A: Dorys Mariela Guerrero Moreno

TUTOR/ A: Ing. David Patricio Cando Garzón, Mg

AÑO: 2017

ÍNDICE

| | | |
|---------|-----------------------------------------------------------|----|
| 1. | INTRODUCCION | 1 |
| 1.1 | SITUACION ACTUAL..... | 1 |
| 1.2 | PROBLEMÁTICA | 2 |
| 1.3 | OBJETIVOS | 3 |
| | OBJETIVO GENERAL | 3 |
| | OBJETIVOS ESPECÍFICOS:..... | 3 |
| 2. | MARCO TEORICO Y ANÁLISIS DE REQUERIMIENTOS | 4 |
| 2.1 | SISTEMA DISTRIBUIDO | 4 |
| 2.2 | FUNDAMENTOS DE VIDEO | 5 |
| 2.2.1 | Señal de video..... | 6 |
| 2.2.2 | Sistema de video Análogo..... | 6 |
| 2.2.3 | Sistema de video Digital..... | 8 |
| 2.2.4 | Formatos de Video | 9 |
| 2.3 | REDES: CONCEPTO Y TOPOLOGÍA | 9 |
| 2.3.1 | TIPOS DE REDES | 10 |
| 2.3.2 | CABLEADO ESTRUCTURADO..... | 16 |
| 2.3.2.1 | Definición de Cableado Estructurado..... | 16 |
| 2.3.2.2 | Estándares para cableado | 17 |
| 2.3.3 | GENERALIDADES DE SISTEMAS DE VIDEO VIGILANCIA | 19 |
| 2.3.3.1 | Características de los sistemas de video vigilancia | 19 |
| 2.3.4 | Redes IP..... | 20 |
| 2.3.4.1 | Direccionamiento IP | 20 |
| 2.3.4.2 | Direccionamiento interdominio sin clase | 21 |
| 2.3.4.3 | Internet | 22 |
| 2.3.4.4 | Protocolos | 22 |
| 2.3.4.5 | Protocolos TCP/IP..... | 22 |

| | | |
|-----------|----------------------------------------------------------------------------|----|
| 2.3.4.6 | Direccionamiento IPv4 | 25 |
| 2.3.4.7 | Diferencias entre IP fija e IP Dinámica..... | 28 |
| 2.3.4.8 | Direccionamiento IPV6..... | 28 |
| 2.4 | VIDEO VIGILANCIA | 29 |
| 2.4.1.1 | Ventajas de la vigilancia IP inalámbrica | 30 |
| 2.4.2 | CÁMARAS IP | 31 |
| 2.4.2.1 | Características de una cámara IP | 32 |
| 2.4.2.2 | Ventajas de la Cámara IP | 33 |
| 2.4.2.3 | Funcionamiento de la vigilancia ip inalámbrica..... | 33 |
| 2.4.2.4 | Monitoreo Remoto..... | 35 |
| 2.4.3 | TECNOLOGIA OPEN SOURCE | 36 |
| 2.4.3.1 | Beneficios de las soluciones open source | 37 |
| 3. | ARQUITECTURA DEL PROYECTO..... | 38 |
| 3.1 | DIAGRAMA DE FLUJO FUNCIONAMIENTO SISTEMA DE SEGURIDAD (Un Evento)..... | 38 |
| 3.2 | CABLEADO ESTRUCTURADO..... | 39 |
| 3.3 | UBICACION CÁMARAS IP | 40 |
| 3.4 | Cámaras IP JideTech HD 1.0 MegaPixel..... | 41 |
| 3.5 | SOFTWARE BASE | 43 |
| 3.5.1 | CENTOS 6. 5 | 43 |
| 3.5.2 | INSTALACION DE ZONEMINDER | 44 |
| 3.5.2.1 | ZONEMINDER, LA SOLUCIÓN DE CÁMARAS DE SEGURIDAD TODO-EN-UNO LINUX GPL..... | 46 |
| 3.6 | PRESENTACION DE RESULTADOS..... | 47 |
| 3.6.1 | DISEÑO DE LA RED EN LA UEZ..... | 47 |
| 3.6.2 | SERVIDOR WEB | 48 |
| 3.6.2.1 | CAPA DE PRESENTACIÓN | 49 |
| 3.6.2.2 | CAPA DE APLICACIÓN | 49 |
| 3.6.2.2.1 | APLICACIÓN..... | 50 |

| | |
|------------------------------------------------------------------------------------|----------|
| 3.6.2.2.2 APLICACIÓN EN DISPOSITIVOS MÓVILES | 53 |
| 3.6.2.3 CAPA DE DATOS | 55 |
| 3.6.2.4 NOTIFICACIONES POR E-MAIL | 56 |
| 3.6.2.5 FILTRANDO EVENTOS | 58 |
| CONCLUSIONES | 63 |
| RECOMENDACIONES | 64 |
| BIBLIOGRAFÍA | 65 |
| ÍNDICE MANUAL DE USUARIO | 2 |
| Antes de usar los dispositivos | 1 |
| 1) Por su seguridad. | 1 |
| 2) Características de las cámaras: | 1 |
| Video Compression: H.264 Main Profile/Baseline. | 2 |
| 3) Formas de Monitoreo | 3 |
| 3. La aplicación empieza a conectarse con el servidor | 4 |
| 4. Solicitará nombre de usuario y password: | 4 |
| 4) TABLA DE FALLOS | 6 |
| TABLA DE FALLOS | 6 |
| 5.1) Contacto para soporte: | 7 |
| Instalando Centos 6.5 | 1 |
| Seleccionamos el dispositivo en donde se encuentra el boot a ejecutar. | 1 |
| Inicia el entorno gráfico. Damos click al botón Next | 2 |
| Elegimos el Idioma a usar durante la instalación y presionamos al botón Next | 3 |
| Elegimos la Distribución del teclado. Click al botón Siguiente | 3 |
| -Muestra el disco detectado. Click al botón Si descarte todos los datos. | 4 |
| -Escribimos un nombre para Centos (hostname). Click al botón Configure la red. ... | 5 |
| -La tarjeta (ethernet) debe estar conectada. | 5 |
| -IMPORTANTE, | 6 |
| -Ya configurada la conexión, presionamos click al botón Cerrar y Siguiente | 6 |

| | |
|--------------------------------------------------------------------------------|----|
| -Elegimos la Zona donde está ubicado el equipo. Click al botón siguiente. | 7 |
| -Escribimos una Contraseña para el usuario root. | 7 |
| -Siguiendo el paso, elegir como instalar Centos..... | 9 |
| -Comienza la instalación. | 9 |
| - Linux Centos está instalado. Click al botón Reiniciar | 10 |
| -Al hacer boot por primera vez en el Centos instalado. | 10 |
| -Se descargan los paquetes y así queda actualizado el sistema centos 6.5..... | 11 |
| Usar usuario de root para iniciar | 1 |
| Iniciando la instalación de mysqld..... | 2 |
| Cambio de credenciales..... | 3 |
| Editar /etc/php.ini. | 3 |
| Verificar que inicialmente ZoneMinder esté bien configurado. | 4 |
| Configura un servidor automáticamente. | 4 |
| Instalación de la política SELinux | 5 |
| Finalmente ,se puede iniciar el servicio de ZonemMnder | 6 |

ÍNDICE IMÁGENES

| | |
|----------------------------------------------------------------------------------------------|----|
| Imagen 1: Red LAN..... | 10 |
| Imagen 2: Red Man..... | 11 |
| Imagen 3: Red WAN | 11 |
| Imagen 4: Redes Alámbricas | 12 |
| Imagen 5: Redes Inalámbricas | 14 |
| Imagen 6: Red Bus o Lineal..... | 15 |
| Imagen 7: Red Estrella..... | 15 |
| Imagen 8: Red Anillo..... | 16 |
| Imagen 9: Red Malla..... | 16 |
| Imagen 10: Cableado Estructurado | 18 |
| Imagen 11 : Esquema de un sistema de Cableado Estructurado..... | 19 |
| Imagen 12: Elementos de una capa de red | 24 |
| Imagen 13: Cabecera en IPv4 | 25 |
| Imagen 14: Campos DS de la Cabecera de IPv4 | 26 |
| Imagen 15: Formato de una dirección IPv6 | 28 |
| Imagen 16: 0's Iniciales | 29 |
| Imagen 17: Doble dos puntos | 29 |
| Imagen 18: Representación de un Sistema de Vigilancia IP inalámbrica..... | 30 |
| Imagen 19 : Cámara IP y sus partes..... | 31 |
| Imagen 20 : CCTV Camera Solution vs IP Camera Solution..... | 32 |
| Imagen 21 : Vigilancia..... | 34 |
| Imagen 22: Monitoreo | 34 |
| Imagen 23 : Visualización de Imagen receptada por una cámara Inalámbrica en un monitor | 35 |
| Imagen 24 : Centro de Control de video vigilancia | 35 |
| Imagen 25: Funcionamiento sistema de Seguridad..... | 38 |

| | |
|--------------------------------------------------------------------|----|
| Imagen 26: Cableado Cámaras IP. Vista Frontal..... | 39 |
| Imagen 27: Ubicación Cámaras IP (Vista Superior) | 40 |
| Imagen 28: Cámaras IP | 41 |
| Imagen 29 : Ubicación Cámara IP 1 (Vista inferior)..... | 41 |
| Imagen 30: Vista y alcance de la cámara IP | 42 |
| Imagen 31: Vista posterior para el cableado..... | 43 |
| Imagen 32: Diagrama de red del sistema de seguridad | 48 |
| Imagen 33: Servidor Web | 48 |
| Imagen 34: Capa de Presentación..... | 49 |
| Imagen 35: Capa de Aplicación | 49 |
| Imagen 36 : Instalación repositorio zoneminder | 50 |
| Imagen 37 : Instalación repositorio zoneminderb | 51 |
| Imagen 38 : Instalación del servicio mysql..... | 52 |
| Imagen 39: Funciones..... | 53 |
| Imagen 40: Aplicación desde el dispositivo móvil | 54 |
| Imagen 41: Aplicación desde el dispositivo móvil | 54 |
| Imagen 42: Aplicación desde el dispositivo móvil | 55 |
| Imagen 43: Capa de Datos | 55 |
| Imagen 44: Configuración envío alertas vía mail en Zoneminder..... | 58 |
| Imagen 45: Filtros y condiciones..... | 59 |
| Imagen 46 : Filtrar evento | 60 |
| Imagen 47 : Configuración Filtro PurgeWhenFull | 60 |
| Imagen 48 : Guardar Filtro PurgeWhenFull | 61 |

ÍNDICE DE CUADROS:

| | |
|--------------------------------------------------------|----|
| Cuadro 1: Modelo de referencia para TCP/IP..... | 24 |
| Cuadro 2: Requerimientos del hardware | 43 |
| Cuadro 3: Presupuesto Proyecto..... | 62 |
| Cuadro 4 : Presupuesto en el mercado | 62 |

1. INTRODUCCION

La seguridad en la actualidad experimenta avances; la era digital de la información se enrumba hacia la tendencia de nuevas tecnologías, por esta razón las redes y sistemas de comunicación dan inicio a la video vigilancia IP (Internet Protocol).

Por los recientes registros de ataques a la seguridad en el mundo, los equipos de video vigilancia están sometidos a un desarrollo de aplicaciones, debido a la información que pueden captar y por la manera de facilitar una reacción veloz y eficaz a los equipos de seguridad.

En la era actual la vídeo vigilancia IP reemplaza a los tradicionales sistemas de seguridad porque ofrecen: bajos costos, mejores servicios con el desarrollo y robustez de la internet hacen posible la video vigilancia remota. Con la ayuda de protocolos complementarios, la red se adaptará para transmitir imágenes y video en tiempo real.

El presente proyecto de tesis de grado titulado: "DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE VIDEO VIGILANCIA UTILIZANDO CÁMARAS IP Y TECNOLOGÍA OPEN SOURCE QUE PERMITAN EL ACCESO REMOTO POR WEB AL SISTEMA Y EL ENVÍO DE NOTIFICACIONES VÍA CORREO ELECTRÓNICO PARA EL LABORATORIO DE COMPUTACIÓN DE LA UNIDAD EDUCATIVA "ZEUS" se enfoca al diseño de un sistema de monitoreo, vigilancia y almacenamiento de videos e imágenes digitales; mediante el uso y acoplamiento de cámaras IP a la red que se instalará para el modelo de la seguridad IP. Adicional se lo podrá visualizar en tiempo real y a su vez permitirá enviar notificaciones de alerta vía correo electrónico.

Para realizar con efectividad y ejecutar lo expuesto, se utilizará la tecnología OPEN SOURCE (código abierto) que es el software distribuido y desarrollado libremente, el mismo permitirá la administración y control del proyecto.

1.1 SITUACION ACTUAL

Existe, en la sociedad contemporánea, un alto índice de inseguridad que preocupa a las autoridades en la aplicación de políticas sociales. El tema de inseguridad es recurrente en el sur de la ciudad de Quito. Para entender la magnitud de la inseguridad ciudadana, es necesario comprender que afecta a la tranquilidad de la población y los intereses de la ciudad.

La video vigilancia actualmente es una de las principales defensas contra la delincuencia registrada en los últimos tiempos. Los equipos que conforman el sistema de video vigilancia son esenciales y necesarios dentro de la infraestructura de seguridad actual, ya que la institución no posee ningún sistema de seguridad por los bajos recursos de la misma.

La Unidad Educativa “ZEUS” que alberga en horario matutino alrededor de 40 niños de educación inicial, actualmente no cuenta con un sistema de seguridad para el laboratorio de computación implementado por la Universidad Tecnológica “ISRAEL”.

En respuesta a los requerimientos de seguridad, el sistema de video vigilancia IP se plantea como la herramienta indispensable, para el control de las actividades que se desarrollan dentro de la UEZ.

1.2 PROBLEMÁTICA

En la actualidad los sistemas de seguridad experimentan un gran avance; la digitalización de la información logra su convergencia a una nueva tecnología, es así como las redes y sistemas de comunicación dan origen a la video vigilancia IP (Internet Protocol), la evolución hacia IP le permite adaptarse a los actuales protocolos y estándares de red.

Quedan atrás los sistemas analógicos convencionales como CCTV (Circuito cerrado de televisión), ya que los sistemas de video vigilancia IP brindan mejores prestaciones y junto a la expansión y desarrollo del internet permiten la video vigilancia remota. Por otra parte; a pesar que el internet no fue diseñado para aplicaciones de video en tiempo real, éste se adapta mediante el uso de protocolos complementarios.

El desarrollo de este proyecto permitirá conocer los sistemas de video vigilancia basados en tecnología IP, que poco a poco ocupan un lugar importante dentro de las infraestructuras robustas y de alto rendimiento en cuanto a seguridad con el monitoreo y reporte de alertas.

Se utiliza el software Open Source para disminuir el costo de la implementación de un sistema de video seguridad, ya que la Unidad Educativa “Zeus” es de bajos recursos económicos.

En este trabajo se pretende utilizar las características de la video vigilancia conjuntamente con protocolos IP para crear un sistema de vigilancia no convencional.

Por los reportes mencionados se procederá a implementar un sistema de seguridad en el segundo piso de la Institución, ubicada en el sur oriente de la ciudad de Quito, donde las estadísticas de delincuencia fueron más altas.

1.3 OBJETIVOS

OBJETIVO GENERAL

Diseñar e implementar un sistema de seguridad que permita el acceso remoto vía web para la revisión de cámaras, así como la captura de imágenes y video, utilizando Tecnología Open Source que reduzca los costos de implementación y además permita el envío de notificaciones mediante correo electrónico; en el segundo piso de la Unidad Educativa “Zeus” ubicada en el sur oriente de la ciudad de Quito.

OBJETIVOS ESPECÍFICOS:

- Analizar de requerimientos de seguridad para el laboratorio de computación de las Unidad Educativa “ZEUS”
- Diseñar una solución que cumpla con los requerimientos especificados en el análisis realizado.
- Evaluar los diferentes tipos cámaras IP que se adaptan a la necesidad.
- Evaluar el software Open Source a utilizar que cumpla con los requerimientos.
- Ejecutar la instalación del sistema de video vigilancia y las cámaras IP acorde al diseño realizado.

2. MARCO TEORICO Y ANÁLISIS DE REQUERIMIENTOS

2.1 SISTEMA DISTRIBUIDO

Un Sistema Distribuido tiene dos componentes básicos software y hardware, es una conexión de computadoras independientes que trabajan en conjunto pero que se encuentran ocultos para los usuarios como una única computadora, se consolidan para que se establezca el tipo de conexión en Red de un sistema distribuido.

Es aquel en el que los componentes son localizados en computadores los cuales son conectados y entre estos a su vez se comunican, corrigen cada una de sus acciones únicamente con el paso de los mensajes. Su finalidad principal es compartir los recursos fácilmente de modo que al editar, borrar o actualizar un dato desde un punto, lo hace un servidor de un cliente y este puede ser actualizado en tiempo real, para esto se establece una comunicación entre un protocolo practicado con esquema cliente servidor.

Un sistema distribuido tiene 4 características esenciales las cuales son:

1. La Concurrencia. En un único sistema que tiene varios procesos, pueden ser utilizados al mismo tiempo por varios usuarios. En los sistemas distribuidos hay muchos sistemas con uno o más procesadores que actúan cuando muchos usuarios solicitan simultáneamente comandos o aplicaciones (por ejemplo, café net). Muchos procesos de servidor se ejecutan simultáneamente, cada uno responde a la petición del cliente diferente, por ejemplo, servidor de archivos.
2. La Escalabilidad. Los pocos PC's conectados a servidores dentro de una Red de área local y los sistemas de aplicaciones de software que están interconectados en una red de área amplia, no deben tener la necesidad de cambio cuando la escala aumenta. La escalabilidad depende de:
 - Hardware
 - Software
 - Redes
 - Almacenamiento
3. La Tolerancia en fallos, es la capacidad para operar bajo el fallo o error, posiblemente en un nivel de rendimiento degradado. Tiene dos enfoques:

- Redundancia de hardware: El uso de componentes redundantes.
- Recovery Software. Diseño de programas para recuperar.

En los sistemas distribuidos los servidores pueden ser replicados al igual que las bases de datos se pueden replicar. El software de recuperación consiste en un diseño de manera que el estado de los datos permanentes se recupera. Los sistemas distribuidos, en general, proporcionan alta disponibilidad.

4. La Transparencia es la ocultación por parte del usuario la separación de componentes de un sistema distribuido de modo que el sistema se percibe como un todo. Ejemplos :

- Transparencia de Acceso, permite que los objetos locales y remotos puedan acceder mediante operaciones idénticas (lectura de archivos).
- Ubicación transparencia, ubicación de los recursos está oculta.
- Transparencia Migración, los recursos se pueden mover sin cambiar sus nombres.
- Transparencia de replicación, los usuarios no pueden decir cuántas copias existen.
- Concurrencia Transparencia, varios usuarios pueden usar los recursos libremente en forma automática.
- Paralelismo Transparencia, las actividades puede ocurrir en paralelo sin que el usuario lo sepa
- Transparencia de errores, oculta los errores que se producen cuando utilizan los recursos

2.2 FUNDAMENTOS DE VIDEO

El video es una captura, grabación, almacenamiento, reconstrucción de una secuencia de imágenes que representan escenas en movimiento y provistas de sonido del estudio.

Del análisis del principal dispositivo de captura de imagen del que se dispone, el ojo humano, se deriva la tecnología usada en los artefactos creados por el hombre para registrar imágenes. Esos artefactos, las cámaras, actúan a imagen y semejanza del ojo humano. Al menos en cierta medida.

Las células foto receptoras se denominan conos y bastoncillos, siendo los conos los responsables principales de la percepción del color. Según estudios, existen 3 tipos de conos, sensibles cada uno a longitudes de onda distintas, en concreto a las correspondientes a los colores ROJO (Red), VERDE (Green) y AZUL (Blue).

Es decir, el ojo sería un dispositivo RGB, que es capaz de reproducir muchos colores a base de la combinación aditiva de estos 3 únicos colores. Básicamente el video se compone de dos elementos: la luminancia y la crominancia por separado.

Luminancia: Es la que recibe la información con toda la intensidad luminosa y se representa la imagen en blanco y negro con todos los tonos mediante la escala de grises.

Crominancia: Comprende los canales RGB, es decir rojo, verde y azul, representa la combinación de los tres colores primarios.

2.2.1 Señal de video

La señal de vídeo se origina a partir de la conversión de variaciones de intensidad de luz por cambios de intensidad eléctrica. Todo esto se produce cuando existen materiales fotosensibles.

La imagen de vídeo se forma partiendo de la reproducción de una serie de imágenes por segundo. Con esta sucesión de imágenes a una determinada frecuencia, se logra la sensación de movimiento (framerate). La velocidad a través el cual se visualizan las imágenes se denomina framerate y es equivalente al número total de imágenes (frames) mostradas en un segundo.

2.2.2 Sistema de video Análogo

Los impulsos electrónicos de las imágenes (señal de vídeo) y del sonido (señal de audio) se graban y almacenan en la cinta de vídeo (que es un soporte de plástico recubierto de óxido de hierro que queda magnetizado). Durante la reproducción, la información almacenada se vuelve a convertir en señales de audio y vídeo y son traducidas por el aparato de TV. La cantidad de información electrónica es mucho mayor para la grabación de vídeo que para la de audio. Existen diferentes sistemas de grabación en cinta analógica, de forma generalizada diferenciaremos los sistemas domésticos (fácil manejo, pero no permiten copias para edición o posproducción sin

pérdida) de los sistemas profesionales, cuyas imágenes no se deterioran en posteriores copias para edición o posproducción.

Tanto los sistemas analógicos como los digitales pueden tratar su señal en una de las tres formas básicas: Y/C Componentes, Compuesto, o RGB. Vinculando estos formatos con los cables que sirven para transmitir una señal de forma que faciliten su identificación.

Sistema Y/C Componentes. La señal de luminancia (Y) y la de crominancia (C) se mantienen separadas durante el proceso de codificación (nivel de escritura) y en el proceso de decodificación (nivel de lectura), pero ambas señales se combinan y ocupan la misma pista en la cinta de vídeo. La configuración Y/C requiere dos hilos de cable diferentes para transformar la señal componente

Los cables **BNC**, conector coaxial, se utilizan para equipos profesionales por componentes, un cable lleva la señal de luminancia Y, y el otro la señal de crominancia C.

El cable **S-Vídeo** lleva los dos componentes Y, C por separado. La señal se transmite por 4 hilos separando luminancia (Y) y crominancia (C) así como sus respectivos retornos (GND). Las señales no se mezclan por lo que se minimizan las interferencias. El conector normalizado es un minidin de 4 contactos aunque también se pueden usar un Euro-conector con sus entradas luminancia y crominancia. Suele estar disponible en equipos analógicos de VHS y Super VHS, también en videocámaras Hi-8 y Digital-8 y DV en las cuales se aprovecha esa mejor calidad para monitorizar las imágenes.

Sistema Compuesto. La señal de video va por un solo hilo (luminancia y crominancia mezcladas) y aunque la calidad puede ser bastante buena existe una cierta interferencia entre color y luminancia. Esta señal es la que llega por los canales convencionales analógicos de emisión. El conector más usado para esta conexión es el RCA (habitualmente amarillo

Los cables **RCA**, llevan señal compuesta, se utilizan en los sistemas domésticos

Sistema RGB. Las señales roja, verde y azul se tratan por separado a lo largo de todo el proceso de grabación, incluso en la cinta de vídeo. Necesita tres hilos para

transportar la señal de vídeo. Todos los equipos que se utilicen en la edición tienen que mantener esa misma diferencia de señal. Es el formato que utilizaba el sistema profesional U-MATIC, ya casi en desuso, pero también lo incorporan algunos proyectores de vídeo y pantallas de plasma.

2.2.3 Sistema de video Digital

Existen diferentes sistemas de grabación en cinta digital, los sistemas domésticos utilizan cintas de mini DV que tienen una calidad un poco inferior al DVCAM de ¼ pulgada profesional.

El sistema de video digital se maneja a través del ordenador, la información que se procesa es una serie de valores establecidos y entendibles por ordenador basados en 0 y 1 conocido como bit. El video digital dentro del mundo de la informática tiene un formato y un códec.

Un formato es la forma en la que se guardan los datos en un fichero y de esta forma puede cumplir diferentes requisitos según el uso para el que este diseñado.

El Codec es la comprensión algorítmica a la que se somete el contenido del formato del video digital, en otras palabras es cualquier tecnología para comprimir y descomprimir datos, la palabra viene de la partición de las palabras codificar y decodificar. Los codecs pueden ser implementados en software, hardware o en la combinación de ambos.

Sistema Digital DV. Si bien los sistemas de edición digital pueden obtener o volcar la información de vídeo por Componentes o Compuesto, para clarificar la información a nivel práctico, el formato digital que se utiliza es el DV. Presenta la ventaja que un solo tipo de cable y conector sirve a la vez de entrada y salida tanto para audio como para vídeo. La denominación del conector varía según el tipo de aparato, en las cámaras y magnetoscopios digitales se denomina DV IN/OUT, en los ordenadores IEEE-1394 y el cable Fire-wire

El cable **Fire-wire** transporta tanto la señal de audio como la de vídeo. Puede presentar distintos aspectos, dos conectores pequeños (como el de la parte superior de la imagen) para transmitir información de la cámara a un magnetoscopio. Un conector pequeño y otro grande (pequeño para la cámara o magnetoscopio y grande

para el ordenador) o dos grandes para conectar el ordenador a un periférico, por ejemplo un disco externo.

2.2.4 Formatos de Video

Existen 5 tipos de formatos de video que son:

- AVI, es el formato de mejor calidad de imagen, su principal desventaja es el tamaño ya que por ejemplo un video de 10 minutos puede llegar a pesar entre 700-800 Mb.

- MOV, tiene una calidad de imagen buena, un tamaño aceptable pero su desventaja es que necesita la aplicación Quick Time desarrollada por Apple

- MPEG y sus derivados como es MPEG1 es el formato que tiene una buena calidad de video pero para resoluciones pequeñas por ejemplo de 240 x 320 pixeles que son comúnmente los videos reproducidos en celulares. El MPGE2 también brinda una buena calidad de video, tamaños aceptables, también es recomendable trabajarlo en HD y el tercer derivado MPEG4 que es el formato exclusivo para HD y Full HD para este tipo de resoluciones con una calidad de imagen bastante buena.

- FLV (Flash Video), este tipo de formato es bastante conocido en internet, por ejemplo todos los videos de YouTube se encuentran en dicho formato ya que tiene un tamaño bastante ligero y permite que los videos carguen rápido pero una de su desventaja es que pierde un poco la calidad de imagen frente a otros formatos.

- WMV (Windows Media Video), es un formato conocido y su principal característica es que se lo puede reproducir en cualquier computadora que tenga el sistema operativo Windows, tiene una calidad de imagen bastante aceptable y un tamaño regular por lo que su uso es bastante difundido.

2.3 REDES: CONCEPTO Y TOPOLOGÍA

Es un conjunto de dispositivos que están conectados a nodos mediante un enlace de comunicación. Estos enlaces que conectan los dispositivos llamados canales de comunicación.

Una red de ordenadores es un canal de telecomunicaciones a través del cual se comparte los datos. El mejor ejemplo de una red informática es Internet. Software: Son los programas, sistema operativo, driver y los programas de aplicación en red.

Una red está compuesta por ordenadores, módems, routers, servidores y medios de conexión entre todos estos.

2.3.1 TIPOS DE REDES

- ✓ Las redes se clasifican según:
- ✓ Tamaño de red
- ✓ Medio Físico
- ✓ Topología de Red

2.3.1.1 Según su tamaño de Red:

Red LAN: Consiste en una red de computadoras en un solo sitio, por lo general un edificio de oficinas individuales. Una LAN es muy útil para compartir recursos, como impresoras y almacenamiento de datos. Las LAN se pueden construir con un hardware relativamente barato, como concentradores, adaptadores de red y los cables Ethernet, como se detalla en la imagen 1 a continuación:

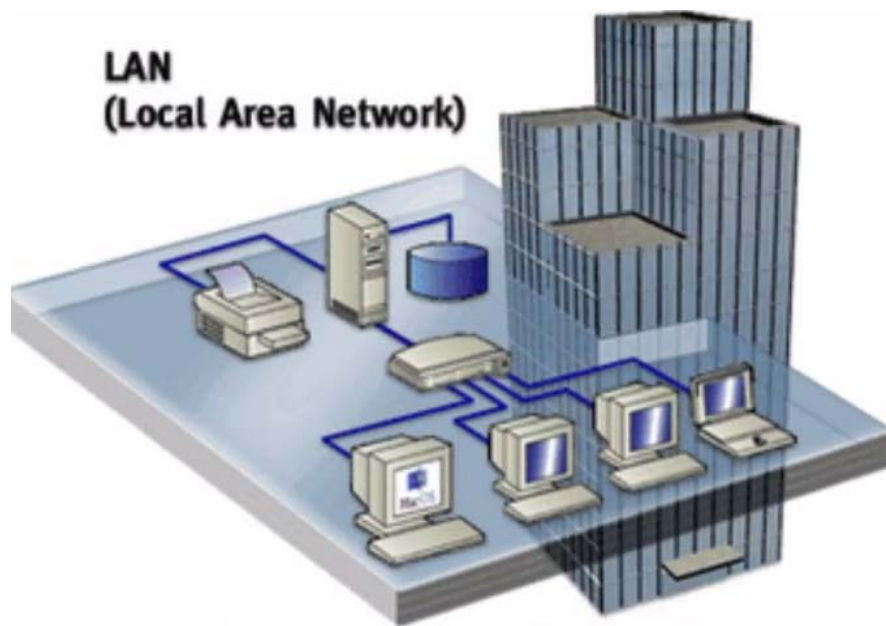


Imagen 1: Red LAN

Fuente: <http://bibdigital.epn.edu.ec/bitstream/15000/9268/3/Cap%202.pdf>

Red MAN: Es una red de ordenadores a través de toda una ciudad, el campus universitario o pequeña región. Es más grande que una red LAN, normalmente se limita a un solo edificio o sitio. Depende de la configuración, este tipo de red puede cubrir un área de varias millas a decenas de millas. Es utilizada para conectar varias LAN entre sí para formar una red más grande según muestra la imagen 2.



Imagen 2: Red Man

Fuente: <https://www.youtube.com/watch?v=tpuiYms6Gaw>

Red WAN: Ocupa una zona muy grande, tal como todo un país o el mundo entero. Una WAN puede contener varias redes más pequeñas, como las redes LAN y MAN. El Internet es el ejemplo más conocido de una WAN pública como se detalla en la imagen 3.

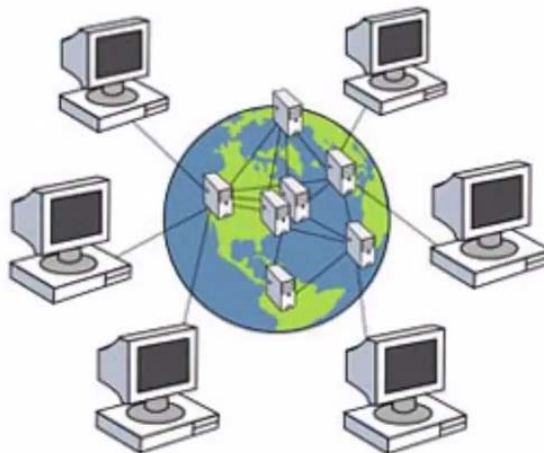


Imagen 3: Red WAN

Fuente: <http://bibdigital.epn.edu.ec/bitstream/15000/9268/3/Cap%202.pdf>

2.3.1.2 Redes Según su Medio Físico

El medio físico es el medio sobre el que se envían las señales eléctricas para realizar la transmisión de la información.

2.3.1.2.1 Redes Alámbricas: Como se observa en la imagen 4, para su funcionamiento se usan cables Rj45 de par trenzado, con cables paralelos conectan el ordenador con el switch y los cables cruzado se usan para conectar PCs entre sí.

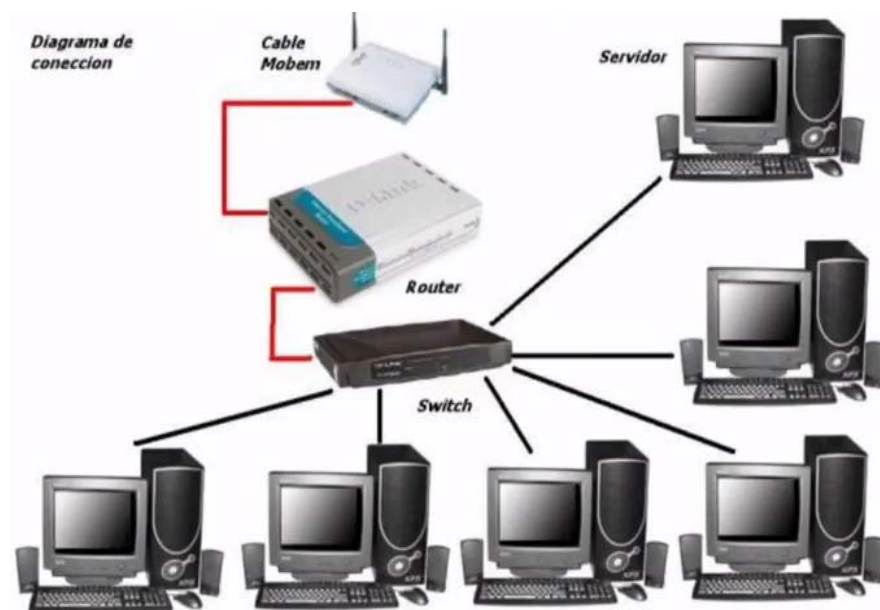


Imagen 4: Redes Alámbricas

Fuente: <https://www.youtube.com/watch?v=tpuiYms6Gaw>

Cables de cobre.

Los cables de cobre utilizados para transmisión son conductores clásicos que en ocasiones no son de este metal, sino aleaciones que mejoran las características eléctricas del cable.

Los tipos de claves más utilizados para la transmisión de datos son:

- ✓ **Coaxial.** El término coaxial quiere decir eje común ya que un cable coaxial está formado por un conductor central rodeado de una capa de material aislante o dieléctrico, rodeada a su vez por una malla de hilos conductores cubierta por una funda de material aislante y protector, Formado así cuatro capas concéntricas.
- ✓ **Twinaxial.** Este tipo de cable es una variación del coaxial que dispone de dos conductores centrales, envueltos cada uno en un aislante. Se utiliza en instalaciones de redes de tipo token ring.
- ✓ **Par trenzado apantallado (STP, Shielded Twisted Pair).** Este tipo de cable está formado por grupos de dos conductores cada uno con su propio aislante trenzados entre sí y rodeados de una pantalla de material conductor, recubierta a su vez por un aislante. Cada grupo se trenza con los demás que forman el cable y, el conjunto total se rodea de una malla conductora y una capa de aislante protector. Esta disposición reduce las interferencias externas, las interferencias entre pares y la emisión de señales producidas por las corrientes que circulan por el cable.
- ✓ **Par trenzado sin pantalla (UTP, Unshielded Twisted Pair).** En este tipo de cable, los conductores aislados se trenzan entre sí en pares y todos los pares del cable a su vez. Esto reduce las interferencias entre pares y la emisión de señales. Estos cables se utilizan, sobre todo, para los sistemas de cableado integral, combinando telefonía y redes de transmisión de datos, principalmente.
- ✓ **Fibra óptica.** Las fibras se utilizan como guías de haces de luz láser sobre los cuales se modulan las señales que transmiten la información, permitiendo que la luz describa trayectorias curvadas, necesarias para poder instalar las redes en los edificios.

2.3.1.2.2 Redes Inalámbricas: Tienen Conexión por medio de ondas electromagnéticas como se detalla en la imagen 5.



Imagen 5: Redes Inalámbricas

Fuente: <https://www.youtube.com/watch?v=tpuiYms6Gaw>

- ✓ **Radio.** Las ondas de radio fueron el primer medio utilizado para transmitir información y, gracias a los avances tecnológicos como la telefonía celular y el auge de los equipos portátiles, se están convirtiendo en uno de los medios de transmisión más utilizados en la actualidad.
- ✓ **Luz.** La luz se utilizó aún antes que la radio para transmitir información, ya los griegos utilizaban espejos para comunicarse con sus barcos en el mar. Pero ha sido necesario mejorar los sistemas de producción de luz láser para permitir transmitir información electrónica con velocidades similares a los cables. Ya existen equipos que pueden establecer enlaces de varios kilómetros a 5-10 Mbits/s con un costo alrededor del millón de pesetas.

2.3.1.3 Redes según su topología

TOPOLOGÍA: o forma lógica de una red se define como la forma de tender el cable a estaciones de trabajo individuales; por muros, suelos y techos del edificio. Existe un número de factores a considerar para determinar cuál topología es la más

apropiada para una situación dada. La topología en una red es la configuración adoptada por las estaciones de trabajo para conectarse entre sí.

- ✓ **Red Bus o Lineal**, consiste en un cable principal con ramales como se evidencia en la imagen 6.

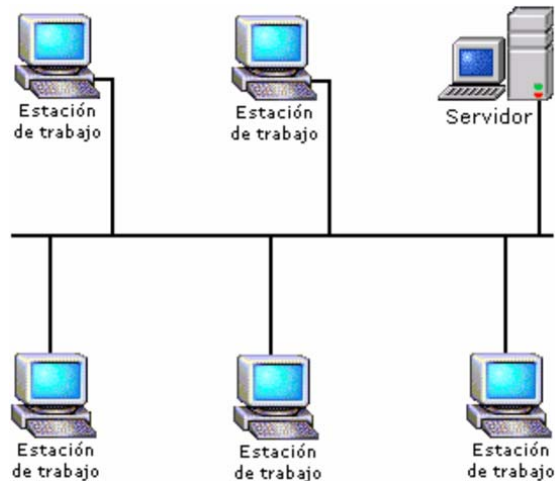


Imagen 6: Red Bus o Lineal

Fuente: <https://www.youtube.com/watch?v=tpuiYms6Gaw>

- ✓ **Red Estrella**. Los Pc's no están conectados entre sí sino que todos van un concentrador central tal como lo describe la imagen 7.

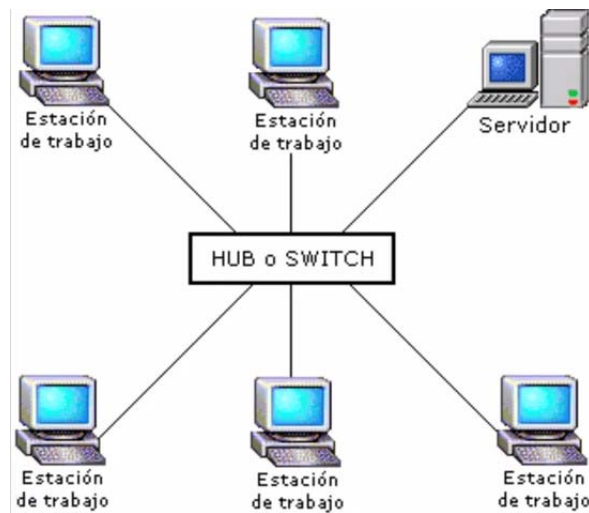


Imagen 7: Red Estrella

Fuente: <https://www.youtube.com/watch?v=tpuiYms6Gaw>

- ✓ **Red Anillo.** Los dispositivos forman un anillo en su conexión, la información llega al ordenador que lo necesita caso contrario pasa al siguiente ordenador según se observa en la imagen 8.

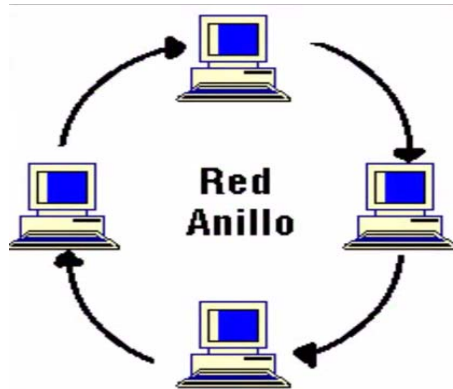


Imagen 8: Red Anillo

Fuente: <https://www.youtube.com/watch?v=tpuiYms6Gaw>

Red Malla: Los ordenadores se conectan entre sí con varios cables como lo muestra la imagen 9.

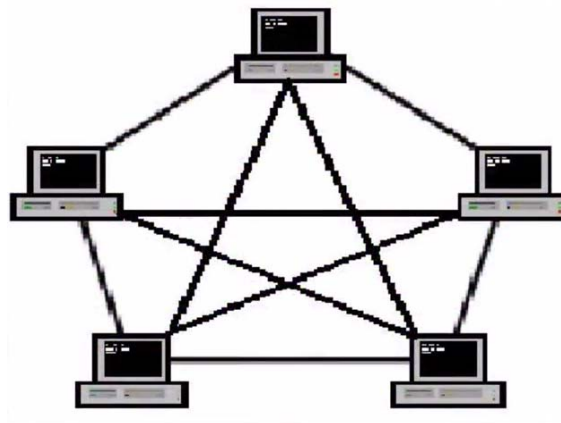


Imagen 9: Red Malla

Fuente: <https://www.youtube.com/watch?v=tpuiYms6Gaw>

2.3.2 CABLEADO ESTRUCTURADO

2.3.2.1 Definición de Cableado Estructurado

El sistema de cableado es un elemento crítico de cualquier red. Existe un alto grado de probabilidad que los errores en general de un sistema sean causados por el

cableado y por tanto es muy esencial para que un sistema de comunicaciones de datos sea eficaz.

El sistema de cableado estructurado comienza en el punto en que el proveedor de servicios (SP) termina. Este punto es el punto de demarcación o un dispositivo de interfaz de red (NID).

El Cableado Estructurado sirve para la integración y administración de tecnologías en edificios comerciales y ambientes de oficina servicios de voz de datos de alta velocidad, videos, dispositivos de control, seguridad y automatización de edificios, edificios inteligentes conectados independientemente de las aplicaciones.

2.3.2.2 Estándares para cableado

Las normas y estándares son necesarios para establecer el diseño de un sistema de cableado estructurado con el fin de construir y gestionar según la necesidad que se presente, se compone por bloques con características específicas. Los bloques están organizados jerárquicamente dentro de un sistema de comunicación unificado. Un bloque de LAN. Los estándares han evolucionado para apoyar las tecnologías de red de alta velocidad

El cableado estructurado define un sistema de cableado de telecomunicaciones genérico para edificios comerciales y está conformado por: cables, conectores y accesorios utilizados para conectar equipos de red como el sistema telefónico local dentro de un edificio.

La industria del cableado EE.UU. acepta la American National Standards Institute (ANSI), en conjunción con la norma TIA / EIA, como la organización responsable de proporcionar y mantener las normas y prácticas dentro de la profesión. Se ha publicado una serie de normas para diseñar, instalar y mantener instalaciones de cableado. Estos ayudan a garantizar una instalación correcta de cableado.

El término estándar de la industria, para una instalación de red que sirve a un área relativamente pequeña (por ejemplo, una instalación de cableado estructurado que sirve un edificio) es una red de área local (LAN).

Las áreas que mantienen un cableado estructurado tienen los siguientes elementos según muestran las imágenes 10 y 11:

- ✓ Instalaciones de entrada
- ✓ Vías de cadena principal vertical y horizontal;
- ✓ Los cables troncales vertical y horizontal
- ✓ Vías horizontales
- ✓ Cables horizontales
- ✓ Salidas del área de trabajo
- ✓ Salas de equipos
- ✓ Armarios de telecomunicaciones
- ✓ Conexión cruzada instalaciones
- ✓ Multiusuario conjuntos de tomas de telecomunicaciones (MUTOA)
- ✓ Puntos de transición
- ✓ Puntos de consolidación.

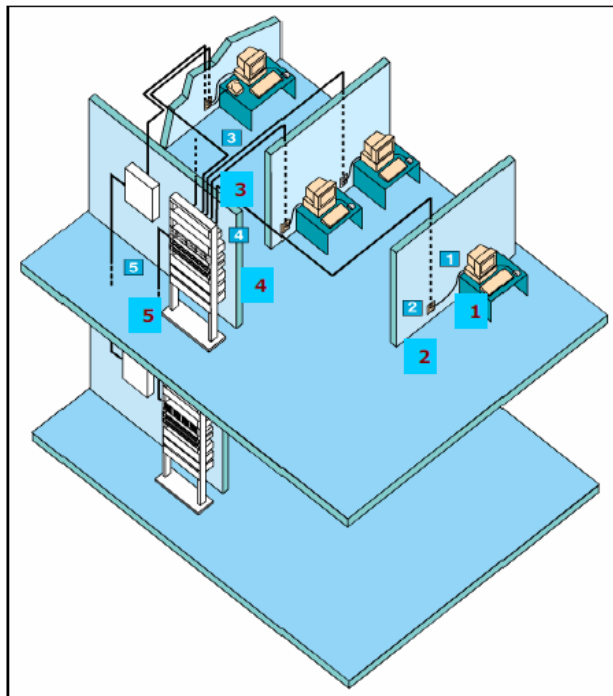


Imagen 10: Cableado Estructurado

Fuente: cableado-estructurado-de-red-1204886726520124-4.pdf

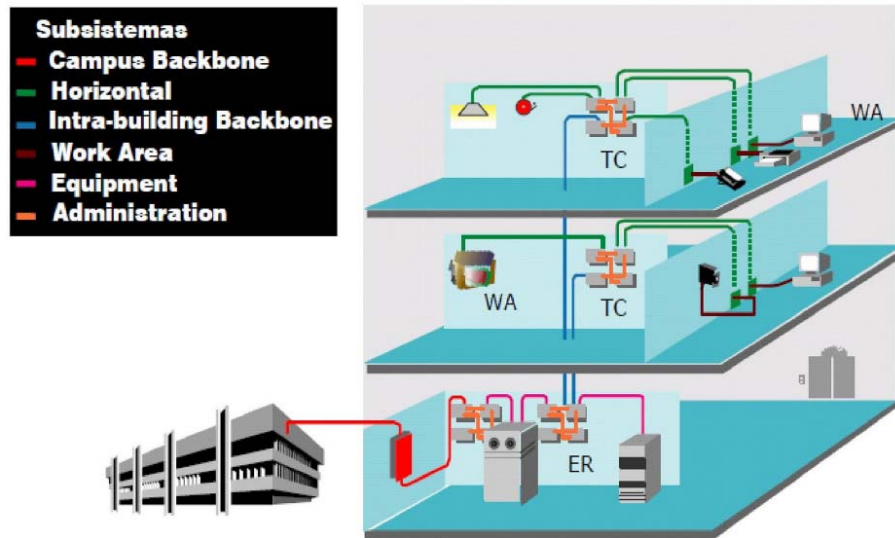


Imagen 11 : Esquema de un sistema de Cableado Estructurado

Fuente: <http://oscarpradosistemas1anoche.blogspot.com/2010/03/cableado-estructurado.html>

2.3.3 GENERALIDADES DE SISTEMAS DE VIDEO VIGILANCIA

Un sistema de video vigilancia usa cámaras para grabar ciertos tipos de circunstancias a cualquier hora ya sea en el día o en la noche. Este tipo de circunstancias pueden ser accidentes robos, entre otras cosas y de acuerdo a esto tomar acciones. Actualmente existen dos grandes tipos de circuito; cerrado de TV CCTV y de las cámaras IP's. También hay que incluir un tercer tipo que es una opción no tan usada y básica que son las web cam.

Estás cámaras son las que se usan para hacer video llamadas a través de Skype. También sirven para vigilar un área determinada, grabar vídeos, y visualizar imágenes a través de internet entre otras cosas.

2.3.3.1 Características de los sistemas de video vigilancia

Se resaltan varias características de las cámaras IP, de las cámaras de circuito cerrado y de las webcam, por ejemplo: el método de grabación en una webcam siempre va a ser la PC en el caso de las cámaras IP es el dispositivo por el que siempre van a grabar.

En el caso de la CCTV de circuito cerrado el dispositivo directo siempre va a ser un DVR que también con la ayuda de un software se puede pasar dichos videos o grabaciones a una PC.

El tipo de cable que la webcam usa es un cable USB de alcance mayor de entre 3 a 5 metros, en el caso de las cámaras IP usa cable UTP y su alcance máximo es de 100 metros. En el caso de las CCTV usa un cable coaxial de 100 hasta 300 metros e incluso un poco más que dependen de la categoría que se llegue a comprar.

2.3.4 Redes IP

Dirección IP es lo que identifica a un dispositivo dentro de una red. Este número de IP no puede ser repetido porque de esa manera hay conflictos en la red para identificar a las computadoras.

2.3.4.1 Direccionamiento IP

Se dice que el direccionamiento IP de una red es el conjunto de parámetros o reglas que permiten la organización de los equipos en un grupo y estas reglas son:

- **IP:** Es un número que permite identificar un computador y hacerlo visible en un conjunto de ordenadores en la red, en el internet para realizar una correcta comunicación. Para compartir información es necesario ser visible y para eso se utiliza en los equipos informáticos una dirección IP.
- **Máscara de red:** Una máscara de subred es un número de 32 bits que enmascara una dirección IP, y divide la dirección IP en la dirección de red y la dirección del host. La máscara de subred se hace mediante el establecimiento de bits de red para todos "1" s y el establecimiento de los bits de host serán todos "0" s. Dentro de una red dada, dos direcciones de host están reservadas con fines especiales, y no pueden ser asignados a los hosts. El "0" dirección se asigna una dirección de red y "255" se asigna a una dirección de difusión, y no puede ser asignado a los hosts.
- **Puerta de enlace:** Es la dirección IP de un equipo físico con funciones NAT, que permite la comunicación o salida de los dispositivos de una red LAN hacia la red externa. Esta IP se puede seleccionar de cualquier Host disponible dentro de un Rango IP definido por la máscara de red

- **DNS (Domain Name System):** Convierte las peticiones o URL de un usuario en direcciones IP y viceversa de esta forma permite al usuario escribir direcciones de dominio en el navegador y no direcciones IP.

2.3.4.2 Direccionamiento interdominio sin clase

Las redes modernas ya no utilizan el direccionamiento IP con clase, y la máscara de subred no se puede determinar mediante el valor del primer octeto. Los protocolos de routing IPv4 sin clase (RIPv2, EIGRP, OSPF e IS-IS) incluyen la información de la máscara de subred con la dirección de red en las actualizaciones de routing. Los protocolos de routing sin clase admiten VLSM y CIDR.

Los protocolos de routing IPv6 son protocolos sin clase. Por lo general, la distinción entre los protocolos de routing con clase y sin clase se aplica únicamente a los protocolos de routing IPv4. Se considera que todos los protocolos de routing IPv6 son protocolos sin clase, dado que incluyen la duración de prefijo con la dirección IPv6.

El direccionamiento interdominio sin clase (CIDR o superred) es una manera de combinar varios rangos de direcciones de clase C y formar una única red o ruta. Este método de direccionamiento añade direcciones IP de clase C. Estas direcciones las reparten los proveedores de servicios Internet (ISP) a sus clientes para que éstos las utilicen. Las direcciones CIDR pueden reducir el tamaño de las tablas de direccionamiento y hacer que haya más direcciones IP disponibles en la empresa.

Antes, era necesario entrar una máscara de subred que fuese igual o mayor que la máscara necesaria para la clase de red. En el caso de las direcciones de clase C, esto significaba que la subred 255.255.255.0 era la de mayor tamaño (253 sistemas principales) que se podía especificar. Para conservar las direcciones IP, cuando las empresas necesitaban más de 253 sistemas principales en una red, Internet emitía varias direcciones de clase C. Esto complicaba la configuración de las rutas y otras cuestiones.

Ahora, CIDR permite que estas direcciones de clase C contiguas se combinen y formen un único rango de direcciones de red gracias a la utilización de la máscara de subred. Por ejemplo, si se reparten cuatro direcciones de red de clase C (208.222.148.0, 208.222.149.0, 208.222.150.0 y 208.222.151.0 con la máscara de subred 255.255.255.0), se podría pedir al ISP que las convirtiese en una superred por

medio de la máscara de subred 255.255.252.0. Esta máscara combina las cuatro redes en una sola a efectos de direccionamiento. CIDR es provechoso porque reduce el número de direcciones IP asignadas pero innecesarias.

2.3.4.3 Internet

Una interconexión de redes es un conjunto de redes individuales, conectadas por medio de dispositivos de red intermedios, que funciona como una única red de gran tamaño.

2.3.4.4 Protocolos

Los protocolos son el conjunto de reglas usadas por los dispositivos para que se comuniquen entre sí y no es suficiente con estar conectados a la misma red sino que además debe entenderse. Los protocolos son fundamentales ya que permiten establecer el idioma común.

2.3.4.5 Protocolos TCP/IP

Los protocolos de la familia TCP/IP son la base de internet:

- **Transmisión Control Protocol (TCP):** Es un protocolo que permite que la comunicación entre los ordenadores se realice libre de errores, sin pérdidas y con seguridad. Se encarga básicamente de los siguientes procesos:
 - ✓ Establecimiento de la conexión
 - ✓ Transferencia de datos
 - ✓ Fin de la conexión
- **Internet Protocol (IP):** Se encarga de enviar los datos en bloques conocidos como paquetes. Además define las direcciones de las máquinas de origen y destino (direcciones IP). Sin embargo IP no proporciona mecanismos para saber si los datos transmitidos llegan a su destino correctamente (se ocupa TCP).

Una dirección IP permite identificar lógicamente y jerárquicamente los dispositivos (ordenadores, móviles) en una red que utiliza el protocolo IP. Actualmente se utiliza la versión IPv4 que usa direcciones de 32 bits (2^{32}) direcciones sin embargo el crecimiento de internet provoca que estas direcciones se agoten

por esta razón la próxima versión del protocolo la IPv6 que utiliza direcciones de 64 bits es decir (2^{64}) direcciones.

DNS, transforma las direcciones IP de la red en términos más sencillos de utilizar por las personas. Permite localizar y direccionar los dispositivos que utilizan este protocolo a nivel mundial.

- **Hypertext Transfer Protocol (HTTP):** Este protocolo es uno de los más importantes y básicos de internet. Ha sido desarrollado por el w3c permite la transferencia de documentos de tipo “hipertexto” es decir documentos que permiten acceder a otros documentos mediante “enlaces”.

Ejemplo: <http://centos-webpanel.com/features>

Las páginas web están desarrolladas en un lenguaje de tipo hipertexto denominado HTML, que por tanto se puede transmitir y usan el protocolo HTTP.

HTTP utiliza el esquema petición-respuesta entre un cliente y un servidor.

El esquema básico para acceder a una página web desde el navegador es el siguiente:

- ✓ El navegador web es el cliente.
- ✓ Una computadora que almacena la información sobre esta página web es el servidor.
- ✓ Desde el navegador solicita la página (petición).
- ✓ Desde el servidor envía la página (respuesta)
- ✓ El navegador muestra la página

Se puede observar las capas del modelo de referencia para TCP/IP en el cuadro 1 e imagen 12.

Cuadro 1: Modelo de referencia para TCP/IP

| | |
|-------------------------|----------------------------------|
| Capa de aplicación | (HTTP, SMTP, FTP, TELNET) |
| Capa de transporte | (UDP, TCP) |
| Capa de red | (IP) |
| Capa de acceso a la red | (Ethernet, Token Ring...) |
| Capa física | (cable coaxial, par trenzado...) |

Fuente : <http://www.saulo.net/pub/tcpip/a.htm>

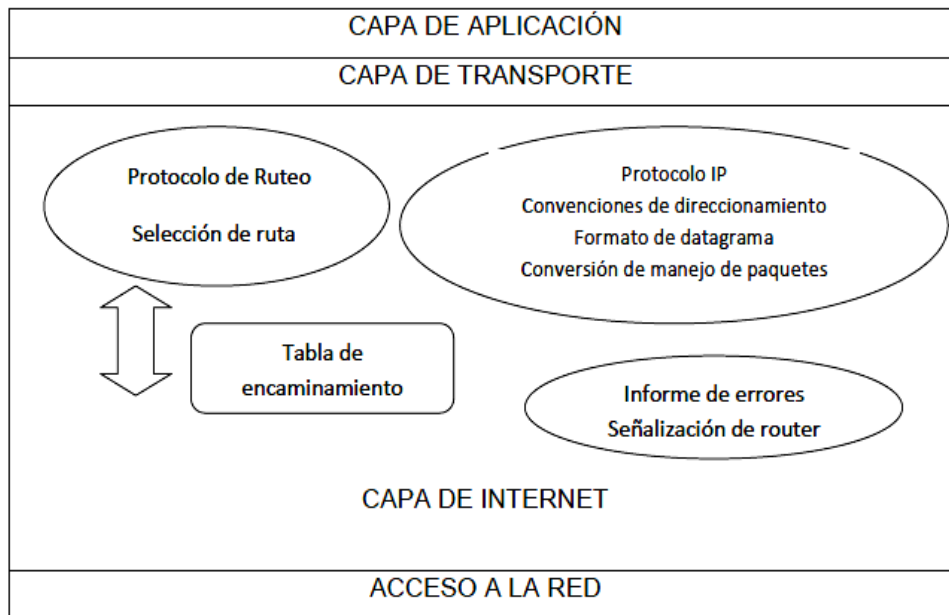


Imagen 12: Elementos de una capa de red

Fuente: <http://www.saulo.net/pub/tcpip/a.htm>

2.3.4.6 Direccionamiento IPv4

En la imagen 13 se observa la cabecera en IPv4:

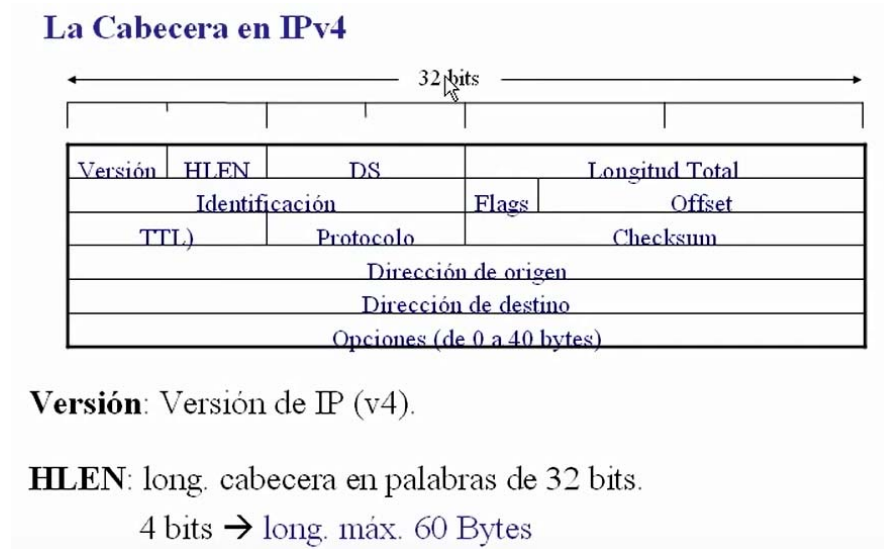


Imagen 13: Cabecera en IPv4

Fuente: <http://www.saulo.net/pub/tcpip/a.htm>

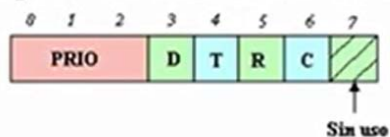
La parte horizontal es de 32bits, existen 5 campos, 5 palabras de 32 bits que son obligatorias, se encuentra una parte opcional que va desde 0 a 40 bytes con lo cual figura 5 palabras de 32 bits que son 20 bytes obligatorios en la cabecera IPv4 más una partición de hasta 40 bytes en IPv4.

Se analiza cada uno de los campos de la cabecera y se toma en cuenta los más importantes que son los de segmentación y ensamblado. En primer lugar está el campo de versión que son 4 bits donde se codifica, 4 es la versión de IP que se analiza.

En segundo lugar existen 4 bits de la longitud de la cabecera representada en palabras de 32 bits como son 4 bits y se puede codificar desde cero hasta 15 con lo cual la longitud máxima es de 15 palabras de 32 bits que son 60 bytes como se muestra en la imagen 14.

La Cabecera en IPv4

Campo DS: QoS requerida para una transmisión. Lo rellena quien envía el datagrama.



PRIO: (Valor 0: datagrama normal; 7: datagrama control).

D (Delay): Se requiere bajo retardo.

T (Throughput): Se requiere alto throughput.

R (Reliability): Se requiere alta fiabilidad.

C (Cost): Se requiere bajo coste.

Sólo se puede poner a '1' uno de los campos D, T, R o C.

Imagen 14: Campos DS de la Cabecera de IPv4

Fuente: <http://www.saulo.net/pub/tcpip/a.htm>

A continuación muestra el campo de servicio en donde se indica la calidad de servicio requerido para una transmisión y este campo de 8 bits, está compuesto por el emisor del datagrama

Existen 3 bits en el campo de prioridades y a continuación 5 bits de los cuales hay uno que no se usa. El campo de prioridades con 3 bits se puede codificar desde cero hasta siete y codifica la prioridad del datagrama de tal manera que si hay un valor cero es un datagrama normal y un valor 7 es de máxima prioridad la máxima prioridad se dará a los datagramas que lleven información de control.

A continuación se encuentran 4 bits donde se indica cuál es la calidad de servicio que se requiere para ese datagrama, solamente puede haber un bit de estos cuatro activado y en función de cuál esté activado tiene un sentido u otro. Si se activa el bit D, el primero de los 4 requiere que el datagrama se envíe por aquellas líneas de bajo retardo. En cambio sí se activa el bit T de Throughput requiere que se envíe por aquellas líneas de ancho de banda el más elevado.

Y si está activado el bit R de Reliability se requiere que se envíe por las líneas de mayor fiabilidad. Si se activa el bit C de Cost se requiere que se envíe por las líneas de menor costo. Luego aparece el campo de longitud total que son 16 bits También incluye la longitud total de datagrama Incluida la cabecera en bytes Con lo cual la longitud máxima sea de 65535 bytes.

El campo protocolo que especifica qué protocolo está encapsulado dentro del datagrama IP. R campo de Checksum: Es un campo de comprobación de errores que comprueba la parte de la cabecera, no comprueban los datos con lo cual cada vez que el datagrama es recibido por un nodo se comprueba el checksum y si todo es correcto se reenvía. El checksum debe ser recalculado y por esa razón el checksum se modifica igual que el TTL en cada salto.

El campo de direcciones IP: De origen y destino ambas a 32 bits cada una ya que esas son las longitudes de las direcciones ipv4 y finalmente está el campo de opciones que incluye las opciones de las que se puede hacer uso en IPv4. Como por ejemplo en este campo guarda un registro de todos los nodos o todas las direcciones IP por los que se pasó. Como la longitud máxima son 40 bytes como máximo sólo cabe 10 direcciones de 10 nodos por los que pasó este datagrama.

Campos de Segmentación y re-ensamblado: El identificador tiene un número de secuencia de tal manera que cuando un datagrama es segmentado y forma datagramas más pequeños llamados datagramas hijos en los cuales se copia el número del identificador que contiene el datagrama original de tal manera que todos los datagramas hijos llevan el mismo identificador.

Offset: Indica la posición de los datos en el datagrama segmentado con respecto a la posición que tiene en el datagrama original y se indica el offset medida o unidades de 64 bits o de 8 bytes.

Antes del offset hay Flags de 3 bits de los cuales solamente se usan 2 que significan lo siguiente:

- ✓ DF "Do Not Fragment": Indica si el datagrama puede o no ser fragmentado en ruta si está 0 significa que puede ser fragmentado y si está en 1 indica que no puede ser fragmentado, esto no activa el que genera el origen del datagrama para indicar si desea que la información que envía pueda ser manipulada en ruta.
- ✓ MF "More Fragments": Se pone en cero si el datagrama es el último segmento, es decir los datagramas hijos llevarán este bit 1 excepto el datagrama que ocupa en la última.

2.3.4.7 Diferencias entre IP fija e IP Dinámica

Una IP es un número o credencial que ocupa una computadora alrededor del mundo para conectarse a internet. La IP dinámica es la que cambia constantemente y depende del proveedor mientras que la IP fija es la que nunca cambia. Si la empresa o el hogar no brinda cualquier tipo de servicios entonces se puede usar una IP dinámica, caso contrario si se brinda servicios como que se puede ser un servidor de mails, servidor de páginas web, servidor de video de cámaras de seguridad o cualquier otro dispositivo que se conecte a internet entonces es recomendable tener una IP fija.

2.3.4.8 Direccionamiento IPV6

Se observa detalladamente en la imagen 15 la notación de las direcciones IPV6.

IPv6 Notación de direcciones

Un dígito hexadecimal = 4 bits

| Dec. | Hex. | Binary | Dec. | Hex. | Binary |
|------|------|--------|------|------|--------|
| 0 | 0 | 0000 | 9 | 9 | 1000 |
| 1 | 1 | 0001 | 10 | A | 1010 |
| 2 | 2 | 0010 | 11 | B | 1011 |
| 3 | 3 | 0011 | 12 | C | 1100 |
| 4 | 4 | 0100 | 13 | D | 1101 |
| 5 | 5 | 0101 | 14 | E | 1110 |
| 6 | 6 | 0110 | 15 | F | 1111 |
| 7 | 7 | 0111 | | | |

Parte 2

2001:0DB8:AAAA:1111:0000:0000:0000:0100/64

1 2 3 4 5 6 7 8

2001 : 0DB8 : AAAA : 1111 : 0000 : 0000 : 0000 : 0100

16 bits 16 bits 16 bits 16 bits 16 bits 16 bits 16 bits 16 bits

- Las direcciones IPv6 son 128-bit representados en:
 - 8 segmentos o "hextets" (no es un termino formal)

Imagen 15: Formato de una dirección IPv6

Fuente: <http://revistas.udistrital.edu.co/ojs/index.php/REDES/article/view/6366/9466>

La notación para IPv6 se basa en el sistema hexadecimal, el sistema hexadecimal a diferencia de sistema decimal tiene 16 dígitos, El sistema decimal tiene dígitos del 0 al 9 el sistema hexadecimal tiene dígitos del 0 hasta la letra F.

La nomenclatura de la IPv6 está formada por 8 segmentos de 4 dígitos hexadecimales cada uno y cada uno de 4 bits y se puede decir que cada segmento ocupa 16 bits separados por dos puntos que no existen en IPv4.

En IPv4 el rango era entre 0 y 255 en IPv6 hexadecimal los valores son desde 0000 hasta FFFF .Las direcciones IPv6 son de 128 bits representadas en 8 segmentos.

Existen dos reglas para compactar la ipv6:

- **0's iniciales.**- Los ceros iniciales o a la izquierda en cualquier segmento de 16 bits no se los escribe como muestra la imagen 16.

```
3ffe : 0404 : 0001 : 1000 : 0000 : 0000 : 0ef0 : bc00
3ffe : 404 : 1 : 1000 : 0 : 0 : ef0 : bc00
```

Imagen 16: 0's Iniciales

Fuente: <http://www.rincondebits.com>

- **Doble dos puntos “::”.**- Esta segunda regla puede reducir aún más esta IP. Es posible reducir, una única vez, una secuencia de ceros contiguos en uno o más segmentos de 16 bits, por doble dos puntos “::”

Sólo se puede aplicar esta regla una única vez para evitar ambigüedades y las dos opciones válidas se detalla en la imagen 17.

```
2001 : 0d02 : 0000 : 0000 : 0014 : 0000 : 0000 : 0095
2001 : d02 :: 14 : 0 : 0 : 95
2001 : d02 : 0 : 0 : 14 :: 95
```

Imagen 17: Doble dos puntos

Fuente: <http://www.rincondebits.com>

2.4 VIDEO VIGILANCIA

Estas aplicaciones pueden evitar el robo y el vandalismo con el monitoreo y más aplicaciones.

Mediante la combinación de características avanzadas de la cámara con unas robustas carcasas para exteriores o diseño de la cámara discreta, una cámara IP se puede instalar en casi cualquier lugar. Esto las hace ideales para la vigilancia dentro y fuera de las empresas y oficinas, grabación en ubicaciones remotas, o la grabación de vídeo de alta calidad para identificar a las personas sospechosas. En la imagen 18 se observa la estructura básica de un sistema de video vigilancia.

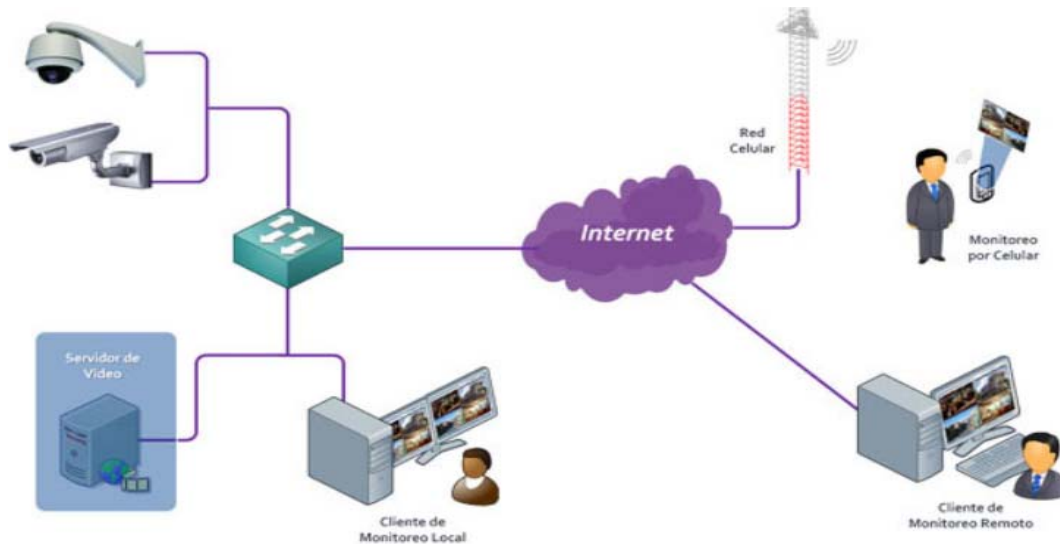


Imagen 18: Representación de un Sistema de Vigilancia IP inalámbrica

Fuente: <http://www.dointech.com.co/video-vigilancia-ip.html>

2.4.1.1 Ventajas de la vigilancia IP inalámbrica

- Los servicios inalámbricos de banda ancha basados en Wi-Fi pueden ser utilizados para los sistemas públicos de vigilancia (vigilancia de una localidad, calle, cruces de carreteras, etc.).
- Las cámaras de vigilancia inalámbricas pueden ser útiles en situaciones en las que es difícil tender cables - Los museos, edificios patrimoniales, plantas industriales, etc.
- El sistema de vigilancia inalámbrica es rentable (en comparación con las redes de cable que implican Cables de Fibra, excavación de zanjas, etc.) para instalar y mantener.
- Las redes inalámbricas se pueden implementar de forma rápida y vigilancia inalámbrica se pueden utilizar para proporcionar temporal Wi-Fi para ferias / exposiciones, etc.
- Un punto-a-punto inalámbrico backhaul de redes puede extender la red a más de 5 km sobre el medio inalámbrico, si es necesario.
- Las redes inalámbricas son bastante seguras en estos días ya que la mayoría de ellos utilizan la autenticación 802.1x y comunicaciones cifradas WPA2.
- Las redes Wi-Fi de malla pueden conectarse entre sí (sobre el medio inalámbrico) para formar una red inalámbrica casi todos en un lugar determinado. Estas redes de malla permiten la propagación de trayectorias

múltiples y pueden elegir automáticamente las vías alternas para evitar un único punto (enlace / dispositivo).

- Las cámaras de vigilancia IP inalámbrica se pueden mover de un lugar a otro sin preocuparse de si la toma del cable / red está disponible en la nueva ubicación. De hecho, toda la configuración inalámbrica (incluye puntos de acceso, etc.) se puede mover a una nueva ubicación con facilidad y rapidez.
- La calidad de las cámaras inalámbricas de interior puede mejorarse mediante el uso de controles inalámbricos para crear y mantener una red inalámbrica.
- Las técnicas de compresión digital como H.264 y H.264 SVC ofrecen un flujo de vídeo de calidad en anchos de banda bajos.

2.4.2 CÁMARAS IP

Una cámara de seguridad IP inalámbrica es un dispositivo que utiliza el protocolo de Internet que sirve para capturar y grabar imágenes. Esto significa que en lugar de utilizar un sistema analógico por cable, una cámara IP inalámbrica funciona mediante el envío de datos a través de una red de área local de otra manera conocido como un LAN. No hay necesidad de instalar cables complicados con este sistema. El hecho de que se observa las imágenes en cualquier dispositivo electrónico que se conecta a Internet es una ventaja. También se observa las imágenes desde cualquier lugar del mundo. El ancho de banda determina el número de cámaras de seguridad inalámbrica que puede instalar en su sistema de cámaras de seguridad. La imagen 19 muestra la estructura interna de la cámara IP.

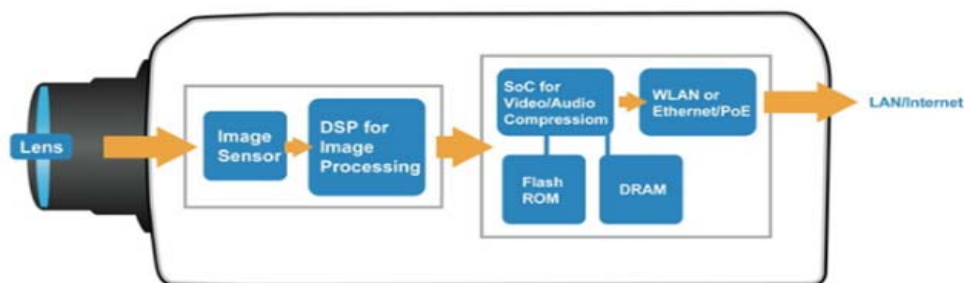


Imagen 19 : Cámara IP y sus partes

Fuente: <https://www.tecnoseguro.com/tutoriales/video-ip/conceptos-basicos-en-comunicaciones-de-video-en-red.html>

La imagen 20 describe la diferencia que existe entre un sistema de seguridad que emplea una cámara IP y una cámara de analógica.

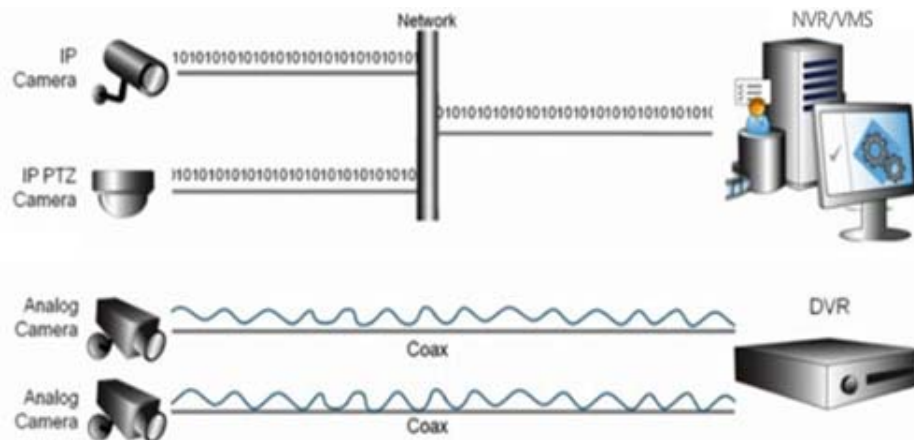


Imagen 20 : CCTV Camera Solution vs IP Camera Solution

Fuente: <http://www.hkvstar.com/technology-news/guide-for-selection-ip-cameras.html>

2.4.2.1 Características de una cámara IP

La mayor tendencia en los sistemas de vigilancia de vídeo es la migración de las cámaras analógicas a la cámara IP. Todas las grabaciones de las cámaras de vigilancia son digitalizadas, tanto para su visualización y almacenamiento utiliza ordenadores. Sin embargo, las cámaras IP digitalizan las señales de vídeo en la cámara, mientras que las cámaras analógicas requieren digitalización codificador de vídeo o DVR.

La cámara IP se compone de lentes, filtros ópticos, sensor CCD, viruta ARTPEC que realizan la función y el controlador de chip de compresión. sensor CCD (Charge Coupled Device) es un elemento básico de la mayoría de las cámaras modernas. Se trata de elementos fotosensibles que componen de fina red de píxeles individuales. La imagen supervisada se centra en a través de un objetivo en la superficie de un elemento y una señal eléctrica se genera en él, que es proporcional a la intensidad de luz que cae sobre ella.

El número típico de píxeles para elementos CCD oscilan entre 250.000 y 500.000 píxeles. El mayor número de píxeles, la mayor calidad de la cámara y la estructura de la cámara IP se da en las que pueden ser controlados a través de cualquier navegador web, es decir, señal de la cámara IP disponibles en la red Internet.

2.4.2.2 Ventajas de la Cámara IP

- La cámara IP en comparación con las cámaras analógicas, tienen mayor resolución de las imágenes.
- El acceso desde cualquier PC conectado a la red requiere DVR.
- Está conectada al servidor web, servidor FTP, correo electrónico, gestión de alarmas, capacidad de programación por medio de la red
- La cámara IP no tiene que estar conectado a la PC, ya que funciona de forma independiente, y puede ser instalado donde quiera que haya una conexión IP.
- Las mayoría de cámaras IP se conectan fácilmente a la infraestructura existente, que tienen la capacidad POE (Power over Ethernet) carga de energía a través del cable de red (datos y carga de energía pasan a través de un cable de red). Las cámaras usadas en este proyecto no tienen esta característica y se instaló tomas para su funcionamiento.
- Algunas cámaras IP disponen de un filtro de infrarrojos automático, este filtro interviene cuando las condiciones de luz bajan y la cámara emite la señal en blanco y negro produciendo más luminosidad, de esta manera aclara la escena con luz infrarroja permitiendo observar en total oscuridad.
- La mayoría de cámaras IP pueden configurarse para grabar localmente en un dispositivo de almacenamiento, poseen sensores de movimiento que permite grabar los eventos solo cuando hay movimiento, evitando ocupar espacio del disco duro.

2.4.2.3 Funcionamiento de la vigilancia ip inalámbrica.

La video vigilancia mejora el control y la seguridad de los negocios. Permite la supervisión del negocio 24 horas desde cualquier lugar usado un dispositivo móvil, desde cualquier ordenador fijo o portátil desde la pantalla de un televisor doméstico.

Aumenta la seguridad del lugar sin contratar personal y permite una conexión rápida con los sistemas de alarma ya que admite una respuesta rápida en caso de incidencias que reduce los intentos de robo.

La cámara IP se encuentra conectada a la red vía cable o wireless a un acces point y no necesita una fuente de energía con un computadora, quiere decir que es independiente de esta sí está prendida o apagada.

Las imágenes 21, 22, 23 y 24 muestran lo que es la vigilancia y el monitoreo del sistema de seguridad IP.

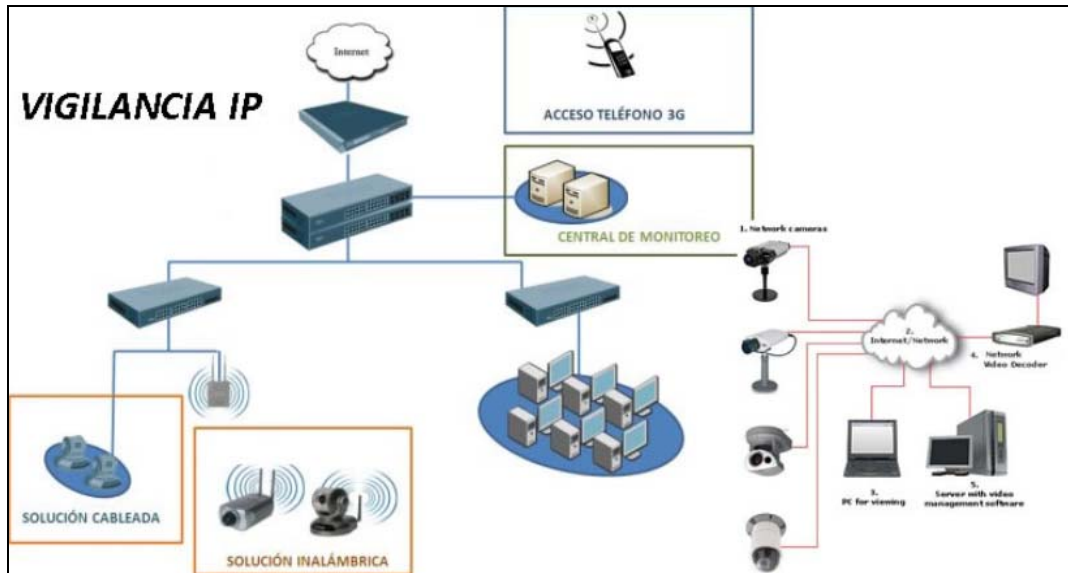


Imagen 21 : Vigilancia

Fuente: <http://www.alamanproyectos.com/camaras-de-seguridad-CCTV.html>

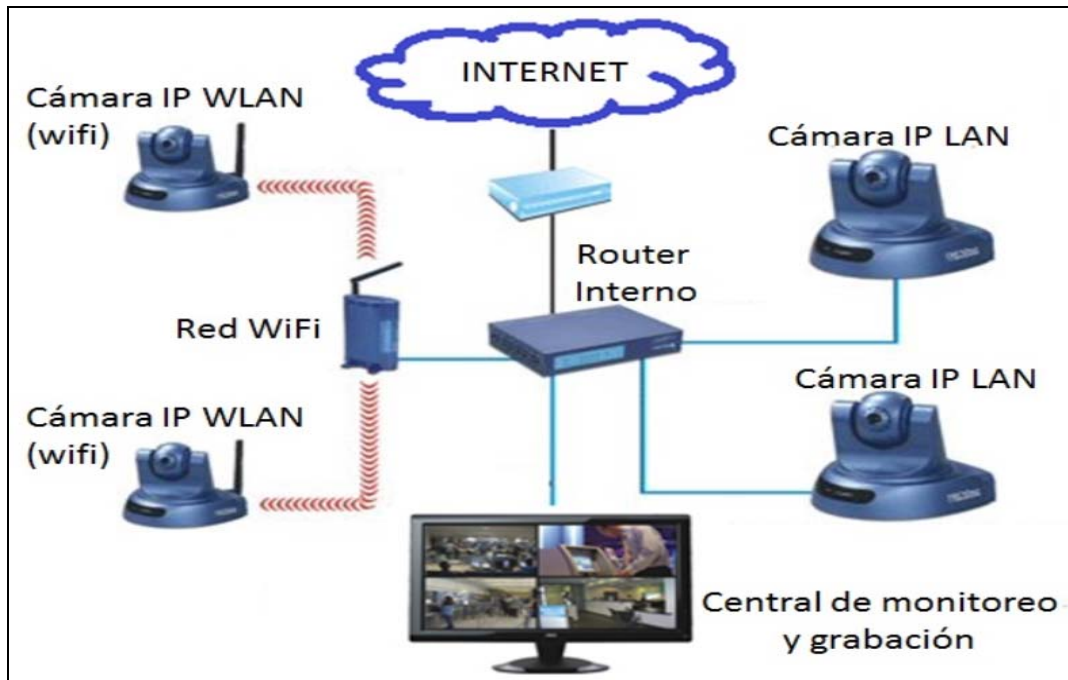


Imagen 22: Monitoreo

Fuente: <http://www.seobogotacolombia.com/productos.html>



Imagen 23 : Visualización de Imagen receptada por una cámara Inalámbrica en un monitor

Fuente: <http://seguridad100.com/?indx=producto&IDProducto=1403>



Imagen 24 : Centro de Control de video vigilancia

Fuente: <http://netkromsolutions.com/seguridad-publica-y-videovigilancia>

2.4.2.4 Monitoreo Remoto

Estas soluciones de seguridad deberá permitir el control de la actividad 24/7, guardar los vídeos de seguridad para su revisión en caso de un incidente. También puede iniciar sesión de forma remota en cualquier cámara y el monitor de su sistema que usa una computadora, tableta o teléfono inteligente si se le notifica de la actividad en el sitio, con una clave de acceso.

2.4.3 TECNOLOGIA OPEN SOURCE

La definición de opensource se divide en tres partes:

- Libertad de uso (Freedom to use) . Implica que todo el mundo puede utilizar el producto, No habrá una versión del producto más costosa que sean las que permita la utilización en su totalidad
- Libertad para modificar (Freedom to Modify), El código puede ser modificado por cualquier desarrollador ya que la licencia no puede discriminar contra un individuo o un grupo.
- Libertad de distribución (Freedom to distribute), Se tiene la libertad de hacer con el producto lo que se desea. Se puede distribuir el mismo modificado o no a través de los medios deseados incluso se puede generar un ingreso del mismo ósea de la modificación si la licencia lo permite. Para que sea una licencia open source debe tener libertad de uso, Libertad de modificar y Libertad en distribución.

Las pequeñas empresas ahorran el 51% y 60% los costes de su negocio para lo cual utilizan software libre en vez de programas con licencia. Los emprendedores pueden adaptar y modificar el programa informático según sus necesidades sin partir de cero. Con el software libre no se pagan licencias ni proveedores privados y se democratiza la informática.

Utilizar software libre te permite ahorrarte el costo de una licencia Y te permite además tener más proveedores entre los que elegir por lo tanto es un poco más la oferta y la demanda.

Con el software libre un informático o un usuario crea un programa para que cualquiera lo utilice estos a su vez lo pueden modificar en función de sus necesidades y liberarlo para que otros también lo usen.

Con el software privado, la empresa crea un programa para un cliente pero éste no se puede cambiar ni ser utilizado libremente. Open Source es una herramienta muy útil para emprendedores y pequeñas empresas ya que pueden arrancar su propia página web o una aplicación para el móvil con un mínimo de costo.

El software libre supone la democratización de las herramientas informáticas en un mundo cada vez más digitalizado. El Hardware y la tecnología de código abierto son una cultura creciente y permite el acceso libre de cómo crear un estilo de vida que

conduce lentamente hacia menos dependencia sobre el sistema de libre mercado capitalista lo que permite desconectar y avanzar en una dirección sostenible y resistente. Sostenible porque permite ser autosuficientes en las comunidades, una tendencia que con el tiempo permitirá a los individuos ser autosuficientes cuando avance lo suficiente.

Resistente porque al aprender cómo funciona la tecnología y como reparar se puede cambiarla y adaptarla a las necesidades particulares, independientemente del lugar en el que se encuentre.

Poseer los conocimientos de cómo funciona la tecnología que utilizas te otorga autonomía también se abre un nuevo camino educativo.

2.4.3.1 Beneficios de las soluciones open source

- La ventaja más obvia de software de código abierto es que puede ser gratis.
- El ejemplo de Ubuntu Linux a diferencia de Windows, puede instalar o distribuir tantas copias de Ubuntu como desee, sin restricciones. Esto puede ser particularmente útil para servidores.
- Si se configura un servidor, sólo puede instalar Linux en él.
- Para configurar un clúster de servidores virtualizados, puede duplicar fácilmente un único servidor de Ubuntu.
- No hay que preocuparse acerca de las licencias y cuántas instancias de Linux que está permitido ejecutar.
- Un programa de código abierto es también más flexible.
- Costes reducidos

3. ARQUITECTURA DEL PROYECTO

3.1 DIAGRAMA DE FLUJO FUNCIONAMIENTO SISTEMA DE SEGURIDAD (Un Evento)

La imagen 25 a continuación describe el funcionamiento de un evento. Las cámaras IP se censan 7/24 hasta cuando existe un movimiento, la cámara recibe una señal, la misma que es enviada al servidor por medio de la red, esta señal hace que el server envíe una notificación al correo y a su vez habilita la opción de grabación mientras dure el movimiento.

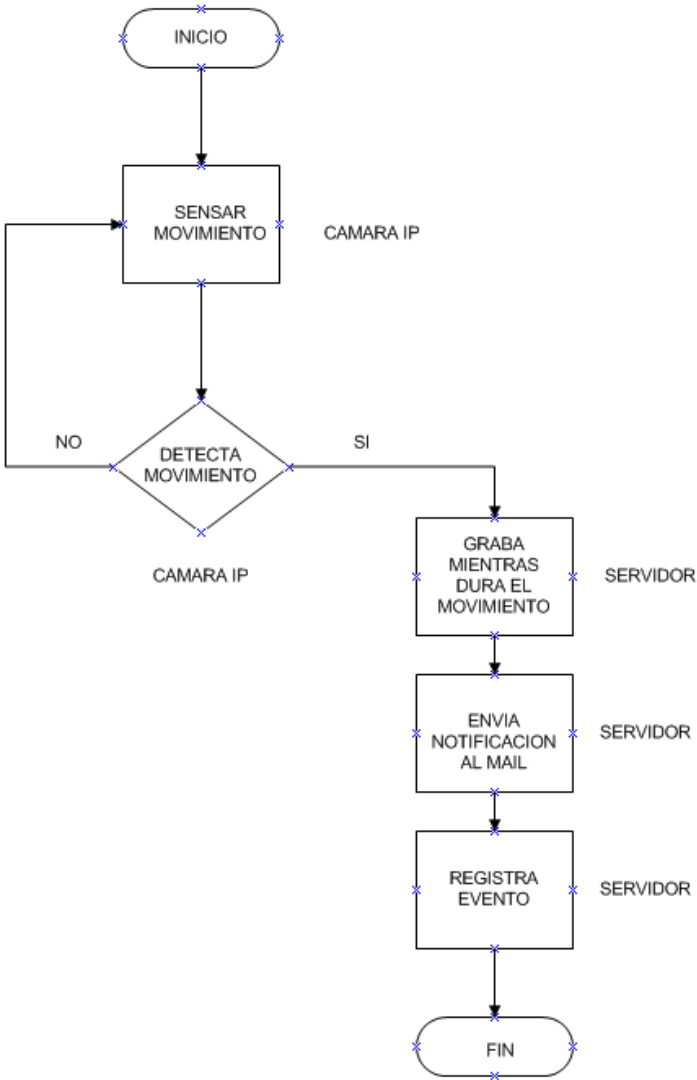


Imagen 25: Funcionamiento sistema de Seguridad

Autor : Dorys Guerrero

Cuando la eventualidad concluyó, la cámara deja de enviar la señal y el servidor abandona su estado de grabación hasta que se presente un nuevo suceso. Por último los movimientos detectados son registrados con los siguientes parámetros.

- ✓ Name, Nombre del Evento
- ✓ Time, Fecha y hora en el que se inició el evento
- ✓ Secs, tiempo transcurrido mientras existe el movimiento

Las eventualidades dependen de los movimientos registrados en el lugar en el que se colocó la cámara y estos pueden ser diferentes en tiempo, hora y fecha. En la imagen 25 se muestra el orden del evento que será repetitivo las veces que sean necesarias.

3.2 CABLEADO ESTRUCTURADO

Se instaló el cableado estructurado en la UEZ, desde la oficina de la Rectora de la institución en planta baja en donde está el servidor con la aplicación hasta el segundo piso en donde se encuentran las cámaras al igual que las tomas eléctricas necesarias para su funcionamiento.

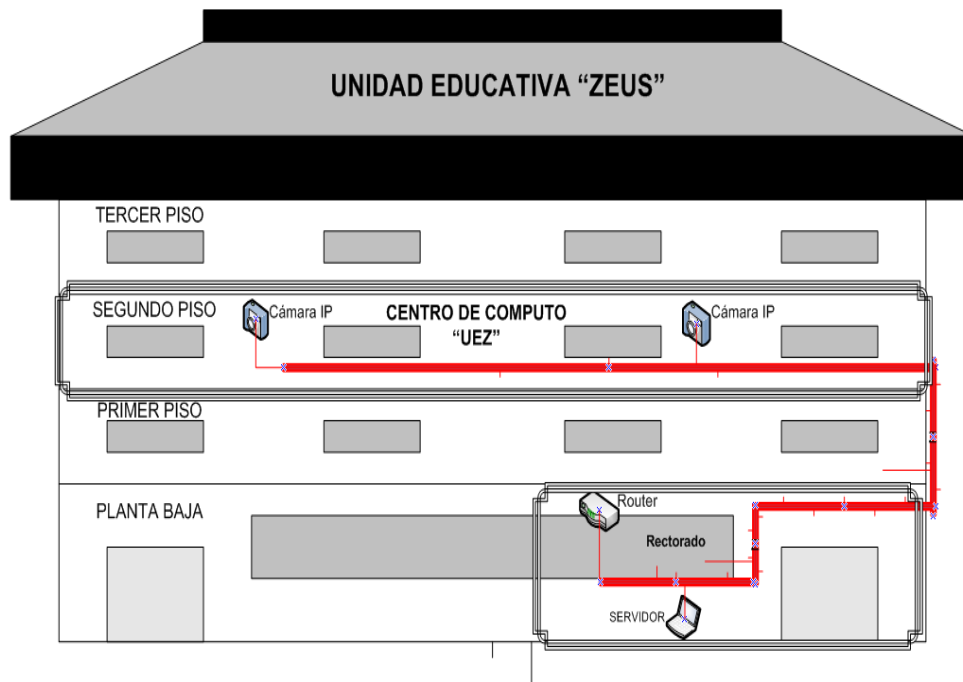


Imagen 26: Cableado Cámaras IP. Vista Frontal

Fuente: Unidad Educativa "ZEUS "

En el Rectorado se encuentra el router del proveedor de Internet y por esa razón es que se toma como origen el lugar en mención, en el cual están conectadas las cámaras IP por medio del cableado cat. 6. Todo lo mencionado anteriormente está detallado en la imagen 26.

3.3 UBICACION CÁMARAS IP

Para ubicar las cámaras se considera los puntos más vulnerables si se considera probabilidades de intento de robo en el centro de cómputo a proteger. Las mismas apuntan a dichos sectores.

En la imagen 27 se muestra la vista superior en la que distingue e identifica las cámaras, accesos al espacio a proteger y el 2 do piso en general.

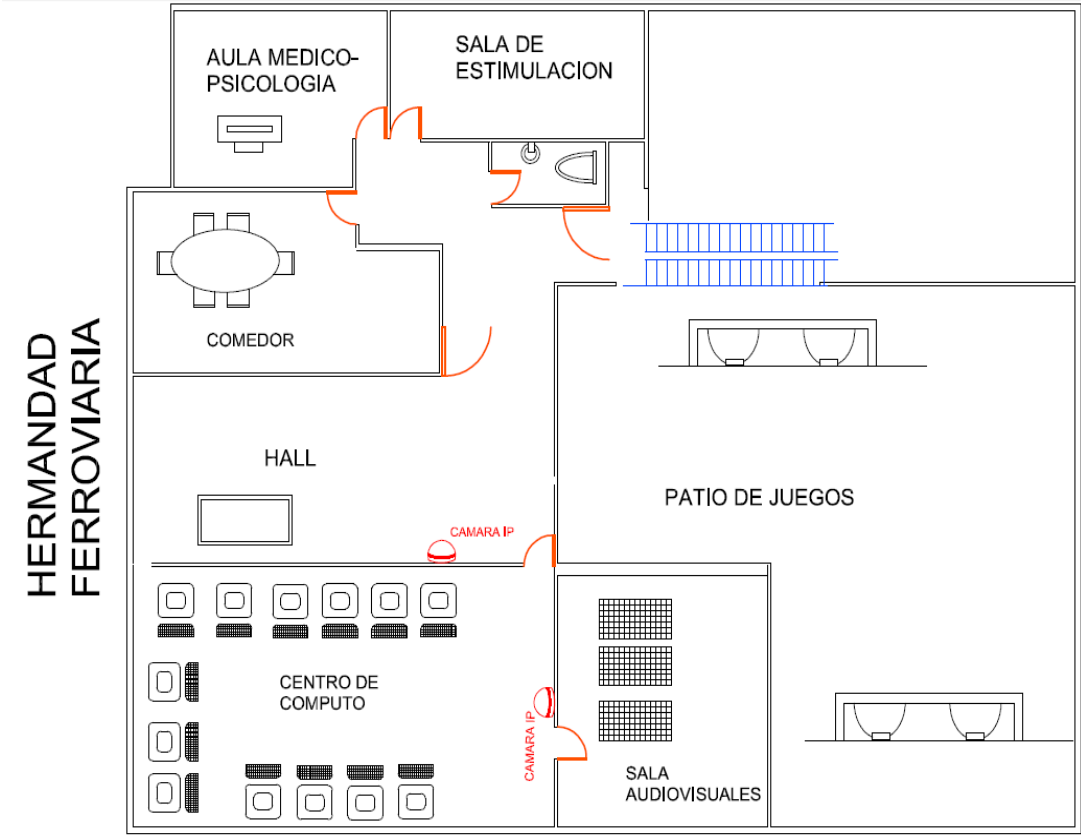


Imagen 27: Ubicación Cámaras IP (Vista Superior)

Fuente: Unidad Educativa “ZEUS “

3.4 Cámaras IP JideTech HD 1.0 MegaPixel

Se utilizó la cámara IP JideTech HD 1.0 MegaPixel principalmente por su tamaño, la visión nocturna como una de sus funcionalidades más importante , sensor de movimiento, para su control se puede usar protocolos de red, tiene una aplicación que es soportada por Iphone y Smartphone. La cámara descrita corresponde a la imagen 28.



Imagen 28: Cámaras IP

Fuente: Unidad Educativa “ZEUS

Las cámaras tienen una cobertura de imagen y video de 15 metros, distancia suficiente para cubrir el espacio a ser tratado. En la imagen 29 se muestra como queda ya instalada una de las cámaras y en la imagen 30 muestra el alcance dela misma.



Imagen 29 : Ubicación Cámara IP 1 (Vista inferior)

Fuente: Unidad Educativa “ZEUS



Imagen 30: Vista y alcance de la cámara IP

Fuente: Unidad Educativa “ZEUS “

Las ventanas que se observan en el fondo de la sala son las que se van a monitorear pues es el área considerada como vulnerable ante cualquier siniestro inesperado.

El servidor administrador de las cámaras será instalado en una oficina del primer piso en donde se encuentra la dirección de la UEZ., pues se compartirá el internet existente en el área .

Las cámaras estarán conectadas al server con cable UTP cat 6 para aprovechar al máximo las características técnicas de las mismas, por tanto el cableado se distribuirá desde el primer piso en donde se encuentra el server hasta el segundo piso en donde están ubicadas las camaras IP como lo muestra la imagen 31 .



Imagen 31: Vista posterior para el cableado

Fuente: Unidad Educativa “ZEUS”

3.5 SOFTWARE BASE

3.5.1 CENTOS 6.5

Es un sistema basado en Linux que se utiliza en servidores. Es un versátil y poderoso sistema operativo con licencia libre “programático libre”, esto significa que el usuario puede destruir o modificar el sistema operativo de acuerdo a necesidades específicas siempre que se incluya el código fuente como lo indica la licencia pública generada. En el cuadro 2 se describe los requerimientos técnicos básicos del hardware.

Requerimientos del Hardware (Min)

Cuadro 2: Requerimientos del hardware

| | Cantidad/Tipo |
|----------------|--------------------------------|
| Memoria | 4GB RAM |
| Procesador | Intel(R) Pentium(R) IV 2.8 GHz |
| Disco duro | 20 GB |
| Tarjeta de red | 1 GB Ethernet (2) |

Fuente : Unidad Educativa Zeus

3.5.2 INSTALACION DE ZONEMINDER

ZoneMinder puede ser instalado en cualquier distribución Linux. Se recomienda instalarlo en un servidor sobre todo si el uso que le va a dar a ZoneMinder es de vigilancia o seguridad.

RPM Package Manager (o RPM, originalmente llamado Red Hat Package Manager), es una herramienta de administración de paquetes pensada básicamente para GNU/Linux. Es capaz de instalar, actualizar, desinstalar, verificar y solicitar programas. RPM es el formato de paquete de partida del Linux Standard Base.

Yum es una aplicación de CentOS que permite instalar / desinstalar otras aplicaciones para Linux que vienen empaquetadas bajo el formato RPM nativo de Red Hat. Los paquetes RPM provienen de repositorios que deben estar predefinidos en el sistema. Yum obtiene automáticamente las dependencias entre paquetes y previene sobre lo que debe existir para poder instalar correctamente los paquetes. Esto permite hacer más fácil la actualización sin tener que manipular manualmente cada RPM que se utiliza.

Para comenzar la instalación de zoneminder , debe estar previamente instalado una configuración básica de servidor. (Centos 6.5).

Empezamos accediendo como root:

```
Sudo su
```

y seguidamente actualizamos los repositorios:

```
apt-get update
```

```
apt-get upgrade
```

```
apt-get dist-upgrade
```

Una vez que el servidor ha terminado de actualizarse, recomiendo configurar nuestro servidor con una IP fija, sobre todo si se accederá desde otras máquinas. De

esta forma nos aseguraremos que nuestro servidor de seguridad no cambiará nunca de IP, aunque usemos DHCP en nuestra red. También podremos acceder incluso si el servidor de DNS falla y no podemos acceder por el nombre de host, entonces podremos seguir accediendo por la dirección IP de nuestra máquina.

Activamos CGI ya que no viene activado por defecto. 'Common Gateway Interface' es de las primeras formas de programación web dinámica:

```
a2enmod cgi
```

Guardamos y reiniciamos el servidor para que se actualice la nueva configuración.

```
service apache2 restart
```

Añadimos repositorio de la siguiente manera:

```
apt-get install software-properties-common python-software-properties
```

```
add-apt-repository ppa:iconnor/zoneminder
```

```
apt-get update
```

Instalamos ZoneMinder:

```
apt-get install zoneminder
```

A continuación creamos enlace simbólico al fichero de configuración de apache en zoneminder:

```
ln -s /etc/zm/apache.conf /etc/apache2/conf-enabled/zoneminder.conf
```

Apache es un servidor HTTP de código fuente abierto y licenciamiento libre que funciona en Linux, sistemas operativos derivados de Unix

Ahora activamos el fichero de configuración de apache en Zoneminder:

```
a2enconf zoneminder
```

Creamos un nuevo usuario:

```
adduser www-data video
```

Y reiniciamos apache:

```
service apache2 restart
```

3.5.2.1 ZONEMINDER, LA SOLUCIÓN DE CÁMARAS DE SEGURIDAD TODO-EN-UNO LINUX GPL.

ZoneMinder es usado para grabar, permitir búsquedas fáciles y exportación. Las grabaciones son de la mejor calidad posible, fácil de filtrar y encontrar, y fácil de exportar, utiliza cualquier sistema con un navegador web. También supervisa.

Una PC Pentium II debe ser capaz de realizar un seguimiento de una cámara por dispositivo en hasta 25 cuadros por segundo con esta caída a la mitad aproximadamente para cada cámara adicional en el mismo dispositivo. Cámaras adicionales en otros dispositivos no interactúan por lo que puede mantener esta velocidad de fotogramas. Incluso el seguimiento de varias cámaras todavía no se sobrecarga el CPU como el procesamiento de cuadro está diseñado para sincronizar con la captura y no estancar la misma.

Además de ser ZoneMinder rápido está diseñado para ser amigable e incluso más que eso, realmente útil. Así como el núcleo de interfaz de vídeo rápida que también viene con un agradable y completa interfaz web basado en PHP (*Hypertext Preprocessor*, es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML) de usuario permite administrar y monitorear las cámaras desde su casa, en el trabajo, en la carretera, o incluso un teléfono celular habilitado para la web. Es compatible con las capacidades web variables en función de la anchura de banda disponible. La interfaz web también le permite ver los acontecimientos que sus cámaras capturan y archivarlos o revisarlos, una y otra vez, o borrar las que ya no desee conservar. Las páginas web interactúan directamente con los demonios del núcleo, lo que garantiza una plena cooperación en todo momento. ZoneMinder incluso se puede instalar como un servicio del sistema así asegura que está justo allí si el equipo tiene que reiniciar el sistema por cualquier razón.

El núcleo de ZoneMinder es la captura y análisis de imágenes y hay un conjunto altamente configurable de los parámetros que aseguran eliminar falsos positivos al tiempo garantiza no perder la oportunidad de captura y grabación. ZoneMinder le permite definir un conjunto de "zonas" para cada cámara de la variación de sensibilidad y funcionalidad. Esto le permite eliminar eventos que no desea realizar el seguimiento o definir las áreas que serán alarma si se exceden los umbrales diferentes en conjunción con otras zonas.

3.6 PRESENTACION DE RESULTADOS

3.6.1 DISEÑO DE LA RED EN LA UEZ

En la inspección realizada a la institución, se consideró las posiciones de las cámaras según la vulnerabilidad y la necesidad de seguridad en sectores determinados como se muestra en la figura:

Para administrar las cámaras IP fue necesario diseñar una pequeña red LAN que está compuesta por:

- Un Router , servicio del proveedor
- Dos cámaras IP
- La nube
- Una laptop
- Un switch
- Cableado estructurado

Una vez que los dispositivos se encuentran conectados en la misma red y configurados cada uno con una IP estática, logran establecer una comunicación, la que es necesaria para transmitir las señales que permiten iniciar el funcionamiento del sistema, tal como lo muestra la imagen 32.

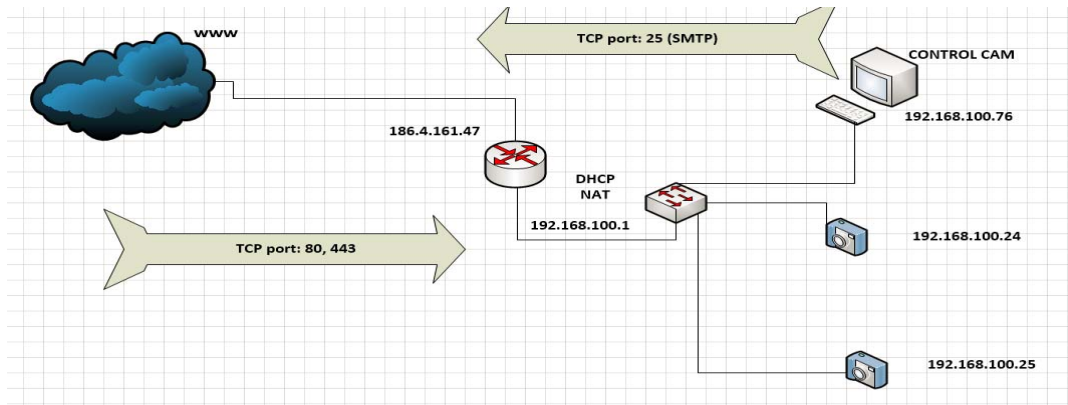


Imagen 32: Diagrama de red del sistema de seguridad

Fuente: Unidad Educativa “ZEUS “

3.6.2 SERVIDOR WEB

Para el funcionamiento del sistema de seguridad, se distribuyó al servidor como se muestra en la imagen 33:

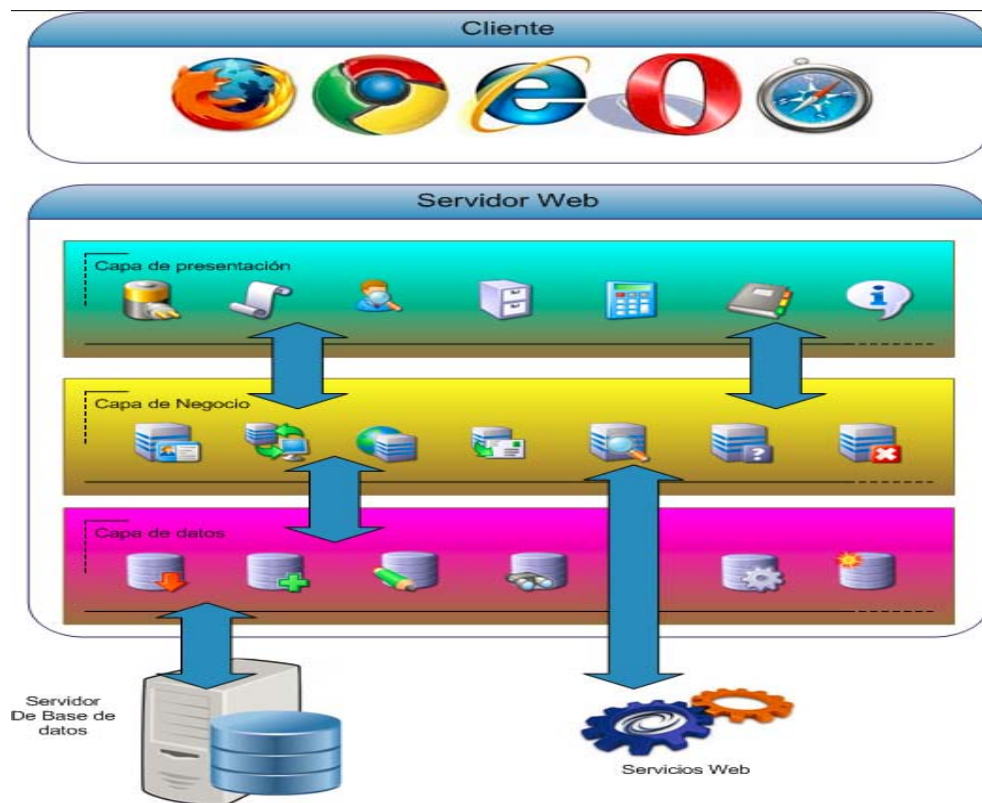


Imagen 33: Servidor Web

Fuente: <http://jmaw.blogspot.com/2013/01/arquitectura-de-aplicaciones-web.html?m=1>

3.6.2.1 CAPA DE PRESENTACIÓN

Es el espacio en donde se encuentra el servicio HTTP, es la interface que ve el usuario en forma de página web y esta es amigable de fácil entendimiento. Esta capa se comunica con la siguiente capa que la capa de aplicación y se observa en la imagen 34.

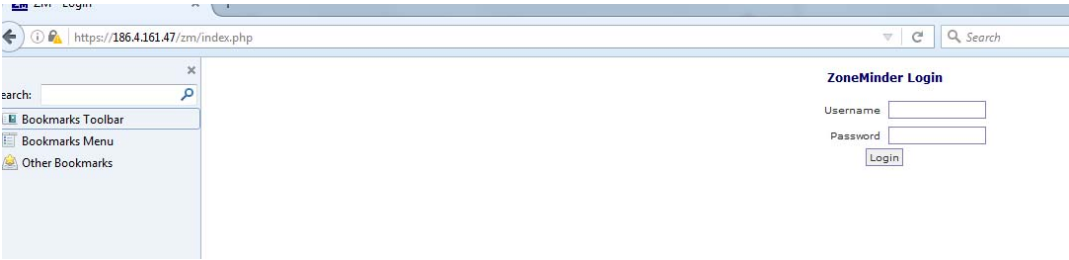


Imagen 34: Capa de Presentación
Fuente: <https://186.4.161.47/zm/index.php>

3.6.2.2 CAPA DE APLICACIÓN

En esta capa el sistema recibe las solicitudes del usuario y envía las respuestas después de seguir un proceso. Es esta capa en donde se configuran las condiciones que se debe cumplir y es la que se comunica con las capas de presentación y datos para recibir los requerimientos y mostrar respuestas deseadas. En la imagen 35 se distingue lo mencionado.

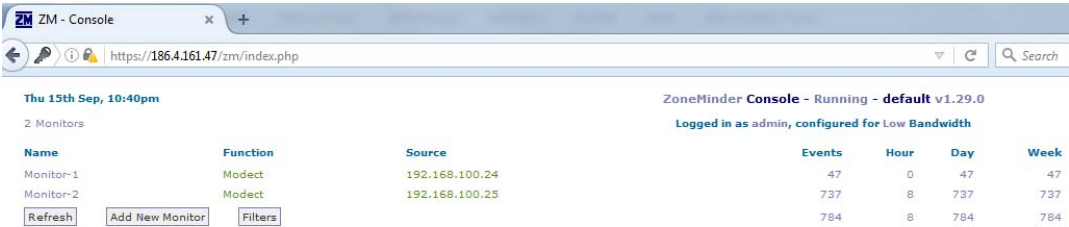


Imagen 35: Capa de Aplicación
Fuente: <https://186.4.161.47/zm/index.php>

Las condiciones para el funcionamiento requerido se lo manejó con el aplicativo ZONEMINDER

3.6.2.2.1 APLICACIÓN

En la imagen 36 y 37 se observa el proceso de instalación de la aplicación zoneminder , se descarga del fichero para posteriormente ser instalado.

```
File Edit View Search Terminal Help
[admin@controlcam Desktop]$ wget http://zmrepo.zoneminder.com/el/6/i386/zmrepo-6-7.el6.noarch.rpm
--2016-05-11 20:56:50-- http://zmrepo.zoneminder.com/el/6/i386/zmrepo-6-7.el6.noarch.rpm
Resolving zmrepo.zoneminder.com... 69.165.169.197
Connecting to zmrepo.zoneminder.com|69.165.169.197|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16068 (16K) [application/x-redhat-package-manager]
Saving to: "zmrepo-6-7.el6.noarch.rpm.1"

100%[=====>] 16,068      75.0K/s   in 0.2s

2016-05-11 20:56:51 (75.0 KB/s) - "zmrepo-6-7.el6.noarch.rpm.1" saved [16068/16068]

[admin@controlcam Desktop]$ sudo yum install --nogpgcheck zmrepo-6-7.el6.noarch.rpm
[sudo] password for admin:
Loaded plugins: fastestmirror, refresh-packagekit, security
Setting up Install Process
Examining zmrepo-6-7.el6.noarch.rpm: zmrepo-6-7.el6.noarch
Marking zmrepo-6-7.el6.noarch.rpm to be installed
Loading mirror speeds from cached hostfile
 * base: mirror.uta.edu.ec
 * extras: mirror.uta.edu.ec
 * updates: mirror.uta.edu.ec
Resolving Dependencies
--> Running transaction check
--> Package zmrepo.noarch 0:6-7.el6 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                Arch      Version      Repository      Size
=====
Installing:
  zmrepo              noarch   6-7.el6      /zmrepo-6-7.el6.noarch 25 k
=====
Transaction Summary
=====
Install      1 Package(s)

Total size: 25 k
=====
```

Imagen 36 : Instalación repositorio zoneminder

Fuente: Dorys Guerrero (Autor)

```

File Edit View Search Terminal Help
perl-Time-modules          noarch      2006.0814-5.el6      base        38 k
perl-TimeDate             noarch      1:1.16-13.el6        base        37 k
perl-URI                   noarch      1.40-2.el6           base        117 k
perl-URI-Encode           noarch      0.09-1.el6           zmrepo     18 k
perl-X10                   noarch      0.03-1               zmrepo     26 k
perl-YAML-Syck            x86_64     1.07-4.el6           base        75 k
perl-libwww-perl          noarch      5.833-2.el6          base        387 k
php                        x86_64     5.3.3-46.el6_7.1     updates    1.1 M
php-cli                   x86_64     5.3.3-46.el6_7.1     updates    2.2 M
php-common                x86_64     5.3.3-46.el6_7.1     updates    529 k
php-gd                    x86_64     5.3.3-46.el6_7.1     updates    111 k
php-mysql                 x86_64     5.3.3-46.el6_7.1     updates    86 k
php-pdo                   x86_64     5.3.3-46.el6_7.1     updates    80 k
schroedinger              x86_64     1.0.8-4.el6          zmrepo     213 k
soxr                      x86_64     0.1.2-1.el6          zmrepo     71 k
twolame-libs              x86_64     0.3.13-2.el6         zmrepo     48 k
vlc-core                  x86_64     2.1.6-2.el6          zmrepo     9.8 M
vo-amrwbenc               x86_64     0.1.1-2.el6.1        zmrepo     72 k
x264-libs                 x86_64     0.120-5.20120303.el6 zmrepo     286 k
x265-libs                 x86_64     1.6-1.el6            zmrepo     595 k
xvidcore                  x86_64     1.3.2-3.el6          zmrepo     257 k
zvbi                      x86_64     0.2.35-1.el6         zmrepo     432 k

Transaction Summary
=====
Install      95 Package(s)

Total download size: 44 M
Installed size: 143 M
Is this ok [y/N]: y
Downloading Packages:
(1/95): SDL_image-1.2.12-9.el6.x86_64.rpm | 39 kB 00:00
(2/95): a52dec-0.7.4-15.el6.3.x86_64.rpm | 50 kB 00:00
(3/95): cambozola-0.93-1.el6.noarch.rpm | 99 kB 00:00
(4/95): celt-0.11.3-1.el6.x86_64.rpm | 73 kB 00:00
(5/95): dirac-libs-1.0.2-4.el6.x86_64.rpm | 335 kB 00:00
(6/95): enca-1.18-1.el6.x86_64.rpm | 103 kB 00:00
(7/95): faad2-libs-2.7-2.el6.3.x86_64.rpm | 145 kB 00:00
(8/95): ffmpeg-2.6.4-1.el6.x86_64.rpm | 1.2 MB 00:02
(9/95): ffmpeg-libs-2.6.4-1.el6.x (11%) 57% [=====] 400 kB/s | 2.8 MB 00:05 ETA

```

Imagen 37 : Instalación repositorio zoneminderb

Fuente: Dorys Guerrero (Autor)

```

sudo yum install --nogpgcheck zmrepo-6-7.el6.noarch.rpm
sudo yum install zoneminder

```

less /usr/share/doc/zoneminder-*/README.CentOS

New installs

=====

1. instalación de base de datos MySQL, Ejecutar el siguiente comando :

```

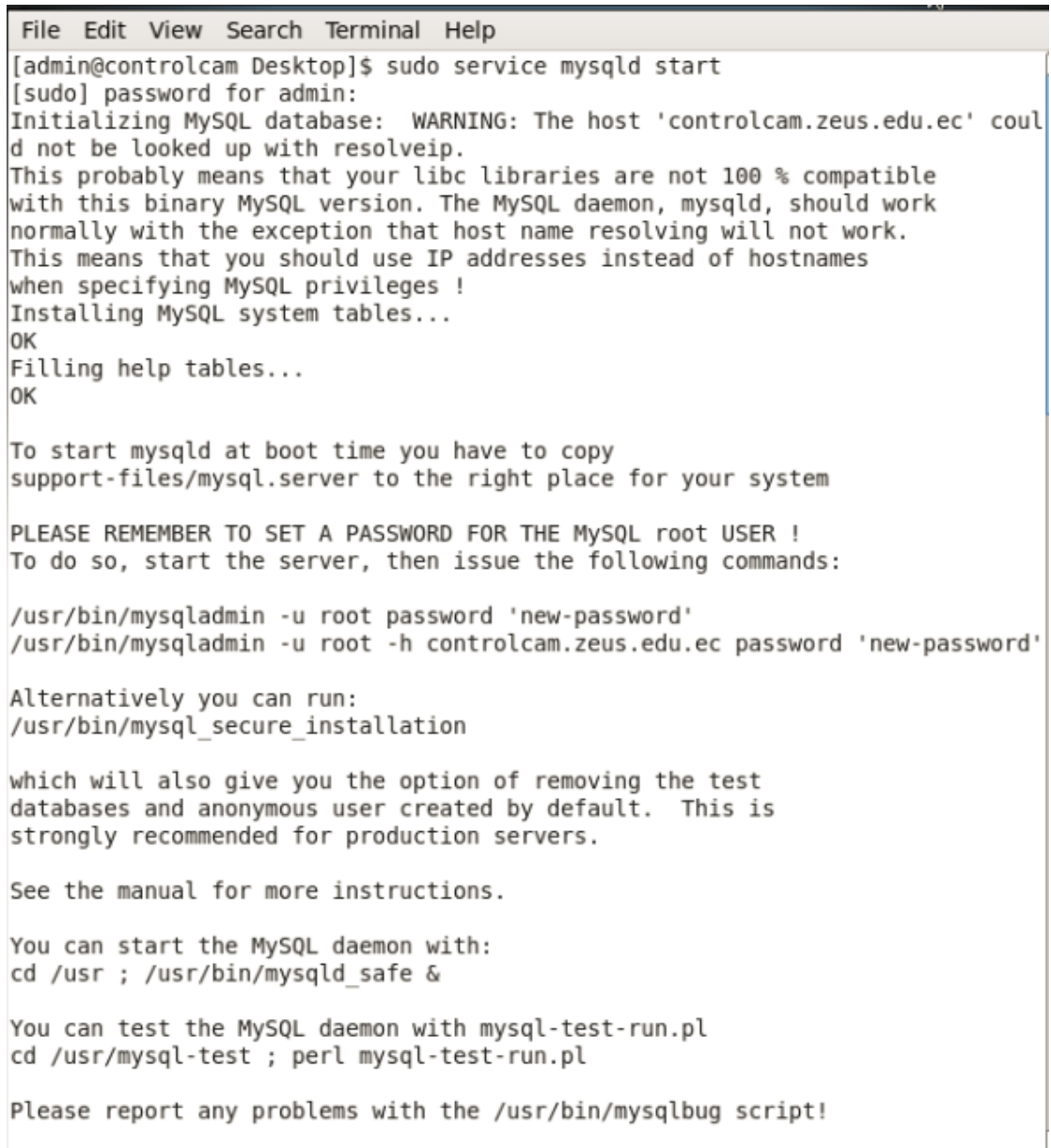
sudo yum install mysql-server

```

2. Unless you are already using MySQL server, you need to ensure that the server is confired to start during boot and properly secured by running:

```
sudo service mysqld start
/usr/bin/mysql_secure_installation
sudo chkconfig mysqld on
```

En la imagen 38 detalla el proceso de carga de la aplicación MySQL.



```
File Edit View Search Terminal Help
[admin@controlcam Desktop]$ sudo service mysqld start
[sudo] password for admin:
Initializing MySQL database: WARNING: The host 'controlcam.zeus.edu.ec' could not be looked up with resolveip.
This probably means that your libc libraries are not 100 % compatible with this binary MySQL version. The MySQL daemon, mysqld, should work normally with the exception that host name resolving will not work. This means that you should use IP addresses instead of hostnames when specifying MySQL privileges !
Installing MySQL system tables...
OK
Filling help tables...
OK

To start mysqld at boot time you have to copy
support-files/mysql.server to the right place for your system

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
To do so, start the server, then issue the following commands:

/usr/bin/mysqladmin -u root password 'new-password'
/usr/bin/mysqladmin -u root -h controlcam.zeus.edu.ec password 'new-password'

Alternatively you can run:
/usr/bin/mysql_secure_installation

which will also give you the option of removing the test
databases and anonymous user created by default. This is
strongly recommended for production servers.

See the manual for more instructions.

You can start the MySQL daemon with:
cd /usr ; /usr/bin/mysqld_safe &

You can test the MySQL daemon with mysql-test-run.pl
cd /usr/mysql-test ; perl mysql-test-run.pl

Please report any problems with the /usr/bin/mysqlbug script!
```

Imagen 38 : Instalación del servicio mysql

Fuente: Dorys Guerrero (Autor)

Las funciones de la imagen 39 que se despliegan en el monitor 1 y son las que definen esencialmente lo que el monitor hace.

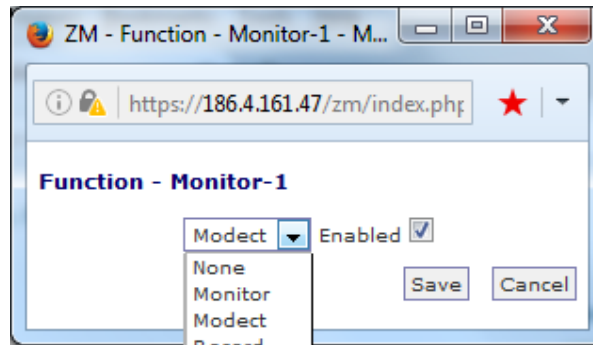


Imagen 39: Funciones

Fuente: <https://186.4.161.47/zm/index.php>

- None - El monitor está activa en este momento. No hay corrientes, se pueden ver o eventos generados. No hay nada grabado.
- Monitor - El monitor sólo está disponible para la transmisión en vivo. Ningún análisis de imágenes se realiza de modo no se generará alarmas o eventos, y no se grabará nada.
- Modect - o el movimiento DEteCTtion. Todas las imágenes capturadas serán analizados y eventos generados con vídeo grabado en el que se detecta movimiento.
- Record - El sistema grabará continuamente. Se generarán eventos de una longitud fija independientemente del movimiento, de forma análoga a una grabadora de vídeo de lapso de tiempo convencional. No detección de movimiento se lleva a cabo en este modo.
- Mocord – Es una función que se activa con cualquier movimiento que se destacó dentro de los eventos.
- Nodect - o No DEteCTtion. Este es un modo especial diseñado para ser utilizado con disparadores externos. En Nodect sin detección de movimiento se lleva a cabo.

3.6.2.2.2 APLICACIÓN EN DISPOSITIVOS MÓVILES

También se puede instalar en dispositivos móviles con aplicaciones que permiten visualizar las cámaras desde el browser del dispositivo.

Estas son algunas de las opciones para el uso en dispositivos móviles ZoneMinder: clientes móviles de terceros también detallados en la imagen 40:

- zmNinja (código fuente, necesita API para ser instalado a trabajar o disponible en App Store y Play Store - sitio web).
- zmView (limitado, libre) y zmView Pro (más características, a pagar) o disponible en App Store y Play Store, se basa en la página web ZM.
- Se puede utilizar directamente la interfaz ZoneMinder con el lanzamiento de un navegador y accede al servidor ZoneMinder tal como lo hace en el escritorio.



Imagen 40: Aplicación desde el dispositivo móvil

Fuente: <https://186.4.161.47/zm/index.php>

La imagen 41 muestra la interfaz de la aplicación desde el smathphone .

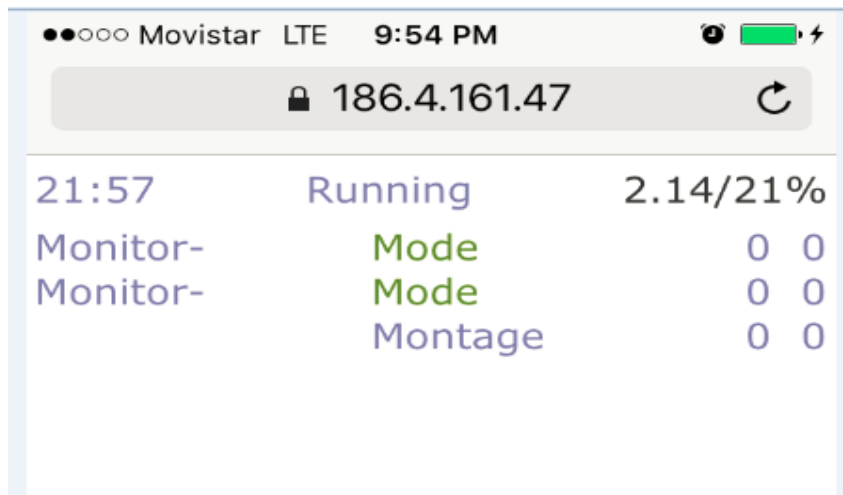


Imagen 41: Aplicación desde el dispositivo móvil

Fuente: <https://186.4.161.47/zm/index.php>

La imagen 42 muestra la visión nocturna de la cámara, también se distingue que se pueden usar hasta 8 cámaras y registra la hora real de evento .



Imagen 42: Aplicación desde el dispositivo móvil

Fuente: <https://186.4.161.47/zm/index.php>

3.6.2.3 CAPA DE DATOS

Está asignada para acceder a los datos de la capa de aplicación según la imagen 43, se encarga de almacenar datos y recuperación de información desde la capa anterior.

Mode: Live Zoom: 1.0x

| Id | Name | Time | Secs | Frames | Score |
|-----------|-------------|---------------------|-------------|---------------|--------------|
| 1090 | Event-1090 | 2016-09-15 22:13:46 | 3.54 | 62/12 | 50/66 |
| 1089 | Event-1089 | 2016-09-15 22:10:14 | 3.48 | 61/11 | 38/57 |
| 1088 | Event-1088 | 2016-09-15 22:09:42 | 2.58 | 51/1 | 54/54 |
| 1087 | Event-1087 | 2016-09-15 21:45:51 | 7.31 | 115/65 | 9/16 |
| 1086 | Event-1086 | 2016-09-15 21:44:43 | 4.26 | 74/23 | 6/11 |
| 1085 | Event-1085 | 2016-09-15 21:44:25 | 4.09 | 71/21 | 9/16 |
| 1084 | Event-1084 | 2016-09-15 21:41:57 | 3.74 | 68/18 | 5/9 |
| 1083 | Event-1083 | 2016-09-15 21:41:43 | 4.15 | 70/20 | 5/9 |
| 1082 | Event-1082 | 2016-09-15 21:39:07 | 5.07 | 83/33 | 8/13 |
| 1081 | Event-1081 | 2016-09-15 21:34:52 | 3.81 | 68/18 | 5/9 |
| 1080 | Event-1080 | 2016-09-15 21:32:39 | 6.26 | 101/51 | 10/18 |
| 1079 | Event-1079 | 2016-09-15 21:23:05 | 2.63 | 52/2 | 43/46 |

Imagen 43: Capa de Datos

Fuente: <https://186.4.161.47/zm/index.php?view=watch&mid=2>

3.6.2.4 NOTIFICACIONES POR E-MAIL

Zoneminder puede enviar las notificaciones de alertas (eventos) detectados utilizando el servicio de correo electrónico para lo cual es necesario contar con un servidor de correo que realice el envío de las mismas.

En la institución debido a la baja cantidad de usuarios y cuentas de correo necesarias no se tiene planificado realizar la adquisición e instalación/configuración de un servidor de correo ya que adicionalmente se debe cambiar el plan contratado de internet; actualmente tiene contratado un plan básico el cual no permite abrir el puerto 25 para el envío de correos.

Para probar la funcionalidad de envío de notificaciones no es necesario la recepción de correos por lo cual se configuró en el mismo servidor Zoneminder el servicio "postfix como relay" utilizando el servidor de "gmail" como servidor de correo (SMTP).

La configuración realizada es la siguiente:

- Instalando Postfix : Ejecutamos el siguiente comando como root :

```
yum install postfix mailx cyrus-sasl-plain
```

- Ejecutando Postfix

Básicamente, es necesario crear un archivo de contraseñas para que Postfix pueda autenticarse en los servidores de Gmail. Para ello, cree un archivo denominado `sasl_passwd` en `/etc/postfix`.

```
echo "smtp.gmail.com smtp_user:smtp_passwd" > /etc/postfix/sasl_passwd
```

- A continuación, ejecutamos la instrucción `hash` para que la contraseña no se almacena en texto visible. Este comando creará un archivo llamado `sasl_passwd.db` en el directorio `/etc/postfix/`.

postmap hash:/etc/postfix/sasl_passwd

- Después se añade en la raíz de /etc/postfix/main.cf. Esto es suponiendo que sus certificados raíz instalados desde openssl se encuentran en /etc/pki/tls/certs/ca-bundle.crt.

```
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous
# Secure channel TLS with exact nexthop name match.
smtp_tls_security_level = secure
smtp_tls_mandatory_protocols = TLSv1
smtp_tls_mandatory_ciphers = high
smtp_tls_secure_cert_match = nexthop
smtp_tls_CAfile = /etc/pki/tls/certs/ca-bundle.crt
relayhost = smtp.gmail.com:587
```

- Restauramos el Postfix

service postfix restart

Realizamos una prueba para comprobar su funcionamiento ejecutando la siguiente instrucción.

mail email@domain

Escribir el asunto al igual que en el cuerpo del mail y pulsar enter.

Si todo está correcto, se recibirá un correo electrónico en la dirección de correo electrónico que ingresó. Si lo hace, puede eliminar el archivo que tiene la contraseña.

rm /etc/postfix/sasl_passwd

La configuración en la consola de Zoneminder se realizó de acuerdo a su propia documentación:

Options - Email — ZoneMinder documentation



Options - Email — ZoneMinder documentation

El imagen 44 se detalla la configuración en la aplicación Zoneminder para el envío de alerta por mail.

ZM - Options - Mozilla Firefox

https://192.168.100.76/zm/index.php?view=options&tab=mail

Options

Display System Config Servers Paths Web Images Logging Network Email Upload X10 High BW Medium BW Low BW Phone BW eyeZm Users

| Name | Description | Value |
|------------------|-------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| OPT_EMAIL | Should ZoneMinder email you details of events that match corresponding filters (?) | <input checked="" type="checkbox"/> |
| EMAIL_ADDRESS | The email address to send matching event details to (?) | cb_z Zeus@hotmail.com |
| EMAIL_SUBJECT | The subject of the email used to send matching event details (?) | ZoneMinder Alarm - %MN%- %E% (%ESM%) |
| EMAIL_BODY | The body of the email used to send matching event details (?) | <p>Hello,</p> <p>An alarm has been detected on your installation of the ZoneMinder.</p> <p>The details are as follows :-</p> |
| OPT_MESSAGE | Should ZoneMinder message you with details of events that match corresponding filters (?) | <input checked="" type="checkbox"/> |
| MESSAGE_ADDRESS | The email address to send matching event details to (?) | |
| MESSAGE_SUBJECT | The subject of the message used to send matching event details (?) | ZoneMinder Alarm - %MN%- %E% |
| MESSAGE_BODY | The body of the message used to send matching event details (?) | ZM alarm detected - %EL% secs, %EF%%EFA% frames, %EST%/m/%ESM%/a/%ESA% score. |
| NEW_MAIL_MODULES | Use a newer perl method to send emails (?) | <input type="checkbox"/> |
| EMAIL_HOST | The host address of your SMTP mail server (?) | smtp.gmail.com:587 |
| FROM_EMAIL | The email address you wish your event notifications to originate from (?) | zeus.controlcam@gmail.com |
| URL | The URL of your ZoneMinder installation (?) | https://192.168.100.76/zm |

Save Cancel

3.6.2.5 FILTRANDO EVENTOS

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

- Enviar un correo electrónico cada vez que se produzca un nuevo evento para un monitor específico.
- Eliminar eventos con más de 10 días o más de antigüedad entre otros.

La ventana de filtro se puede acceder desde varias vistas, una de las cuales es simplemente se presiona en el botón de filtro en la vista web principal:

Sun 23rd Aug, 2:23pm ZoneMinder Console - Running
Group: All: 5 Monitors Logged in as admin, configured

| NAME | FUNCTION | SOURCE | EVENTS | HOURS |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|---------------|--------|-------|
| FirstLevel | Modect, disabled | 192.168.1.129 | 6546 | 0 |
| Garage | Modect | 192.168.1.33 | 2004 | 0 |
| Basement | Modect | 192.168.1.125 | 1295 | 0 |
| BabyRoom | Modect, disabled | 192.168.1.24 | 0 | 0 |
| unfinished | Modect | 192.168.1.17 | 47 | 0 |
| <input type="button" value="REFRESH"/> <input type="button" value="ADD NEW MONITOR"/> <input style="border: 2px solid red;" type="button" value="FILTERS"/> | | | 9892 | 0 |

Imagen 45: Filtros y condiciones

Fuente: <http://zoneminder.readthedocs.io/en/stable/userguide/filterevents.html>

Se utiliza la ventana de filtro para crear filtros específicos o para modificar los existentes, incluso se puede guardar los filtros favoritos para volver a usarlos en un futuro. El filtrado es bastante simple; Primero se elige cuántas condiciones necesitamos que contenga el filtro. Cambiar este valor hará que la ventana se vuelva a desplegar con una fila correspondiente para cada condición. A continuación, seleccione lo que desea filtrar y cómo se relacionan las condiciones eligiendo si son "y" o "o" las relaciones. Esto es lo que parece la ventana de filtro:

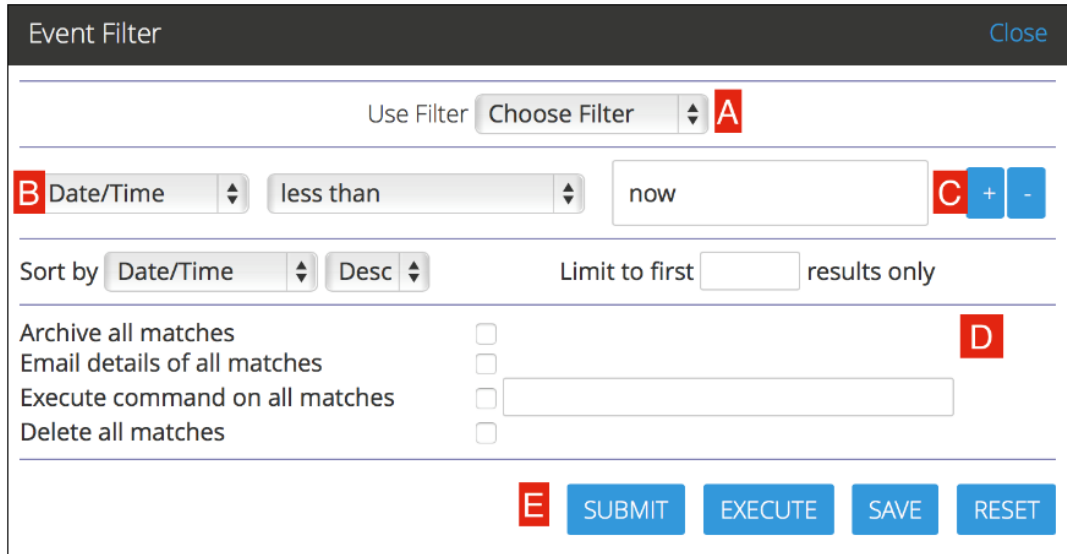


Imagen 46 : Filtrar evento

Fuente: <http://zoneminder.readthedocs.io/en/stable/userguide/filterevents.html>

A: Esta es una lista desplegable donde puede seleccionar filtros predefinidos. Se observa que ZoneMinder viene con un filtro PurgeWhenFull que está configurado para eliminar eventos si alcanza el 95% de espacio en disco como se observa en las imágenes 47 y 48.

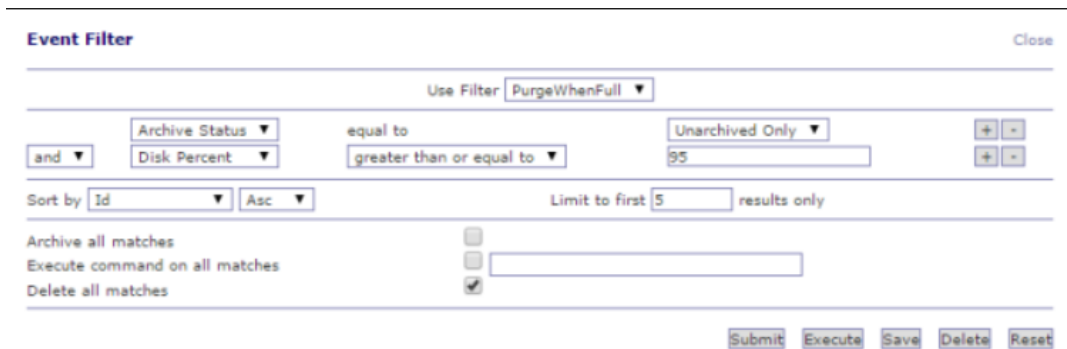


Imagen 47 : Configuración Filtro PurgeWhenFull

Fuente: <https://192.168.100.76/zm>

Save Filter

Save as or enter new name

Run filter in background

Imagen 48 : Guardar Filtro PurgeWhenFull

Fuente: <https://192.168.100.76/zm>

B y C: Aquí es donde se especifican las condiciones que deben coincidir antes de que se ejecute el filtro. Utiliza los botones "+" y "-" para agregar / eliminar condiciones

D: Especifica qué debe suceder cuando las condiciones coinciden:

- Archive all matches, puede ver eventos archivados más adelante y también asegurarse de que los eventos archivados no se eliminen, por ejemplo.
- Email details of all matches: Envía un correo electrónico a la dirección configurada con detalles sobre el evento.
- Execute command on all matches: Le permite ejecutar cualquier comando arbitrario en los eventos coincidentes.
- Delete all marches: elimina todos los eventos coincidentes.

3.7 PRESUPUESTO PROYECTO

En el cuadro 3 se detalla el valor real de la implementación del proyecto, cabe mencionar que en el mismo no se encuentra registrado el valor de lo que es el costo de la aplicación y administración ya que ésta se acopla a la necesidad del sitio a proteger.

Cuadro 3: Presupuesto Proyecto

| PRESUPUESTO | | | |
|--------------------|---------------------------------------------------|-----------------------|--------------------|
| CANTIDAD | DESCRIPCION | V. UNITARIO \$ | V. TOTAL \$ |
| 1 u | Materiales para cableado e instalación de cámaras | 290 | 290 |
| 2 u | cámaras IP | 140 | 280 |
| 1 u | laptop Thinkpad Lenovo X200 | 500 | 500 |
| 1 u | Otros | 100 | 100 |
| TOTAL | | | \$1170 |

Autor: Dorys Guerrero

En comparación con los costos de este servicio implementado por alguna empresa como lo describe el cuadro 4, este proyecto tiene un valor muy bajo, resulta así un buen producto competitivo que tendrá apertura en las actividades comerciales, así se cumple el resultado deseado en cuanto a competencia en el mercado ya que se verifica que este sistema es escalable y su funcionamiento es 100 % efectivo como las implementaciones de otras empresas.

Cuadro 4 : Presupuesto en el mercado

| PRESUPUESTO LIGHTINTHEBOX | | | |
|----------------------------------|---------------------------------------------------|-----------------------|--------------------|
| CANTIDAD | DESCRIPCION | V. UNITARIO \$ | V. TOTAL \$ |
| 1 u | Materiales para cableado e instalación de cámaras | 500 | 500 |
| 2 u | cámaras IP | 155 | 310 |
| 1 u | Sistema de grabación | 700 | 700 |
| 1 u | desarrollo de la aplicación | 850 | 850 |
| TOTAL | | | \$2360 |

Fuente: LIGHTINTHEBOX asesoría en seguridad tecnológica.

CONCLUSIONES

- El desarrollo de este proyecto permite comparar el software licenciado con open source y analizar la ventaja del uso de éste último ya que se obtienen alta disponibilidad, escalabilidad que utiliza principios básicos de un servidor de aplicación.
- El uso del software libre y open source reduce notablemente los costos de inversión en licencias y a su vez mejora la infraestructura y el rendimiento de los negocios, los mismos que obtienen como resultado más productividad pues no están limitados a utilizar un determinado software.
- Open Source y el software libre, tecnológicamente deben considerarse como una de las primeras opciones a tomarse en cualquier tipo de negocio pues existen muchas alternativas para desarrollar un requerimiento determinado, de esta manera no se necesitan de empresas privadas y menos extranjeras para mejorar una infraestructura que se inició con Open Source.
- El sistema de video vigilancia con cámaras IP implementado exclusivamente para la Unidad Educativa “ZEUS” se convierte en un necesario instrumento para la administración efectiva de la seguridad.

RECOMENDACIONES

- Al usar Open Source y software libre, la implementación adquiere flexibilidad ya que puede ser modificada con el objetivo de mejorarla y personalizarla a través de su código fuente sin tener que realizar inversiones económicas significativas.
- Antes de iniciar una implementación con Open Source o software libre se debe definir con claridad los estándares para la plataforma a implementarse y así en un futuro evitar problemas de funcionalidad del sistema.
- El uso de las claves de acceso debe ser confidencial pues se trata de un sistema de seguridad lo que hace que dicha información se vuelva sensible.
- El sistema debe ser operado por una persona con conocimientos básicos de computación.
- El sistema está diseñado para funcionar tanto en el día como en la noche por lo cual se recomienda tener el suministro de energía suficiente (UPS, uninterruptible power supply), para mantener su funcionamiento de manera ininterrumpida. Cabe recalcar que la institución (ZEUS) no brindó la apertura necesaria para la conexión eléctrica de backup.

BIBLIOGRAFÍA

- Jboss In Action ,Jamae Javid, Jhonson Peter , Orelly & associates Inc
- CLUSTER_COMPUTING_THEORY , Morrison, Richard S , Public Licence, abril 2003.
- IDG Communications , Computer word. Ecuador,. – Vol.2 N° 48,49
- <http://dvron.eu/es/2009/05/11/apllication-load-balancing-and-in-memory-session-saring-with-tomcat-and-apache/> ,fecha de acceso 10/07/2015
- <http://docs.jboss.org/jboss4guide/r4/html/jbosscache.chapt.html> , fecha de acceso 10/07/2015
- IEEE: 802.15, <http://www.ieee802.org/15/pub/TG4.html> , fecha de acceso: 21/06/2015
- Mobotix, Como funcionan las Cámaras de Red, http://www.mobotix.com/esl_ES/region/index/esl_ES/?URL=Productos/Tecnolog%C3%Ada/C%C3%B3mo-Funcionan-las-C%C3%A1maras-de-Red, fecha de cceso: 21/06/2015
- Freescale: Manual de ZED, http://www.freescale.com/files/rf_if/doc/user_guide/ZEDQSG.pdf?WT_TYPE=Users%20Guides&WT_VENDOR=FREESCALE&WT_FILE_FORMAT=pdf&WT_ASSET=Documentation, fecha de acceso: 8/05/15
- <http://www.jtech.ua.es/j2ee/2003-2004/abierto-j2ee-2003-2004/sa/sesion1-apuntes.htm>
- cableadoestructurado-101229105452-phpapp02.ppt
- <http://www.saulo.net/pub/tcpip/a.htm>
- <http://revistas.udistrital.edu.co/ojs/index.php/REDES/article/view/6366/9466>
- <http://www.dointech.com.co/video-vigilancia-ip.html>
- <http://netkromsolutions.com/seguridad-publica-y-videovigilancia>
- <http://zmrepo.zoneminder.com/el/6/i386/zmrepo-6-7.el6.noarch.rpm>

ZMVIEW

IP/Network Camera



MANUAL DE USUARIO

7.0.3

ÍNDICE MANUAL DE USUARIO

| | |
|------------------------------------------------------------|---|
| ÍNDICE MANUAL DE USUARIO..... | 2 |
| Antes de usar los dispositivos | 1 |
| 1) Por su seguridad..... | 1 |
| 2) Características de las cámaras:..... | 1 |
| Video Compression: H.264 Main Profile/Baseline. | 2 |
| 3) Formas de Monitoreo | 3 |
| 3. La aplicación empieza a conectarse con el servidor..... | 4 |
| 4. Solicitará nombre de usuario y password: | 4 |
| 4) TABLA DE FALLOS | 6 |
| TABLA DE FALLOS | 6 |
| 5.1) Contacto para soporte: | 7 |

Antes de usar los dispositivos .

Con la tecnología actual, ahora se pueden mejorar los servicios en especial en seguridad, con las que se puede vigilar 7*24 y tener conocimiento de lo que ocurre en tiempo real incluso grabar desde un PC, Tablet o Smartphone. La configuración de la cámara es amigable y fácil de usar, solo se requiere conectar la cámara al router que tiene el servicio de internet de la unidad Educativa “Zeus” y con la ayuda de una aplicación y un software adecuado, logra identificarla y crea una pequeña red.

Antes de usar estos dispositivos por favor lea las instrucciones con detenimiento.

- Estos dispositivos no deben ser usados en lugares húmedos o en altas temperaturas pues no está incluidas las protecciones a los mencionados.
- Usar un paño húmedo para la limpieza exterior de las cámaras, no usar productos que contengan químicos.
- No intentar limpiar el lente de la cámara bajo ninguna circunstancia.
- Por ningún motivo comparta el usuario y la clave de acceso a las mismas, independientemente de la forma en la que se vaya a monitorear.
- Mantener activo el servicio de Internet para su buen funcionamiento.

1) Por su seguridad.

- Por ningún motivo trate de desmontar la cámara ni desconectarla de la fuente de poder.
- La toma de corriente a las que están conectadas debe mantenerse secas y en un lugar poco accesible para evitar desconexiones.
- No cubrir las cámaras con ningún paño ya que las luces infrarrojas producen calor.
- Mantenerlas conectadas y no tratar de moverlas de su lugar original.
- Asegúrese que las cámaras se encuentren siempre fijas en su lugar de instalación.

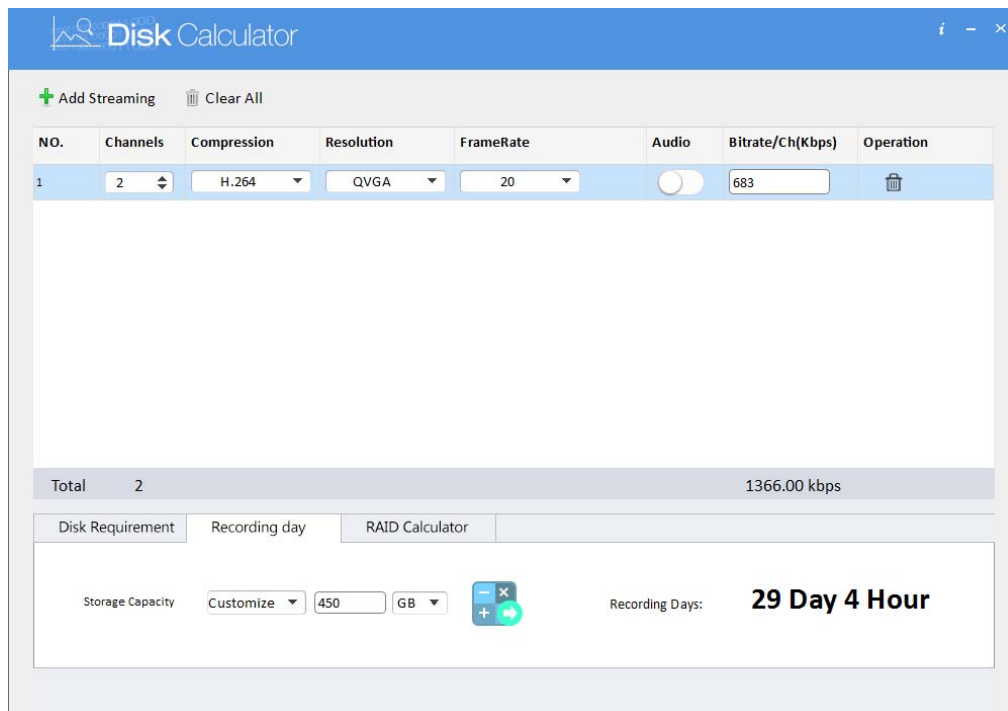
2) Características de las cámaras:

- Visualiza los eventos 7*24 desde el Smartphone, Tablet y PC.
- Graba en el momento que detentan movimientos y almacena las eventualidades en el disco duro de la PC.
- Envía alertas instantáneas

- Visión infrarroja permitiendo monitorear cuando hay ausencia de luz.
- El sistema graba a 20 FPS y requiere 0.6 Mbps para un modelo QVGA a 1028*720 px. Si el ancho de banda es limitado como es el caso de la institución (Unidad Educativa ZEUS”), con la configuración por defecto de FPS en modo automático la cámara IP se adaptará automáticamente al mismo para dar la mejor calidad disponible.

Video Compression: H.264 Main Profile/Baseline.

- Según las características de las cámaras y considerando que estuvieran grabando full time 7/24, se observa que con la capacidad del disco al 95% (en el que empezaría a borrar eventos), grabaría durante 29 días y 4 horas pero en realidad esto depende de las eventualidades registradas en el día. Se concluye que el disco guardará las eventualidades 2 meses aproximadamente si reducimos el tiempo de grabación a la mitad.



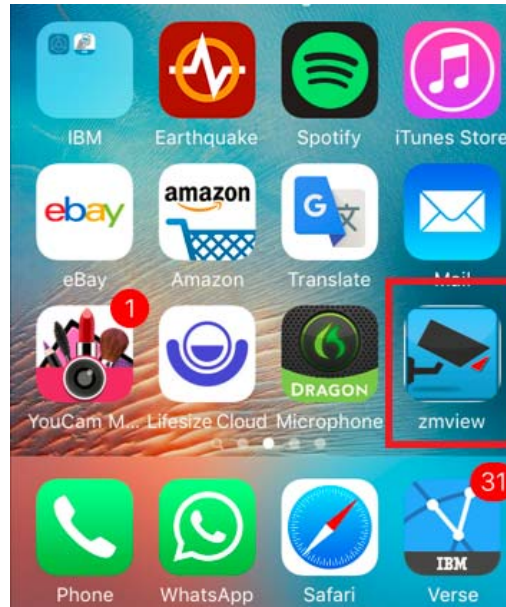
- Los videos capturados en el momento del evento quedan guardados en un ordenador local con espacio disponible en disco duro de aproximadamente 500GB, su saturación dependerá del número de eventos y el tamaño de éstos. Sin embargo en la aplicación zone minder se configuró filters que se ejecutan para borrar automáticamente videos antiguos.

3) Formas de Monitoreo

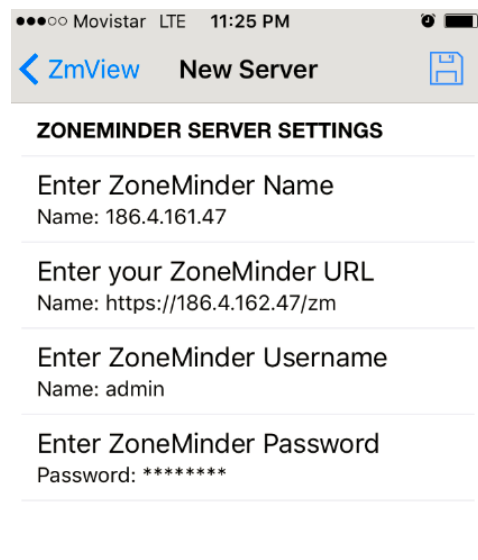
Estas cámaras en particular tienen dos formas de monitoreo:

a) Por medio de la aplicación ZMVIEW en un Smartphone o Tablet para Usuarios de Android e los

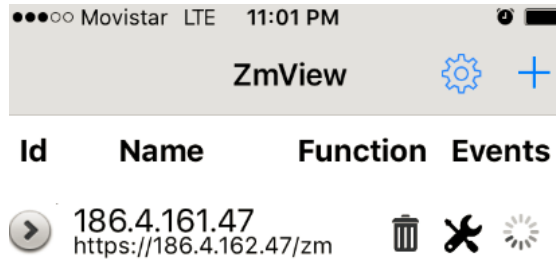
1. Se requiere instalar la aplicación **zmview**.



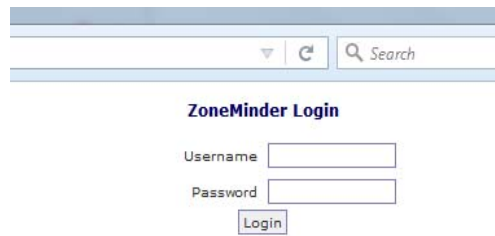
2. Luego de la instalación de la aplicación solicita los siguientes parámetros (información que será proporcionado al usuario):



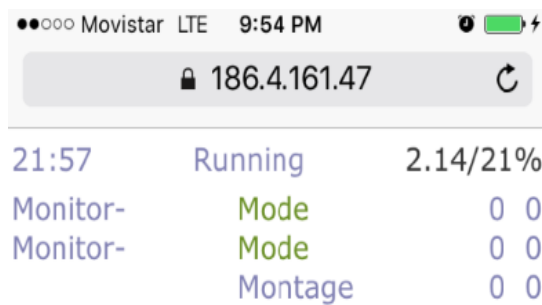
3. La aplicación empieza a conectarse con el servidor

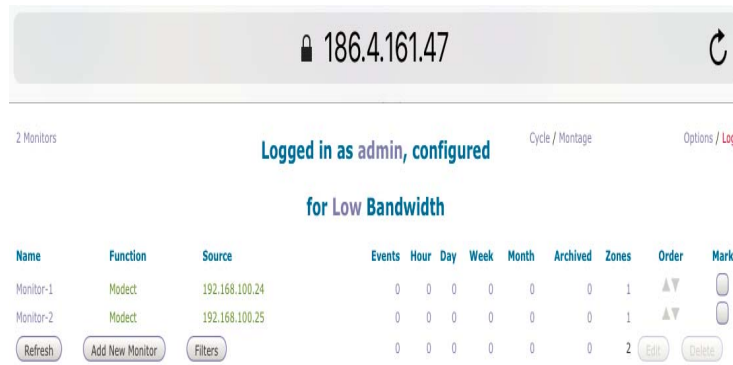


4. Solicitará nombre de usuario y password:



5. Se observa una interfaz en la que se puede escoger cualquiera de las dos cámaras.





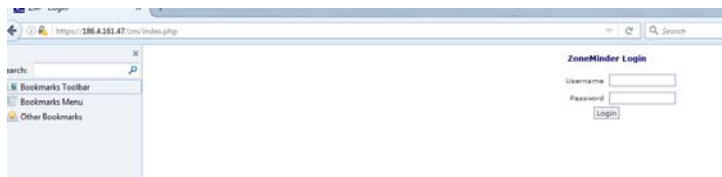
- Despliega la imagen de lo que visualiza la cámara y también la opción de escoger hasta 8 cámaras.



- Por medio de una PC o smartfhone un browser.

- Desde cualquier browser, ingresar en la siguiente URL:
<https://186.4.161.47/mz>

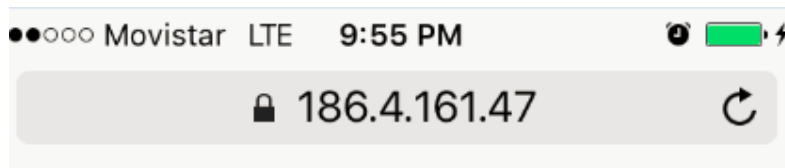
Desplegará una interface en la que solicita usuario y password:



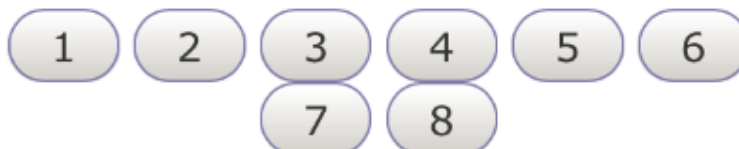
2. Al ingresar con los datos correctos , se visualiza las camaras disponibles para la selección :



3. Seleccionada la cámara y se observa lo siguiente :



Monitor-2: Idle - 20.57 fps



Prev Console Next

4) TABLA DE FALLOS

| TABLA DE FALLOS | |
|------------------------|------------------------------------------------------|
| POSIBLES FALLAS | RECOMENDACION |
| La cámara no enciende. | Compruebe que esté conectada a la fuente de energía. |

| | |
|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| No se visualiza bien desde el lente de la cámara. | Asegúrese que la cámara se encuentre libre de polvo y humedad. |
| La aplicación en el smartpone no se conecta con el servidor de las cámaras. | Asegúrese que el Smartphone tenga activo plan de datos ó esté conectados a una red wifi. |
| El browser no despliega ninguna información. | Verifique la ip ingresada para el acceso sea la correcta. |
| No reconoce las credenciales de acceso. | Comuníquese con el proveedor para corroborar y actualizar la información del sistema. |
| No hay conexión del servidor con el smartphone ni con el browser. | Compruebe que el servidor web esté conectado a la fuente de energía. |
| El servidor web y las cámaras se encuentren prendidos pero no se visualiza por ninguno de los medios. | Contáctese con su proveedor de Internet y luego con el soporte de la aplicación. |
| Las cámaras están encendidas pero no responden. | Contáctese con el soporte de la aplicación. |
| Las cámaras están conectadas a la fuente de luz pero no encienden. | Contáctese con el soporte de la aplicación. |
| el servidor está prendido pero no logran conectarse las cámaras. | Contactese con el soporte de la aplicación. |
| Cualquier circunstancia o problema que no se encuentre detallado en este manual. | Contactese con el soporte de la aplicación. |

5.1) Contacto para soporte:

Dorys Guerrero
domary27@hotmail.com
0999716855 / 3954572

ANEXO 2

Características técnicas Cámara IP:

- ✓ Model No: GTN-HS1022-AFN
- ✓ Device Type: 1/4inch 720P OV9712 CMOS sensor, IR-CUT
- ✓ Min.Scene Illumination:0.01lux (IR ON)
- ✓ IR-led:18PCS IR LED, Night Vision 15m lens: 3.6MM/F1.2 Fixed
- ✓ Video Compression: H.264 Main Profile/Baseline
- ✓ Picture Resolution: 1280X720 @ 20fps
- ✓ Steam flow: Support dual stream
- ✓ Alarm way:Motion Detection: Configure motion detection area, detecting sensitivity is adjustable, Cover alarm: The alarm sensitivity is adjustable.
- ✓ Alarm processing: The control center to monitor, Send E-mail, Log record, etc.
- ✓ Network Protocol: HTTP, TCP/IP, UDP, SMTP, DDNS, DNS, SNTP, DHCP, FTP, RTP, RTSP, UPNP, ONVIF ,28181
- ✓ Ethernet: Ethernet (10/100 Base-T),RJ-45 connector
- ✓ WEB Browser:Microsoft Internet Explorer 6.0 and above, google, firefox etc.
- ✓ Mobile Phone:Support iPhone, Android, Bit rate: 32K - 512K adjustable, frame rate: 6-12 fps.
- ✓ Software Management:CMS and the devices Compatible with ONVIF
- ✓ Remote Access: DDNS, Software, P2P
- ✓ Accessories: Power adapter, Stand, Operation manual, CD, Screw bag Power Consumption: DC 12V ,Module power consumption is less than 2 W
- ✓ Temperature: -20°~60°C
- ✓ Weight:0.48KG
- ✓ Dimensión : 20*17*13cm

ANEXO 3 INSTALACIÓN CENTOS 6.5

INDICE

| | |
|------------------------------------------------------------------------------------|----|
| Instalando Centos 6.5 | 1 |
| Seleccionamos el dispositivo en donde se encuentra el boot a ejecutar. | 1 |
| Inicia el entorno gráfico. Damos click al botón Next | 2 |
| Elegimos el Idioma a usar durante la instalación y presionamos al botón Next | 3 |
| Elegimos la Distribución del teclado. Click al botón Siguiente | 3 |
| -Muestra el disco detectado. Click al botón Si descarte todos los datos. | 4 |
| -Escribimos un nombre para Centos (hostname). Click al botón Configure la red. ... | 5 |
| -La tarjeta (ethernet) debe estar conectada. | 5 |
| -IMPORTANTE, | 6 |
| -Ya configurada la conexión, presionamos click al botón Cerrar y Siguiente | 6 |
| -Elegimos la Zona donde está ubicado el equipo. Click al botón siguiente. | 7 |
| -Escribimos una Contraseña para el usuario root. | 7 |
| -Siguiente paso, elegir como instalar Centos..... | 9 |
| -Comienza la instalación. | 9 |
| - Linux Centos está instalado. Click al botón Reiniciar | 10 |
| -Al hacer boot por primera vez en el Centos instalado. | 10 |
| -Se descargan los paquetes y así queda actualizado el sistema centos 6.5..... | 11 |

ANEXO 3

CAPTURA DE PANTALLAS INSTALACION SOFTWARE BASE CENTOS 6.5

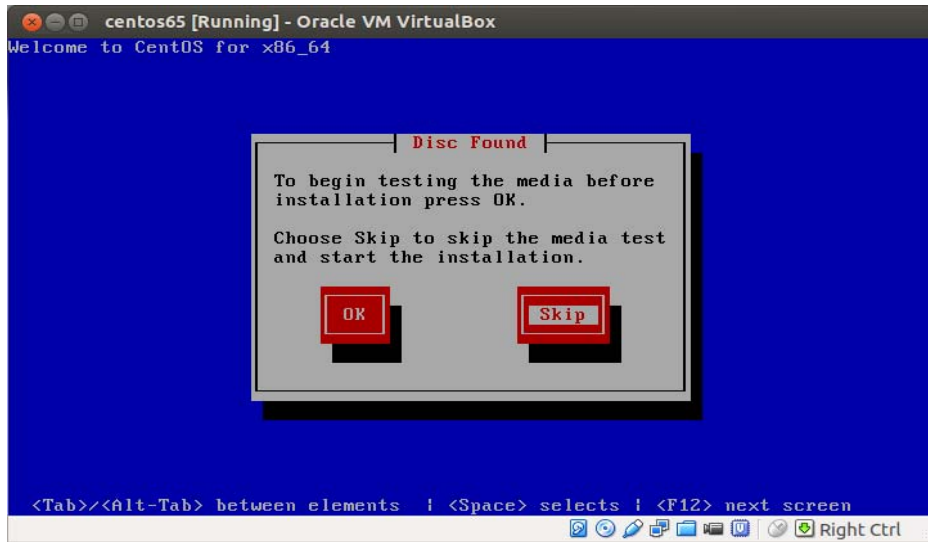
Instalando Centos 6.5

Al hacer boot se muestra 2 opciones para instalar, la primera el sistema detectara la tarjeta de vídeo y entrara en modo gráfico por lo tanto es recomendable elegir la segunda opción, carga un driver básico de vídeo que todos los equipos reconocen sin problemas. Presionamos Enter.



Seleccionamos el dispositivo en donde se encuentra el boot a ejecutar.

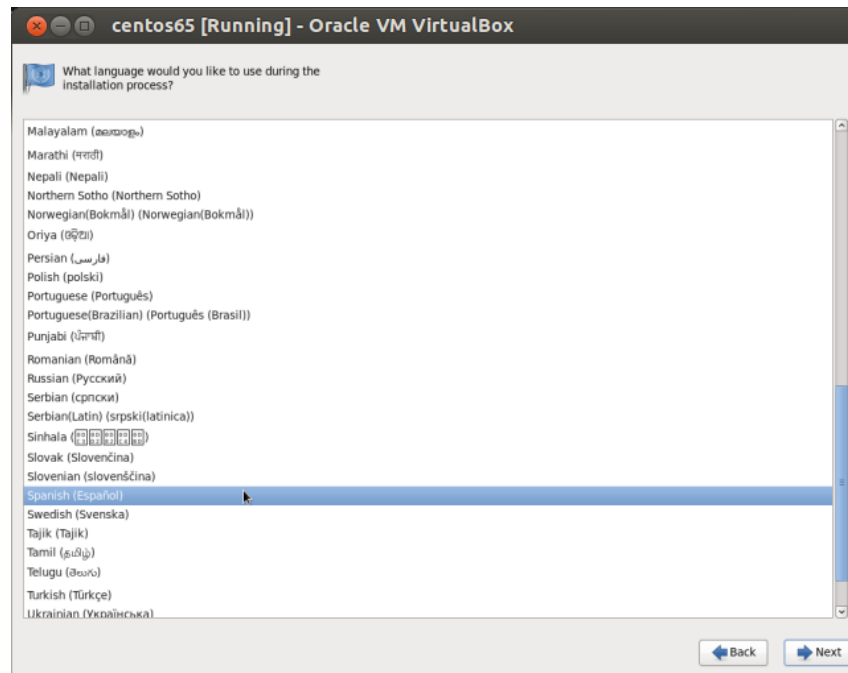
Revisamos si el DVD o instalacion de USB . Skip



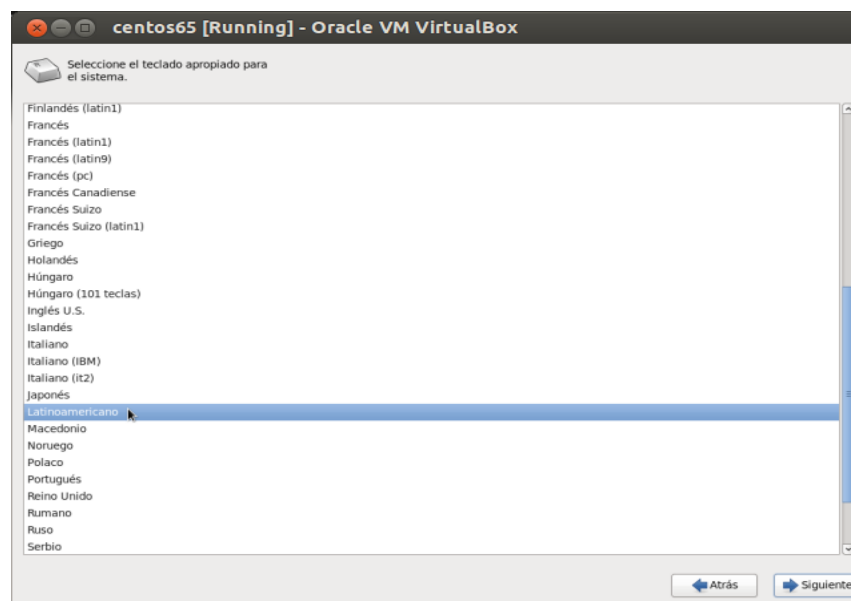
Inicia el entorno gráfico. Damos click al botón Next



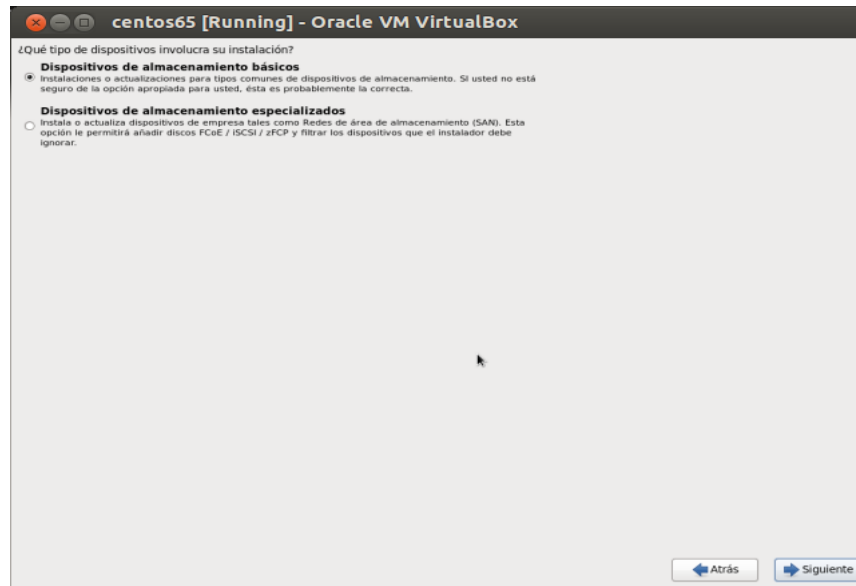
Elegimos el Idioma a usar durante la instalación y presionamos al botón Next



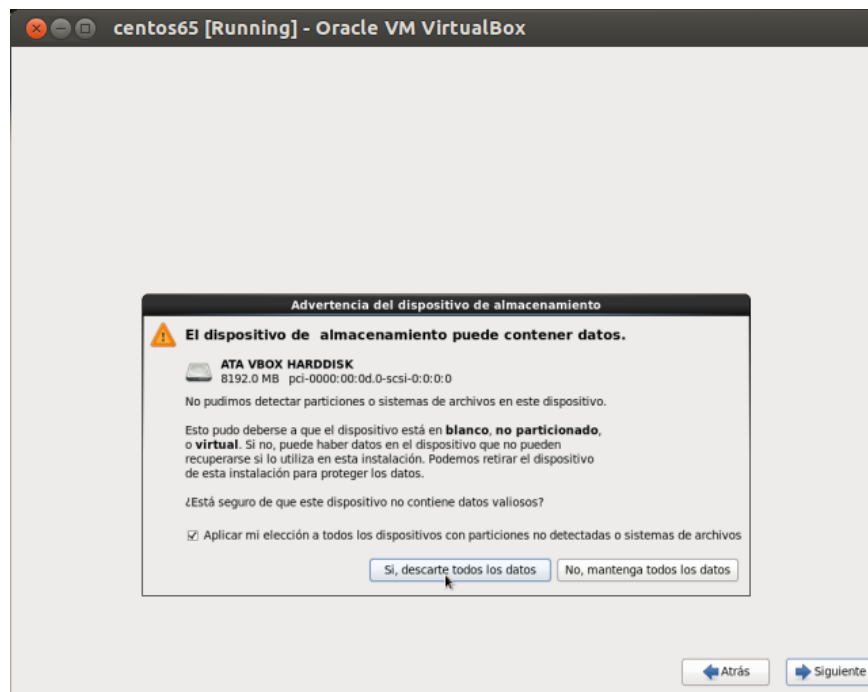
Elegimos la Distribución del teclado. Click al botón Siguiente



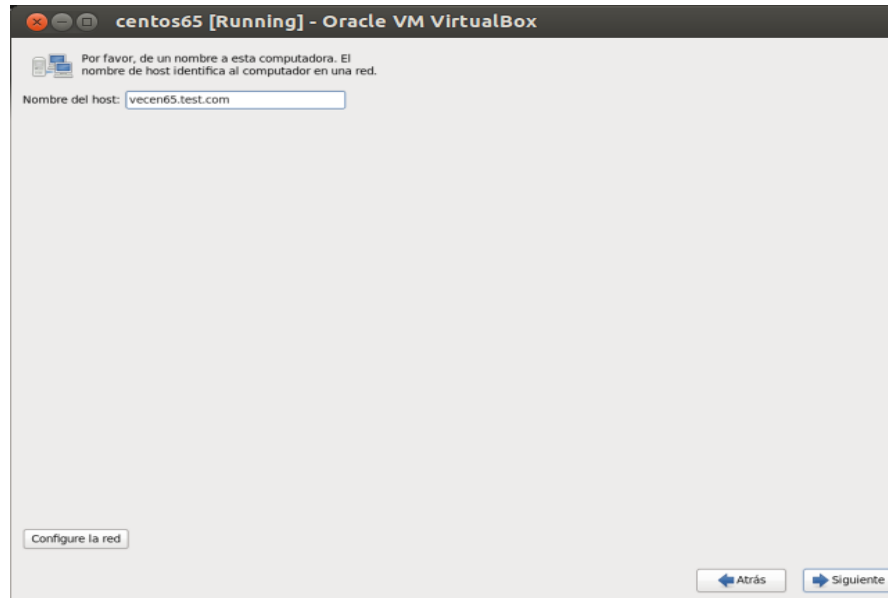
-En caso de contar con dispositivos de almacenamiento especializados como iSCSI, SAN, etc, marcamos la segunda opción, caso contrario, la primera es la que elegiremos. Presionamos el botón Siguiente



-Muestra el disco detectado. Click al botón Si descarte todos los datos.

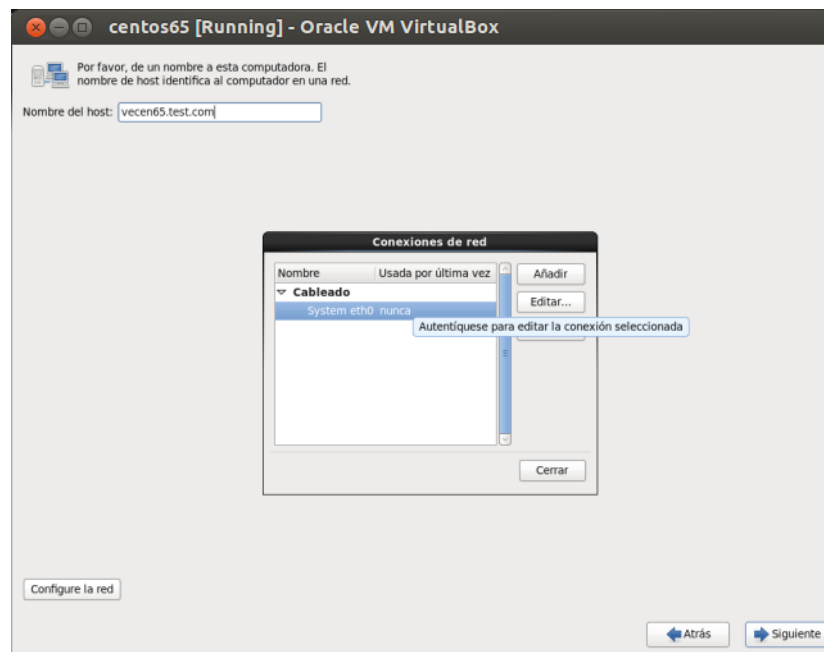


-Escribimos un nombre para Centos (hostname). Click al botón Configure la red.



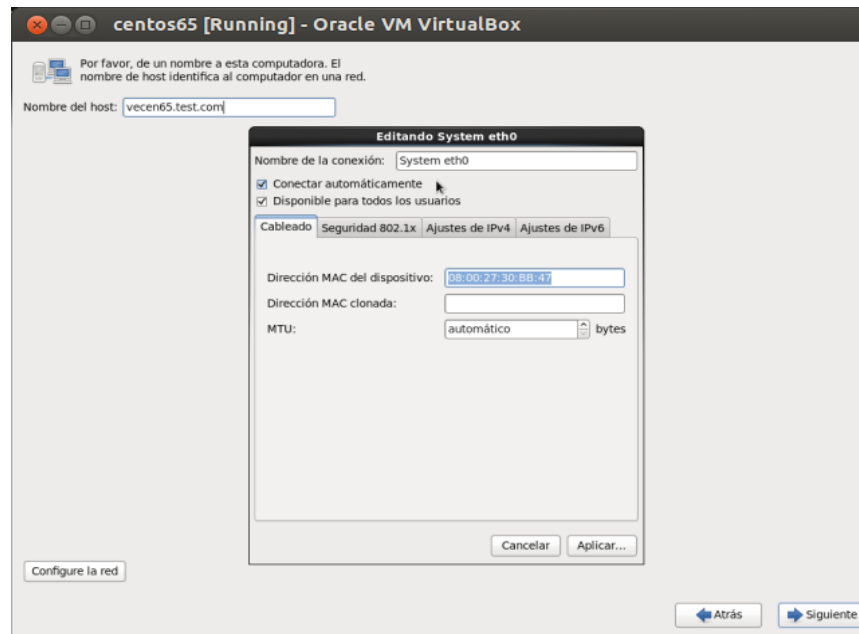
-La tarjeta (ethernet) debe estar conectada.

Para garantizar una buena configuración, marcamos eth0 (o la que usaremos en caso de haber mas). Click al botón Editar

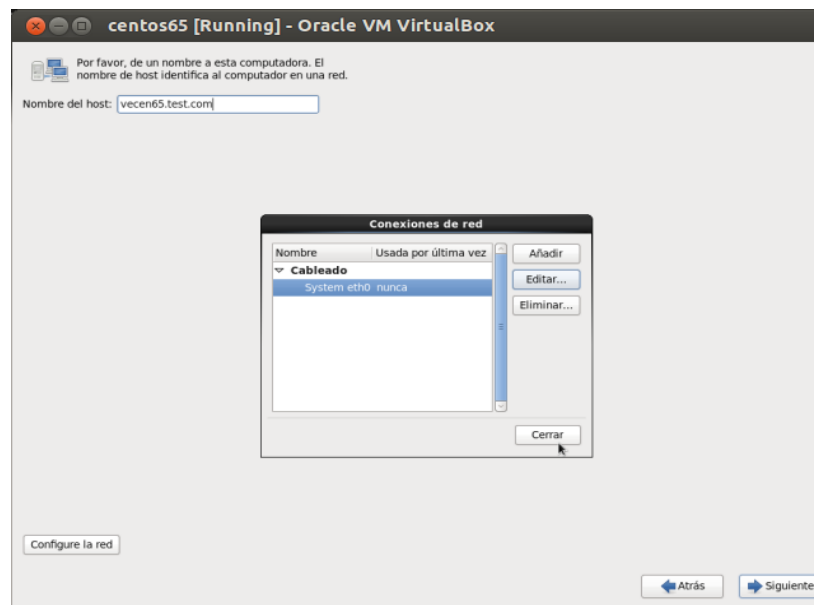


-IMPORTANTE,

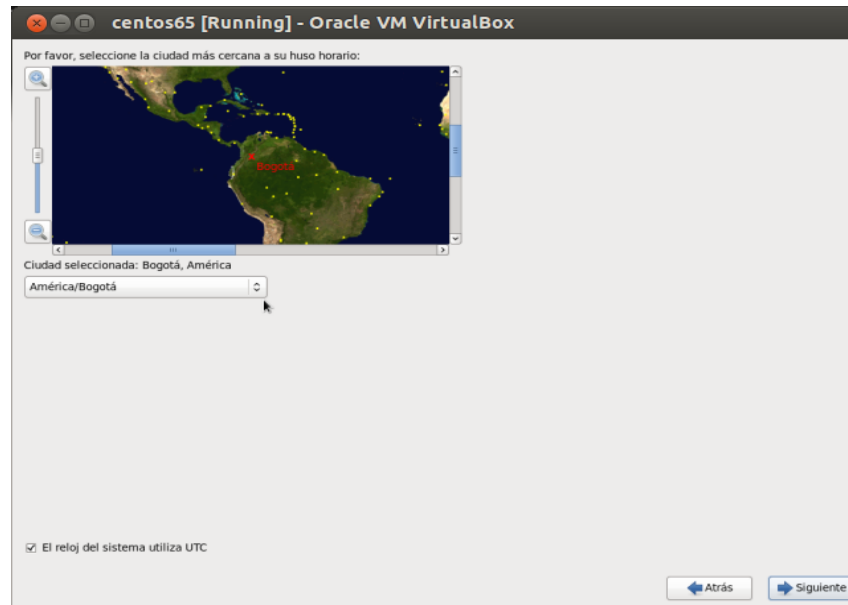
Marcamos la opción Conectar automáticamente. Por lo general la conexión será configurada por DHCP, en caso contrario podemos activar los valores en las otras pestañas de esta ventana. Click al botón Aplicar



-Ya configurada la conexión, presionamos click al botón Cerrar y Siguiente

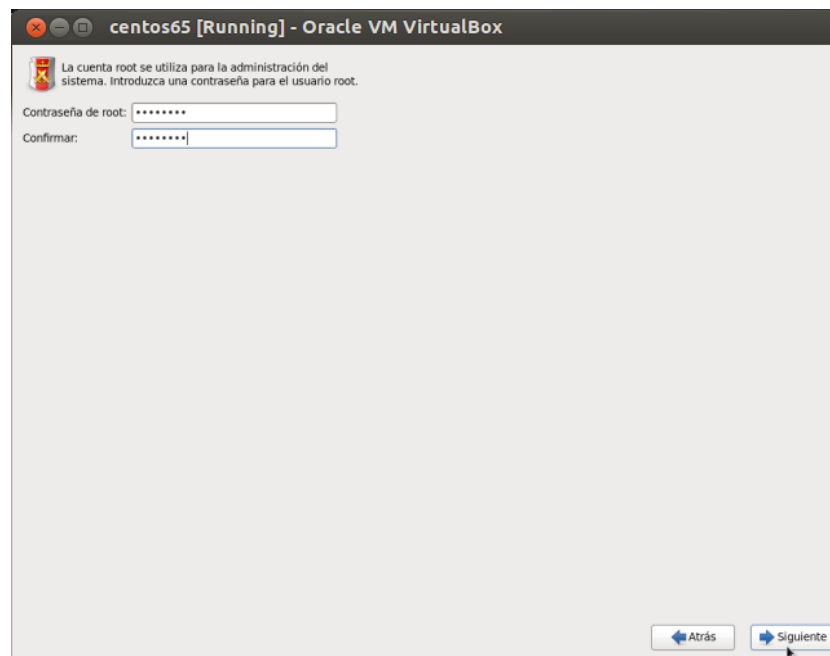


-Elegimos la Zona donde está ubicado el equipo. Click al botón siguiente.

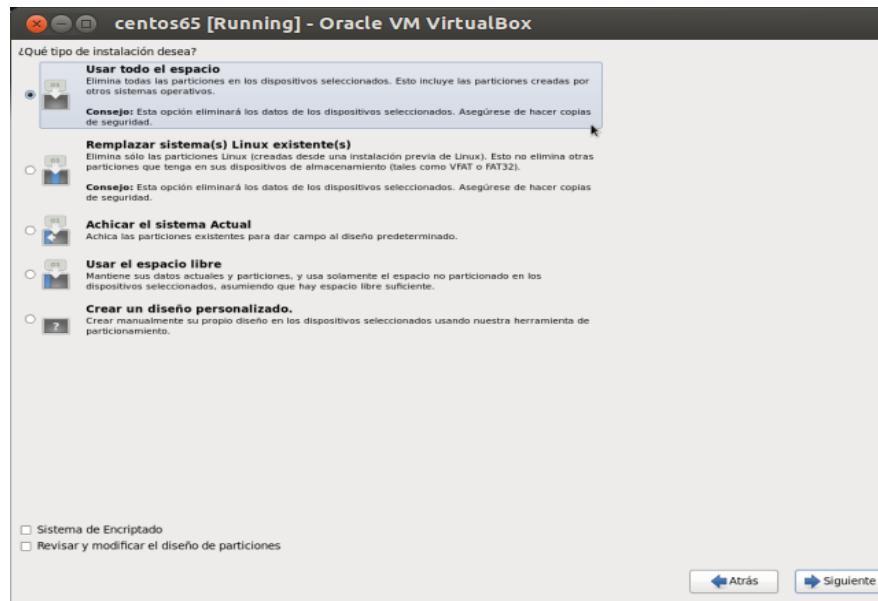


-Escribimos una Contraseña para el usuario root.

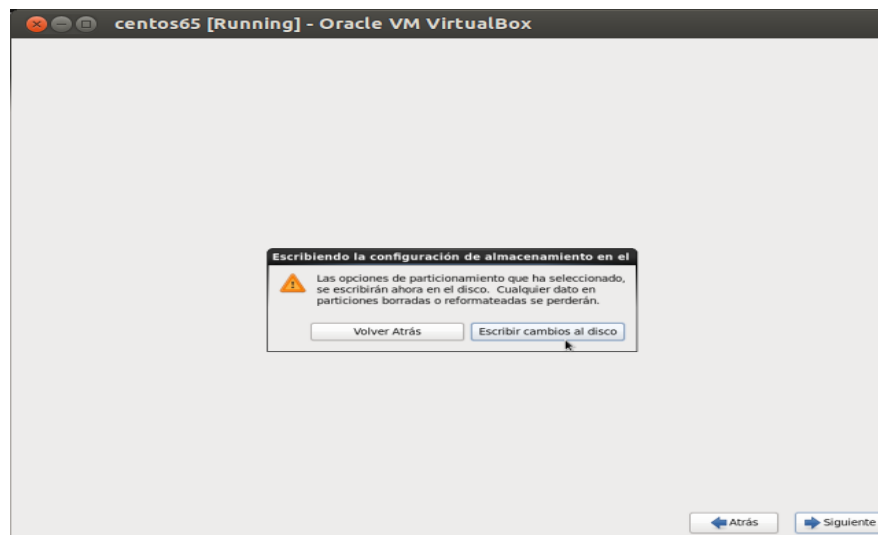
(Administrador del sistema) y presionamos al botón Siguiente.



-En la siguiente pantalla decidiremos como particionaremos el disco para instalar. Si es un equipo que usaremos en su totalidad con la primera es perfecto. Click al botón siguiente

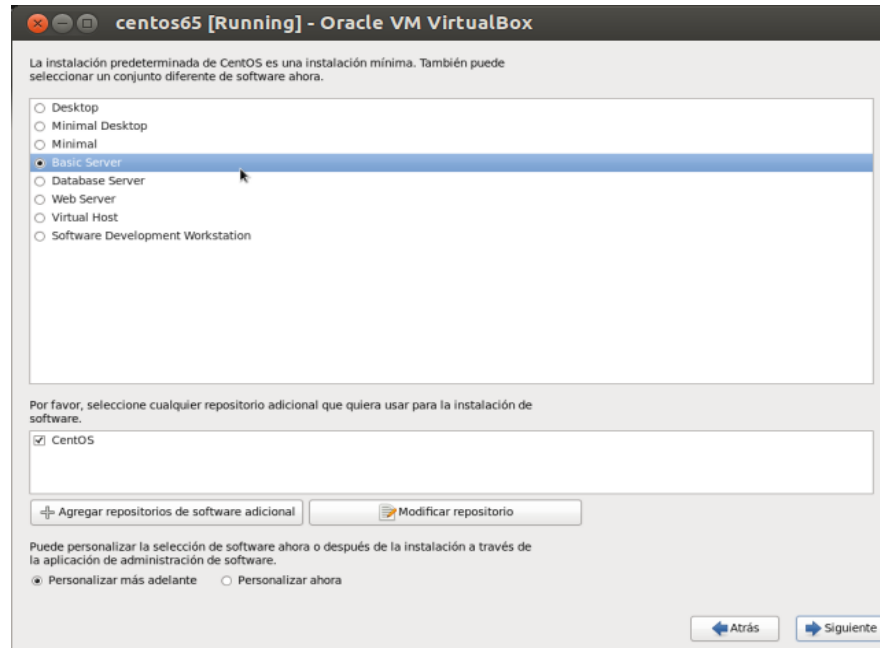


-Ultima oportunidad para no eliminar lo que hay en el disco. Click al botón Escribir cambios al disco.

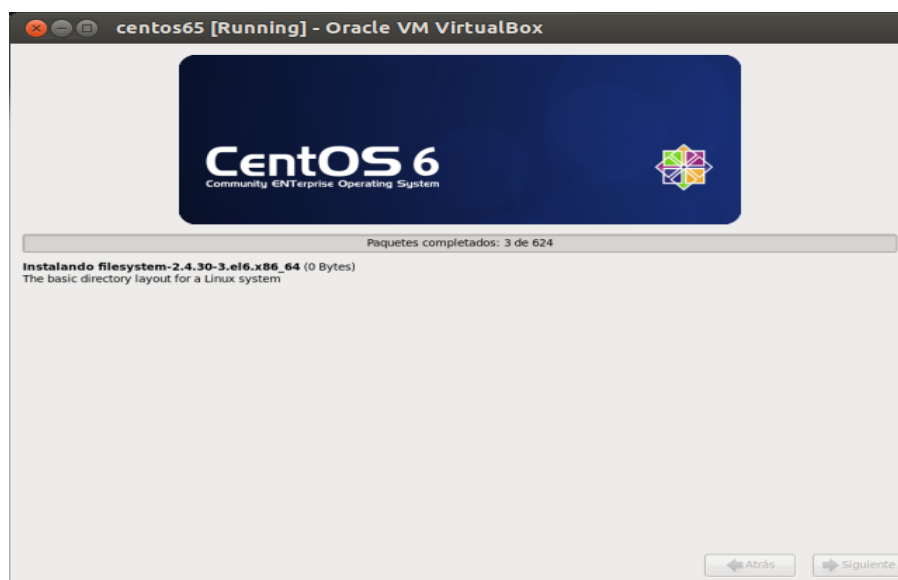


-Siguiente paso, elegir como instalar Centos.

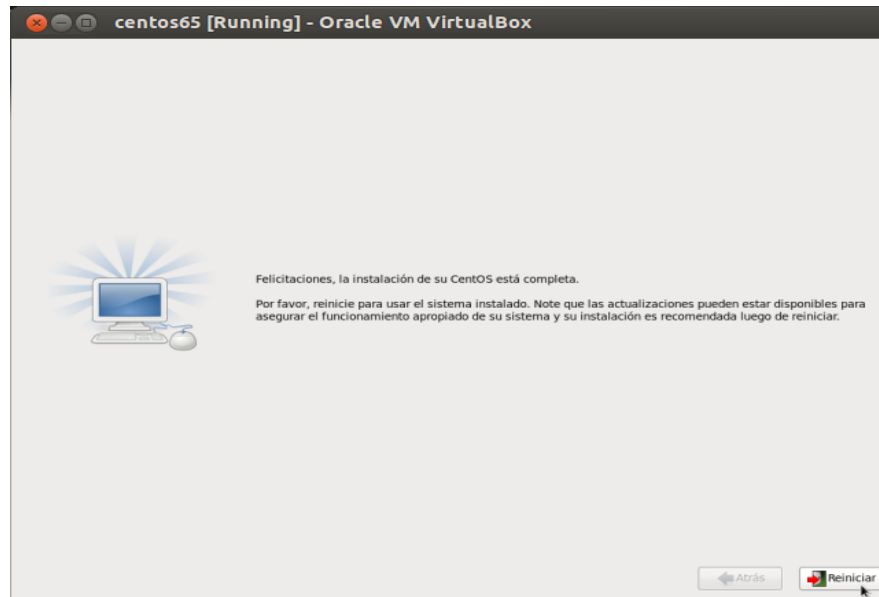
Con la opción Basic Server es suficiente para instalar y tener las herramientas para después personalizarlo. Si deseamos podemos usar las otras opciones que dependen de las necesidades del proyecto. Click al botón Siguiente



-Comienza la instalación.



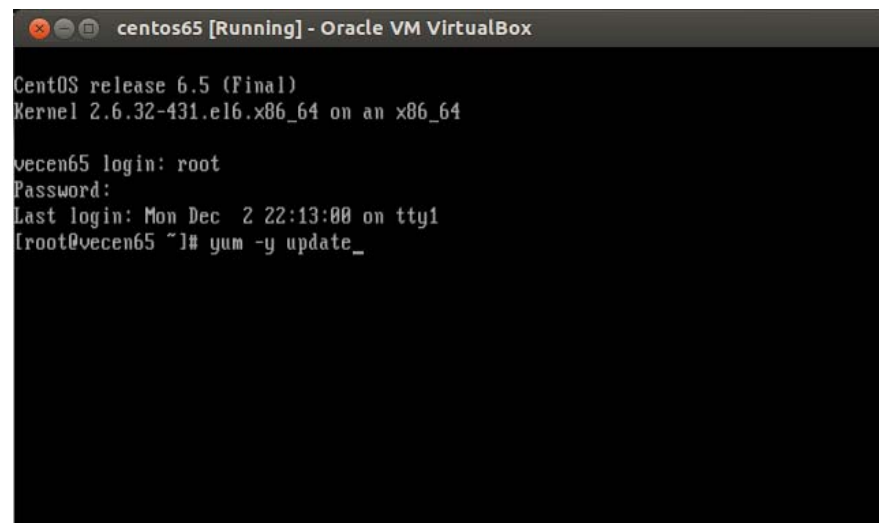
- Linux Centos está instalado. Click al botón Reiniciar



-Al hacer boot por primera vez en el Centos instalado.

Es muy recomendado actualizarlo evitando bugs u otros problemas. Para esto ejecutamos logeados como root

```
yum -y update
```



-Se descargan los paquetes y así queda actualizado el sistema centos 6.5

```
centos65 [Running] - Oracle VM VirtualBox
49.x86_64/6.5)
From : /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Updating   : dracut-004-336.el6_5.2.noarch                1/6
  Updating   : dracut-kernel-004-336.el6_5.2.noarch        2/6
  Updating   : centos-release-6-5.el6.centos.11.2.x86_64  3/6
  Cleanup    : dracut-kernel-004-335.el6.noarch           4/6
  Cleanup    : dracut-004-335.el6.noarch                   5/6
  Cleanup    : centos-release-6-5.el6.centos.11.1.x86_64  6/6
  Verifying  : dracut-004-336.el6_5.2.noarch              1/6
  Verifying  : centos-release-6-5.el6.centos.11.2.x86_64  2/6
  Verifying  : dracut-kernel-004-336.el6_5.2.noarch       3/6
  Verifying  : dracut-004-335.el6.noarch                   4/6
  Verifying  : centos-release-6-5.el6.centos.11.1.x86_64  5/6
  Verifying  : dracut-kernel-004-335.el6.noarch           6/6

Updated:
centos-release.x86_64 0:6-5.el6.centos.11.2 dracut.noarch 0:004-336.el6_5.2
dracut-kernel.noarch 0:004-336.el6_5.2

Complete!
[root@vecen65 ~]# _
```

ANEXO 4

INSTALACION APLICACIÓN ZONEMINDER

INDICE

| | |
|-------------------------------------------------------------------|---|
| Usar usuario de root para iniciar | 1 |
| Iniciando la instalación de mysqld..... | 2 |
| Cambio de credenciales..... | 3 |
| Editar /etc/php.ini. | 3 |
| Verificar que inicialmente ZoneMinder esté bien configurado. | 4 |
| Configura un servidor automáticamente. | 4 |
| Instalación de la política SELinux | 5 |
| Finalmente ,se puede iniciar el servicio de ZonemMnder | 6 |

Usar usuario de root para iniciar

Antes de realizar la instalación de Zoneminder es recomendable trabajar con el usuario root para que tenga todos los permisos y accesos. Para usar un servidor el mismo debe estar configurado con todas las segurides con el comando mysqld como se muestra en la pantalla siguiente

```
File Edit View Search Terminal Help
What's New
=====
1. Due to the active state of the ZoneMinder project, we now recommend granting
ALL permission to the ZoneMinder mysql account. This change must be done
manually before ZoneMinder will run. See the installation steps below.

2. A new permission group called "Groups" has been added. This allows the
system administrator to assign "view", "edit", or "none" permission to
normal users, without giving them access to the rest of the ZoneMinder
system. During an upgrade, existing accounts will default to a Groups
permission of "none".

3. This package now requires the HTTPS protocol to access the web portal.
Requests using HTTP will auto-redirect to HTTPS. See README.https for
more information.

New installs
=====
1. Unless you are already using MySQL server, you need to ensure that
the server is confired to start during boot and properly secured
by running:

    sudo service mysqld start
    /usr/bin/mysql_secure_installation
    sudo chkconfig mysqld on

2. Using the password for the root account set during the previous step, you
will need to create the ZoneMinder database and configure a database
account for ZoneMinder to use:

    mysql -uroot -p < /usr/share/zoneminder/db/zm_create.sql
    mysql -uroot -p -e "grant all on zm.* to \
                        'zmuser'@localhost identified by 'zmpass';"
    mysqladmin -uroot -p reload

The database account credentials, zmuser/zmpass, are arbitrary. Set them to
anything that suits your environment.
```

Iniciando la instalación de mysqld.

Por defecto una instalación mysqld tiene un usuario anónimo para que se registren sin tener que usar el usuario de root y también se lo usa para realizar pruebas .

```
File Edit View Search Terminal Help
Please report any problems with the /usr/bin/mysqlbug script!

Starting mysqld: [ OK ]
[admin@controlcam Desktop]$ /usr/bin/mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
SERVICES IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MySQL to secure it, we'll need the current
password for the root user. If you've just installed MySQL, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password
: YES)
Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MySQL
root user without the proper authorisation.

Set root password? [Y/n] Y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MySQL installation has an anonymous user, allowing anyone
to log into MySQL without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.
```

Cambio de credenciales.

La base de datos cuenta con credenciales arbitrarias y hay que cambiarlas en momento de la instalación con los comandos ZM_DB_USER y ZM_DB_PASS.

Adicionalmete, se edita :

/usr/share/zoneminder/www/api/app/Config/database.php de una forma similar que el cambio de usuario y password en el paso anterior .

```
File Edit View Search Terminal Help
```

```
The database account credentials, zmuser/zmpass, are arbitrary. Set them to anything that suits your environment.
```

3. If you have chosen to change the zoneminder mysql credentials to something other than zmuser/zmpass then you must now edit /etc/zm.conf. Change ZM_DB_USER and ZM_DB_PASS to the values you created in step 2.

```
Additionally, you must also edit /usr/share/zoneminder/www/api/app/Config/database.php in a similar manner. Scroll down and change login and password to the values you created in the previous step.
```

Editar /etc/php.ini.

Quitar comentario de la línea date.timezone y añadir la zona horaria. PHP arrojará un error si no está configurado, o si está configurado Incorrectamente, que aparecerán en el registro de zoneminder.

4. Edit /etc/php.ini, uncomment the date.timezone line, and add your local timezone. PHP will complain loudly if this is not set, or if it is set incorrectly, and these complaints will show up in the zoneminder logging system as errors

```
If you are not sure of the proper timezone specification to use, look at http://php.net/date.timezone
```

```

; Module Settings ;
; Defines the default timezone used by the date functions
; http://www.php.net/manual/en/datetime.configuration.php#ini.date.timezone
date.timezone = America/Guayaquil

; http://www.php.net/manual/en/datetime.configuration.php#ini.date.default-latitude
;date.default_latitude = 31.7667

; http://www.php.net/manual/en/datetime.configuration.php#ini.date.default-longitude
;date.default_longitude = 35.2333

; http://www.php.net/manual/en/datetime.configuration.php#ini.date.sunrise-zenith
;date.sunrise_zenith = 90.583333

; http://www.php.net/manual/en/datetime.configuration.php#ini.date.sunset-zenith
;date.sunset_zenith = 90.583333

[filter]
; http://www.php.net/manual/en/filter.configuration.php#ini.filter.default
E486: Pattern not found: ñ
948,1 57%

```

Verificar que inicialmente ZoneMinder esté bien configurado.

Con la siguiente instrucción se evidenciará que esté correcto:

```
/etc/httpd/conf.d/zoneminder.conf
```

5. Verify the default ZoneMinder Apache configuration meets your needs:

```
/etc/httpd/conf.d/zoneminder.conf
```

When in doubt, leave this configuration as it is.

Configura un servidor automáticamente.

Con la siguiente instrucción :

6. Configure the web server to start automatically:

```
sudo chkconfig httpd on
sudo service httpd start
```

Instalación de la política SELinux

En este paquete se configurará e instalará automáticamente una política SELinux llamado local_zoneminder. Una copia de la documentación de esta política está guardada en una carpeta de zoneminder. Sin embargo, todavía es posible que se generen problemas de SELinux. Si es así, se desactiva SELinux permanentemente editando lo siguiente:

```
/ Etc / selinux / conf
```

7. This package will automatically configure and install an SELinux policy called local_zoneminder. A copy of this policy is in the documentation folder.

It is still possible to run into SELinux issues, however. If this is case, you can disable SELinux permanently by editing the following:

```
/etc/selinux/conf
```

Change SELINUX line from "enforcing" to "disabled". This change will not take effect until a reboot, however. To avoid a reboot, execute the following from the commandline:

```
sudo setenforce 0
```

Cambie la línea SELINUX de "inforced" a "disabled". Este cambio no tendrá efecto hasta un reinicio. Para evitar un reinicio, ejecute la siguiente línea de comandos:

```
Sudo setenforce 0
```

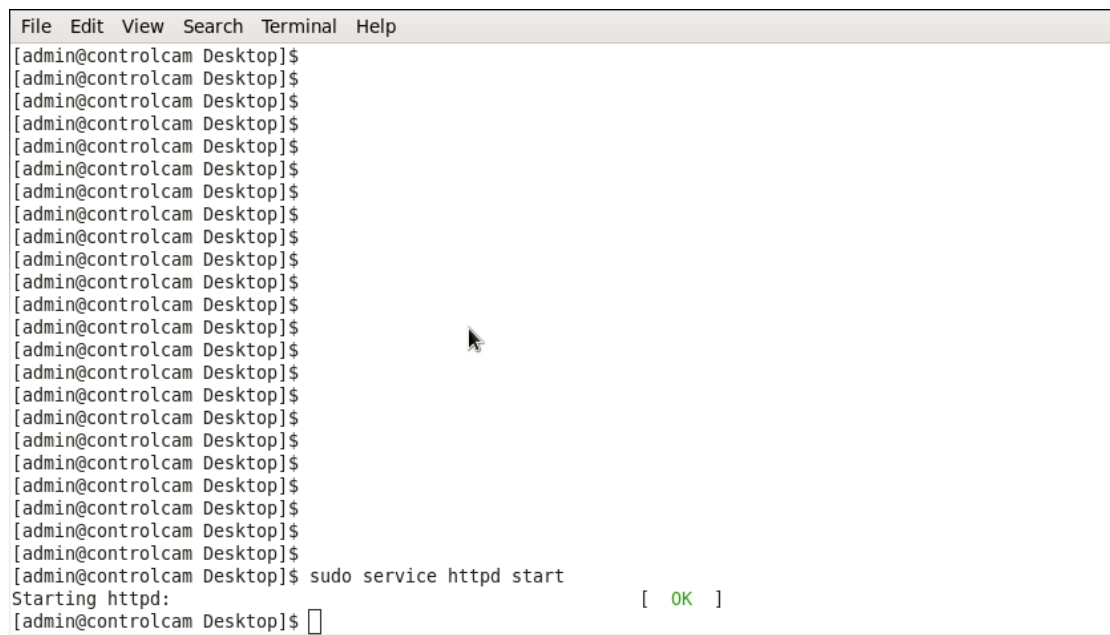
```
File Edit View Search Terminal Help
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#   targeted - Targeted processes are protected,
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Finalmente ,se puede iniciar el servicio de ZonemMnder .

8. Finally, you may start the ZoneMinder service:

```
sudo service zoneminder start
```

Then point your web browser to `http://<machine name or ip>/zm`



```
File Edit View Search Terminal Help
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$
[admin@controlcam Desktop]$ sudo service httpd start
Starting httpd: [ OK ]
[admin@controlcam Desktop]$
```