Universidad Nacional Autónoma De Nicaragua
UNAN - Managua
Recinto Universitario Rubén Darío
Facultad de Ciencias e Ingenierías
Departamento de Tecnología
Ingeniería en Electrónica

Seminario de Graduación

Título:

- **Implementación de un sistema de vigilancia y seguridad con cámaras Web e IP a través de un servidor Web SLES en una casa residencial del departamento de Managua.**

Integrantes:

- **Br. Pérez Estrada Gerson Eliezer.**
- **Br. Obando Lezama Rolan Antonio.**

Tutor:

MSc. Edwin Quintero Carballo.

Managua 3 de Febrero del 2012

TITULO:

- Implementación de un sistema de vigilancia y seguridad con cámaras Web e IP a través de un servidor web SLES en una casa residencial del departamento de Managua.

INDICE

Capítulo I

1.1 RESUMEN

El presente trabajo de Seminario de Graduación, es titulado: Implementación de un sistema de vigilancia y seguridad con cámaras Web e IP a través de un servidor web SLES en una casa residencial del departamento de Managua.

El sistema cuenta con una interfaz Web controlada por un sistema de gestión de contenidos llamado Joomla, que permite editar el contenido de un sitio Web de manera sencilla e incorporar la interfaz Web del software multimedia llamado ZoneMinder compatible con sistemas operativos Linux, que permite la visualización y control de toda la información provenientes de las cámaras.

El ZoneMinder es un conjunto de aplicaciones que proporcionan una completa solución de video vigilancia permitiendo capturar, analizar, grabar y monitorear cualquier cámara CCTV, cámaras IP, Webcam, etc, conectada a un ordenador basado en Linux.

Se realizó una evaluación de la red local con el fin de localizar los puntos estratégicos donde se ubicaran las cámaras, tomando en cuanto una serie de parámetros relacionados con el valor económico de artículos existentes en el local, distancia y rango de cobertura de las cámaras.

El acceso a la Web se hace mediante la url: www.electronicsecurity.com. Este sitio cuenta con una página Web dinámica. La cual tiene una serie de políticas de acceso restringidos al público en general para evitar la divulgación de información privada que solamente concierne al administrador del sistema y al dueño del local.

El servidor está provisto con un servicio de acceso remoto al sistema, mediante el protocolo SSH, permitiéndonos realizar configuraciones de forma segura y manejar por completo el servidor.

1.2 INTRODUCCIÓN

Desde su aparición sobre la tierra, el hombre sintió la necesidad de protegerse. Desde las primeras sociedades humanas, una de las principales funciones del estado fue administrar justicia y proveer seguridad. La inseguridad es un mal que se genera en la sociedad y es más, cuanto mayor es la concentración y la aparente evolución social; pues las causas que la generan son cada vez más complejas e interrelacionadas.

Para contrarrestar este problema, el ser humano ha creado aplicaciones y dispositivos de vigilancia que dan solución a estos conflictos, brindan seguridad y bienestar al usuario y sus bienes.

Con los grandes avances que ha alcanzado el Internet, han surgido aplicaciones que integran voz, audio y video, estos son usados en las radios, TV, móviles y en el campo de los sistemas electrónicos de vigilancia. Los avances tecnológicos han permitido el desarrollo de hardware y software suficientemente potentes y eficientes como para realizar todas las funciones de los sistemas analógicos tradicionales, y superarlos ampliamente con la incorporación de funciones "inteligentes" que eran solo fantasía hasta hace algunos años.

Este trabajo está basado en un sistema de vigilancia con cámaras Web e IP, el cual busca dar un servicio de calidad y de gran satisfacción al usuario, utilizando tecnología de punta y enfocada a la necesidades actuales de seguridad.

En el proyecto se aborda los siguientes aspectos: Implementación de un sistema de vigilancia y seguridad con cámaras Web e IP, un diagnóstico de la red y sus posibles mejoras. Se realizará la configuración de un servidor web bajo plataforma SLES (Linux) compatible con el sistema de vigilancia que será controlado por un software de monitoreo llamado ZoneMinder.

El sistema tiene políticas de acceso restringido y seguro, basados en cuentas de usuarios con atributos y contraseñas. Se incorporó un servicio SSH que permitirá realizar configuraciones, soporte técnico y acceso de forma remota de manera segura al servidor.

Se diseñó una página web, que le permitirá al usuario una interfaz amigable y de fácil navegación para que pueda visualizar imágenes y videos tomadas de forma simultánea en su hogar. El servidor DNS facilitará al usuario el acceso, sin tener que recordar direcciones IP.

Se realizaron las configuraciones necesarias para el buen funcionamiento de ZoneMinder y se tomaron en cuenta parámetros establecidos, que permitan una ubicación estratégica de las cámaras y su monitoreo.

1.3 ANTECEDENTES

En este trabajo se plantea la situación actual de cada una de las tecnologías a utilizar, y cómo ha evolucionado su implementación. Las ventajas y desventajas, su importancia y la factibilidad de sus aplicaciones. Esto nos permitirá diseñar una red que incluya un sistema de vigilancia y seguridad con cámaras Web e IP, a través de un servidor SLES en una casa residencial del departamento de Managua.

Por medio de las investigaciones realizadas en los medios de información, se encontró una serie de trabajos previos, los cuales abordan aplicaciones similares de sistemas de vigilancia en ambientes diferentes, pero siguiendo el mismo objetivo, preservar el bienestar de los usuarios y sus bienes.

A continuación se presenta un breve resumen de los aspectos abordados en dichos trabajos:

En el pasado todas las cámaras de video eran analógicas. La señal de video analógica se conectaba directamente a cualquier monitor, video grabador o Frame grabber. El sensor CCD es también analógico y las primeras generaciones de cámaras CCD se fabricaron para ser compatibles con todos los sistemas analógicos existentes en el momento de su aparición.

Un detector de movimiento es un dispositivo electrónico equipado de sensores que responden a un movimiento físico. Se encuentran, generalmente, en sistemas de seguridad o en circuitos cerrados de televisión. El sistema puede estar compuesto, simplemente, por una cámara de vigilancia conectada a un ordenador, que se encarga de generar una señal de alarma o poner el sistema en estado de alerta cuando algo se mueve delante de la cámara. Aunque, para mejorar el sistema se suele utilizar más de una cámara.

Es por eso que los Ing. Cerda, Suazo y Olivas egresados de la UNAN-MANAGUA en el año (2007), lo abordaron en su trabajo monográfico, titulado: Diseño de un Sistema de Control y Vigilancia a partir de Sensores y Video cámaras en el Instituto Politécnico de la Salud (POLISAL).

La cámaras analógicas su principal característica es la necesidad de conectarlas a su cable. El cable utilizado para las cámaras analógicas es el coaxial, lo cual lo hace algo incómodo para manejarlo. Ya que se debe enviar por cada cámara un cable, y hacer una conexión punto a punto, por lo tanto si son varias cámaras, se va incrementando el diámetro del canal por donde se envía el cable.

Este tipo de sistemas requieren de una gran infraestructura de cableado tanto de vídeo como de energía para cada cámara, una cámara analógica se puede conectar a cualquier DVR, no hay incompatibilidad entre cámaras y DVR. Este Dispositivo es el que almacena video en un disco duro proveniente de una o más cámaras de video. Generalmente son parte de un sistema de seguridad. Suelen tener entradas para 4, 8 o 16 cámaras, con sus respectivas entradas de alarma. Esto es planteado por el Ing. Yuri Ezequiel Valle en su trabajo monográfico titulado: Sistema de Vigilancia y Seguridad con cámaras analógicas con acceso remoto.

El cual plantea que la mayor desventaja de un sistema con cámaras analógicas es su costo, ya que su implementación con acceso remoto incluye el uso de DVR y tarjetas de red Ethernet para poder conectarse de forma remota.

Lo último en tecnologías de vigilancias son las cámaras IP, que son dispositivos autónomos que cuentan con un servidor web de video incorporado, lo que les permite transmitir su imagen a través de redes IP como redes LAN, WAN e Internet. Las cámaras IP permiten al usuario tener la cámara en una localización y ver el vídeo en tiempo real desde otro lugar a través de Internet. Tienen incorporado un ordenador, pequeño y especializado en ejecutar aplicaciones de red. Por lo tanto, la

cámara IP no necesita estar conectada a un PC para funcionar. Esta es una de sus diferencias con las denominadas cámaras web.

Las imágenes se pueden visualizar utilizando un navegador Web estándar y pueden almacenarse en cualquier disco duro. Se necesita una solución de vigilancia IP para garantizar la seguridad de personas y lugares, como para supervisar propiedades e instalaciones de modo remoto o retransmitir eventos en la Web con imágenes y sonidos reales, las cámaras IP satisfacen estas necesidades.

Las cámaras ip poseen muchas ventajas frente a los sistemas tradicionales de vigilancia mediante circuito cerrado de TV (CCTV), las fundamentales son:

- Acceso Remoto: La observación y grabación de los eventos no tiene por qué realizarse en el sitio como requieren los sistemas CCTV.

- Costo reducido: La instalación es mucho más flexible ya que se basa en la infraestructura de la Red Local existente o nueva, o también en la conexión directa a un Router, bien por cable o de forma inalámbrica (Wireless LAN). Se elimina el costo de los sistemas de grabación digital de los CCTV, ya que las grabaciones de las cámaras ip se realizan en el disco duro de un PC de la propia red local o en un PC remoto.

- Flexibilidad frente a la ampliación del sistema: Los sistemas tradicionales CCTV generalmente requieren duplicar los sistemas de monitorización cuando se amplía el sistema, los sistemas de cámaras ip permiten su ampliación sin necesidad de invertir en nuevos sistemas de monitorización (DVR).

En la actualidad en Nicaragua no existen trabajos previos donde se ha implementado sistemas de seguridad y vigilancia con cámaras IP, aunque existen empresas privadas que se dedican a la venta e instalación de estos sistemas, como es el caso de

la empresa CONDOR Comunicaciones, la cual se especializa en telecomunicaciones con más de 20 años de experiencia, ofreciendo soluciones integrales y eficientes. La cual brinda servicios de vigilancia a instituciones bancarias, educativas, industriales y de comercio con tecnología de cámaras IP marca AXIS.

Otras empresas que ofrecen estos servicios son: Intelligent Solutions S.A, Protection Electronic Nicaragua, Compu-Partes S.A, Tecnología computarizada S.A todas distribuyen cámaras IP marca Panasonic.

Todas las empresas antes mencionadas, utilizan sistemas de vigilancia con cámaras IP bajo plataforma Windows, configurando cada uno de los software que ya vienen incorporados en las cámaras por defecto.

En este caso para la implementación de este sistema de seguridad de cámaras Web e IP se configuro un software de vigilancia bajo plataforma Linux que permitirá el monitoreo de las cámaras, un mayor control de toda la información proveniente de cada cámara Web e IP, brindara seguridad y una interfaz agradable al usuario, por medio de una página web creada especialmente para este sistema.

La configuración de sistemas operativos linux es abordado por el del Ing. Noel Bernardino Flores con su trabajo titulado: Configuración de Servidores bajo Plataforma LINUX, para obtener su diploma como Ing. en Sistemas y Computación de la Universidad Popular Nicaragüense (UPONIC). El cual sirvió de guía para la configuración del servidor Suse. En su trabajo aborda a detalle los pasos a seguir para configurar los servicios DNS, WEB o HTTP, SSH en S.O Linux (Debían, Centos).

1.4 JUSTIFICACIÓN

El tema "Implementación de un sistema de vigilancia y seguridad con cámaras Web e IP a través de un servidor web SLES en una casa residencial del departamento de Managua", fue seleccionado debido al deseo de aportar una mejora a los sistemas de vigilancia tradicionales, ya que en la actualidad estos sistemas se basan en servidores administrados bajo plataformas Windows. Gracias al desarrollo que ha tenido en los últimos años las plataformas Linux, permite aplicar y aprovechar los recursos de hardware, es un sistema operativo libre, la mayoría de sus aplicaciones son gratuitas y los niveles de seguridad son muy altos. Además permite hacer actualizaciones automáticas del sistema y sus aplicaciones.

El acceso remoto se configuro mediante SSH, el cual permitirá realizar configuraciones y mantener un control del servidor desde cualquier parte del mundo (acceso con una conexión a internet) a través de otra PC, transferir archivos y realizar respaldo de las imágenes y videos que se estén gravando, dar mantenimiento al sistema operativo (actualizaciones, instalación de nuevas aplicaciones), siempre manteniendo un gran alto nivel de seguridad. Mediante el SSH se usan técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible, para que ninguna otra persona pueda descubrir el usuario y contraseña del sistema, ni lo que se escribe durante toda la sesión.

La interfaz web permitirá que el usuario pueda monitorear sus bienes desde lugares lejanos y al mismo tiempo mantenerse comunicado con el administrador del sistema en caso de anomalías. El acceso a la página web será restringido a través del administrador de contenido Joomla, el cual nos permitirá crear usuarios y contraseñas con atributos, de esta forma se evitara que cualquier persona no autorizada pueda tener acceso a las imágenes trasmitidas por las cámaras Web e IP.

El uso de cámaras IP, permite un gran ahorro en el uso de equipos de alto precio, ya que en los sistemas comunes CCTV (Televisión de Circuito Cerrado) en Windows, son necesarios otros dispositivos para el tratamiento de las imágenes, como es el caso de DVR, video Balum, tarjetas externas de red. La implementación de un software propio de Linux, evita el costo de licencias para las cámaras IP, debido a que la visualización de varias cámaras a la vez requiere de software especializado cuyo costo es bastante alto.

Otra razón es el alto índice delictivo, producto de la posición geográfica de la casa residencial, ya que esta se encuentra en el Bo. Venezuela, el cual limita con barrios como la URZ, Villa Candil y Colonia Nicarao, los cuales poseen muchos grupos antisociales que se dedican al robo y la disputa de territorio.

1.5 OBJETIVOS

1.5.1 Objetivo General:

- Diseñar una red que incluya un sistema de vigilancia y seguridad con cámaras Web e IP a través de un servidor web SLES en una casa residencial del departamento de Managua.

1.5.2 Objetivos Específicos:

- Realizar un diagnóstico de la red LAN actual en la casa residencial y sus posibles mejoras con el objetivo de implementar un sistema de vigilancia y seguridad que permita el control y supervisión de los bienes del dueño de la propiedad.

- Diseñar una red de intranet que incluya cámaras Web e IP con acceso remoto desde cualquier parte del mundo a través de internet.

- Configurar un servidor web bajo plataforma SLES compatible con el sistema de vigilancia y seguridad.

- Configurar el software de monitoreo y vigilancia ZoneMinder para que permita la visualización, almacenamiento y tratamiento de las imágenes capturadas por las cámaras.

- Diseñar y programar una página Web que permita la interacción usuario-sistema de forma fácil, amigable y segura.

Capítulo II

MARCO TEORICO

2.1 Sistemas de vigilancia

Los sistemas de vigilancia por vídeo existen desde hace 25 años. Empezaron siendo sistemas analógicos al 100% y paulatinamente se fueron digitalizando. Los sistemas de hoy en día han avanzado mucho desde la aparición de las primeras cámaras analógicas con tubo conectadas a VCR (Escamilla, 2005).

En la actualidad, estos sistemas utilizan cámaras y servidores de PC para la grabación de vídeo en sistemas completamente digitalizados. Sin embargo, entre los sistemas completamente analógicos y los sistemas completamente digitales existen diversas soluciones, que son parcialmente digitales. Dichas soluciones incluyen un número de componentes digitales pero no constituyen sistemas completamente digitales.

Completamente Analógico	- Sistemas de circuito cerrado de TV analógicos usando VCR.
Parte Digital	- Sistemas de circuito cerrado de TV analógicos usando DVR. - Sistemas de circuito cerrado de TV analógicos usando DVR de red.
Completamente Digital	- Sistemas de video IP que utilizan servidores de Video. - Sistema de red de video usando Cámaras de red.

Tabla 1. Tipos de sistemas de seguridad

2.1.1 Sistemas de circuito cerrado de TV analógicos usando VCR (Figura 1): Un sistema de circuito cerrado de TV (CCTV) analógico que utilice un VCR (grabador de vídeo) representa un sistema completamente analógico formado por cámaras analógicas con salida coaxial, conectadas al VCR para grabar.

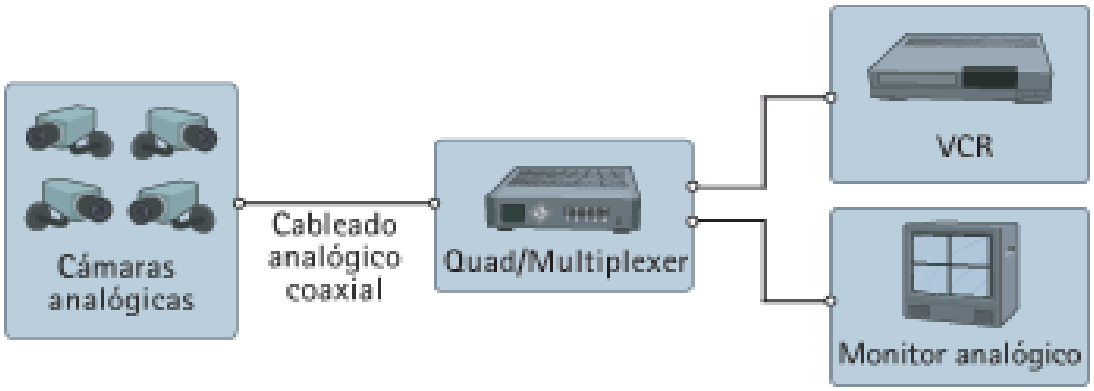


Figura 1. CCTV con VCR

El VCR utiliza el mismo tipo de cintas que una grabadora doméstica. El vídeo no se comprime y, si se graba a una velocidad de imagen completa, una cinta durará como máximo 8 horas. En sistemas mayores, se puede conectar un quad o un multiplexor entre la cámara y el VCR. El quad/multiplexor permite grabar el vídeo procedente de varias cámaras en un solo grabador, pero con el inconveniente que tiene una menor velocidad de imagen. Para monitorizar el vídeo, es necesario un monitor analógico.

2.1.2 Sistemas de circuito cerrado de TV analógicos usando DVR (Figura 2): Un sistema de circuito cerrado de TV (CCTV) analógico usando un DVR (grabador de vídeo digital) es un sistema analógico con grabación digital. En un DVR, la cinta de vídeo se sustituye por discos duros para la grabación de vídeo, y es necesario que el vídeo se digitalice y comprima para almacenar la máxima cantidad de imágenes posible de un día.

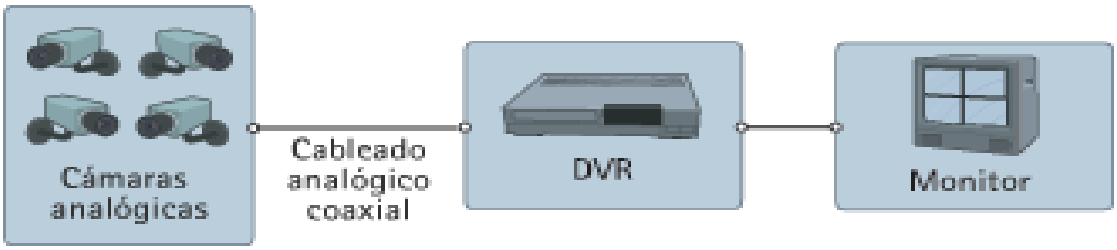


Figura 2. CCTV con DVR

Con los primeros DVR, el espacio del disco duro era limitado, por tanto, la duración de la grabación era limitada, o debía usarse una velocidad de imagen inferior. El reciente desarrollo de los discos duros significa que el espacio deja de ser el

principal problema. La mayoría de DVR dispone de varias entradas de vídeo, normalmente 4, 8 ó 16, lo que significa que también incluyen la funcionalidad de los quads y multiplexores.

El sistema DVR añade las siguientes ventajas:

- No es necesario cambiar las cintas.
- Calidad de imagen constante.

2.1.3 Sistemas de circuito cerrado de TV analógicos usando DVR de red (Figura 3): Es un sistema parcialmente digital que incluye un DVR IP equipado con un puerto Ethernet para conectividad de red. Como el vídeo se digitaliza y comprime en el DVR, se puede transmitir a través de una red informática para que se monitorice desde un PC en una ubicación remota.

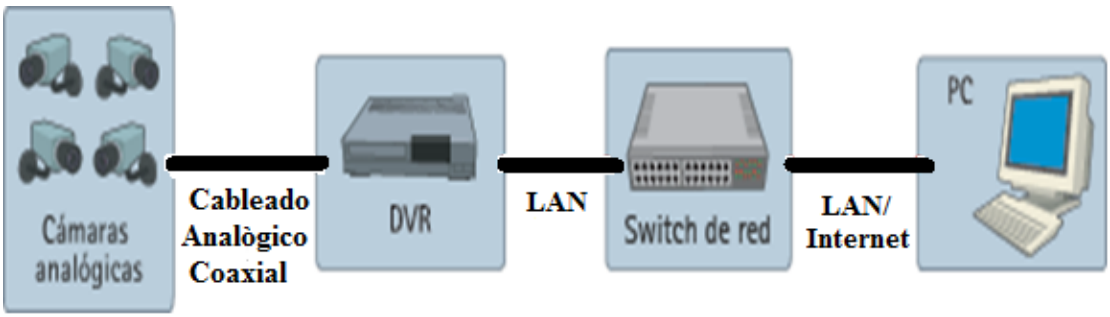


Figura 3. CCTV usando DVR de red

Algunos sistemas pueden monitorizar tanto vídeo grabado como en directo, mientras otros sólo pueden monitorizar el vídeo grabado. Además, algunos sistemas exigen un cliente Windows especial para monitorizar el vídeo, mientras que otros utilizan un navegador web estándar, lo que flexibiliza la monitorización remota.

El sistema DVR IP añade las siguientes ventajas:

- Monitorización remota de vídeo a través de un PC.

- Funcionamiento remoto del sistema.

2.1.4 Sistemas de vídeo IP que utilizan servidores de vídeo (Figura 4): Un sistema de vídeo IP que utiliza servidores de vídeo incluye un servidor de vídeo, un conmutador de red y un PC con software de gestión de vídeo. La cámara analógica se conecta al servidor de vídeo, el cual digitaliza y comprime el vídeo. A continuación, el servidor de vídeo se conecta a una red y transmite el vídeo a través de un conmutador de red a un PC, donde se almacena en discos duros. Esto es un verdadero sistema de vídeo IP.

Un sistema de seguridad que utiliza servidores de vídeo añade las ventajas siguientes:

- Utilización de red estándar y hardware de servidor de PC para la grabación y gestión de vídeo.
- El sistema es escalable en ampliaciones de una cámara cada vez.
- Es posible la grabación fuera de las instalaciones.
- Preparado para el futuro, ya que este sistema puede ampliarse fácilmente incorporando cámaras IP.

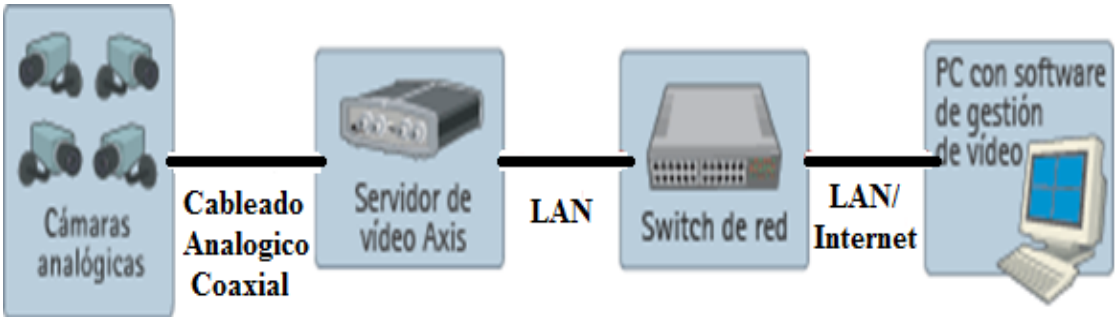


Figura 4. Sistemas de vigilancia IP con servidores de video.

El diagrama de la figura 4 muestra un verdadero sistema de vídeo IP, donde la información del vídeo se transmite de forma continua a través de una red IP. Utiliza

un servidor de vídeo como elemento clave para migrar el sistema analógico de seguridad a una solución de vídeo IP.

2.1.5 Sistemas de vídeo IP que utilizan cámaras IP (Figura 5): Estos sistemas combina una cámara y un ordenador en una unidad, lo que incluye la digitalización y la compresión del vídeo así como un conector de red. El vídeo se transmite a través de una red IP, mediante los conmutadores de red y se graba en un PC estándar con software de gestión de vídeo. Esto representa un verdadero sistema de vídeo IP donde no se utilizan componentes analógicos.

Un sistema de vídeo IP que utiliza cámaras IP añade las ventajas siguientes:

- Cámaras de alta resolución (megapíxel).
- Calidad de imagen constante.
- Alimentación eléctrica a través de Ethernet y funcionalidad inalámbrica
- Funciones de Pan/tilt/zoom, audio, entradas y salidas digitales a través de IP, junto con el vídeo.
- Flexibilidad y escalabilidad completas.

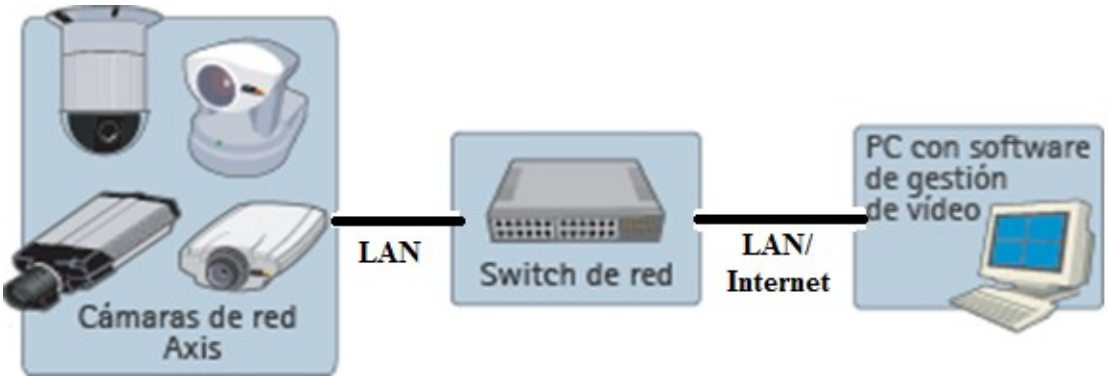


Figura 5. Sistemas de vigilancia con cámaras IP

El diagrama de la figura 5 muestra un verdadero sistema de vídeo IP, donde la información del vídeo se transmite de forma continua a través de una red IP, utilizando cámaras IP. Este sistema saca el máximo partido de la tecnología digital y

proporciona una calidad de imagen constante desde la cámara hasta el visualizador, dondequiera que estén.

2.1.6 Cámaras IP: Son vídeo-cámaras de vigilancia que tienen la particularidad de enviar las señales de video (y en muchos casos audio), estos sistemas han venido actualmente en brindar un fuerte apoyo al tema de la seguridad integral, aludiendo entre sus virtudes ejercer una VIGILANCIA PREVENTIVA, mediante el registro visual de sucesos, estando conectadas directamente a un Router ADSL, o bien a un concentrador de una red local, para poder visualizar en directo las imágenes bien dentro de una red local (LAN), o a través de cualquier equipo conectado a Internet (WAN) pudiendo estar situado en cualquier parte del mundo (Valdivia, 2006).

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

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

Internamente están constituidas por la cámara de vídeo propiamente dicha (Lentes, sensor de imagen, procesador digital de señal), por un motor de compresión de imagen (Chip encargado de comprimir al máximo la información contenida en las imágenes) y por un ordenador en miniatura (CPU, FLASH, DRAM, y módulo ETHERNET/ WIFI) encargado en exclusiva de gestionar procesos propios, tales como la compresión de las imágenes, el envío de imágenes, la gestión de alarmas y avisos, la gestión de las autorizaciones para visualizar imágenes, en definitiva las

cámaras IP son unos equipos totalmente autónomos, lo que permite conectarlo en el caso más sencillo directamente a un Router ADSL, y a la red eléctrica y de esta forma estar enviando imágenes del lugar donde este situada.

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

Aplicaciones más frecuentes de la Cámaras IP

- **Viviendas:** Permitiendo visionar la propia vivienda desde la oficina, desde un hotel, cuando se está de vacaciones.

- **Negocios:** Permitiendo controlar por ejemplo varias sucursales de una cadena de tiendas, gasolineras.

- **Instalaciones industriales:** Almacenes, zonas de aparcamiento, muelles de descarga, accesos, incluso determinados procesos de maquinaria o medidores.

- **Hotelería, restauración, instalaciones deportivas, lugares turísticos:** Cada día es más frecuente que Organismos oficiales, como Comunidades Autónomas, Ayuntamientos, promocionen sus zonas turísticas, o lugares emblemáticos de las ciudades, instalaciones deportivas, implementado en sus páginas Web las imágenes procedentes de Cámaras IP estratégicamente situadas en esos lugares.

- **Instituciones financieras**: Como medida de protección contra fraudes y robos de tarjetas, las instituciones financieras están instalando soluciones de vigilancia para verificar las transacciones de los cajeros automáticos y

proteger áreas delicadas. Cada acción específica, genera archivos de imágenes separados, que son almacenados en una localización central para una posible investigación futura.

- **Tráfico y transporte de personas:** Para satisfacer las necesidades actuales de seguridad en el traslado de viajeros, los nuevos sistemas de vigilancia pueden integrarse con los sistemas de vigilancia existentes, a fin de mejorar la seguridad de los pasajeros en estaciones de ferrocarril, intercambiadores, redes de metro, aeropuertos, y autopistas. Además, las centrales de monitorización de tráfico tienen fácil acceso a las imágenes de carreteras, autopistas y cabinas de peaje.

- **Monitorización de Equipos Técnicos:** En salas de servidores y armarios de conexión de redes, la inspección remota a través de sistemas de vigilancia ayuda a garantizar un servicio de alta calidad en todo momento. La detección de movimiento protege contra entradas no autorizadas. Las funciones de activación de alarmas en función de eventos garantizan que el personal pueda tomar decisiones inmediatas frente a alteraciones ambientales detectadas que pudieran afectar al funcionamiento de los equipos.

- **Prevención contra vandalismo, delincuencia y crimen**: En las áreas urbanas asoladas por problemas de aumento del índice de criminalidad, la instalación de la infraestructura necesaria es costosa y toma mucho tiempo. Los sistemas con cámaras IP reúnen los requisitos de un sistema rentable, de alta calidad, y ha demostrado ser una solución efectiva en la reducción del crimen y la violencia en áreas problemáticas (Gordillo, 2007).

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

- **Acceso Remoto:** La observación y grabación de los eventos no tiene por qué realizarse en el lugar como requieren los sistemas CCTV.

- **Costo reducido:** La instalación es mucho más flexible ya que se basa en la infraestructura de la Red Local existente o nueva, o también en la conexión directa a un Router, bien por cable o de forma inalámbrica (Wireless LAN). Se elimina el costo de los sistemas de grabación digital de los CCTV, ya que las grabaciones se realizan en el disco duro de un PC de la propia red local o en un PC remoto.

- **Flexibilidad frente a la ampliación del sistema:** Los sistemas tradicionales CCTV generalmente requieren duplicar los sistemas de monitorización cuando se amplía el sistema, los sistemas de Cámaras IP permiten su ampliación sin necesidad de invertir en nuevos sistemas de monitorización (Valeriano, 2006).

Un Servidor de Vídeo es una de las partes integradas en el interior de una Cámara de Red. El Servidor de Vídeo internamente está constituido por uno o varios conversores Analógico-Digitales (Chip que pasa la señal de vídeo analógica de las cámaras a formato digital), motor de compresión de imagen (Chip encargado de comprimir al máximo la información contenida en las imágenes), y por un ordenador en miniatura (CPU, FLASH, DRAM, y módulo ETHERNET) encargado en exclusiva de gestionar procesos propios, tales como la compresión de las imágenes, el envío de imágenes, la gestión de alarmas y avisos, la gestión de las autorizaciones para visualizar imágenes, en definitiva es un equipo totalmente autónomo, lo que permite conectarlo, en el caso más sencillo directamente a un Router ADSL, y a la red eléctrica y de esta forma poder enviar imágenes del sistema tradicional de CCTV.

Es posible controlar las cámaras como en los Sistema de Vigilancia CCTV tradicionales. Dentro de la gama de Cámaras IP existe una gran variedad en función

de las aplicaciones que se le vaya a dar, en general existen cámaras Fijas y Cámaras con movimiento. Las Cámaras Pan-Tilt (P/T) así llamadas por disponer de posibilidad de movimiento Horizontal y Vertical, permiten crear un sistema de vigilancia con gran cobertura y gran flexibilidad, ya que en muchas ocasiones pueden sustituir a varias cámaras fijas.

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

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

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

Es posible la conexión de un relé que maneje por ejemplo el encendido de luces, o por ejemplo la apertura de una puerta. Las Cámaras IP y Servidores de Vídeo

disponen de una salida Abierto-Cerrado, que se controla desde el software de visualización.

Las Cámaras IP, y en general todas las cámaras de TV. Están diseñadas para su uso en interiores, en condiciones normales de polvo y humedad y temperatura. Para la utilización de las Cámaras IP o de las cámaras de TV en exteriores o en interiores donde las condiciones de trabajo sean extremas, es necesario utilizar Carcasas de Protección adecuadas a la utilización que se le vaya a dar. Existe gran variedad de carcasas, estancas, con ventilación, con calefacción, metálicas, de plástico, cada aplicación aconsejará la elección del modelo adecuado.

Las cámaras de red y los servidores de video disponen en su software interno de apartados de seguridad que permiten en general establecer diferentes niveles de seguridad en el acceso a las mismas. Los niveles son:

Administrador: Acceso mediante nombre de usuario y contraseña a la configuración total de la cámara.

Usuario: Acceso mediante nombre de usuario y contraseña a la visualización de las imágenes y manejo del relé de salida.

Demo: Acceso libre a la visualización sin necesidad de identificación.

El número de observadores simultáneos que admiten las cámaras IP y los servidores de vídeo en general es de alrededor de 10 a 20. También es posible enviar "snapshots" de forma automática y con período de refresco de pocos segundos, a una página web determinada para que el público en general pueda acceder a esas imágenes (González, 2009).

En general la mayoría de las cámaras IP disponen de micrófonos de alta sensibilidad incorporados en la propia cámara, con objeto de poder transmitir audio mediante el protocolo de conexión UDP.

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

En definitiva los sistemas de compresión de imagen tienen como objetivo ajustar la información que se produce a los anchos de banda de los sistemas de transmisión de la información como por ejemplo el ADSL. Los estándares de compresión actuales son el MJPEG y MPG4, este último es el más reciente y potente.

2.1.7 Uso de cámaras IP en SO Windows.

Para la visualización de las cámaras IP lo único que se necesita es que en el sistema operativo del PC se encuentre instalado el Microsoft Internet Explorer, mediante el mismo tendremos acceso a la dirección propia de la cámara de red, que nos mostrará las imágenes de lo que en ese momento este sucediendo. Esto resulta extremadamente útil, ya que permitirá poder visualizar la cámara desde cualquier ordenador, en cualquier parte del mundo, sin necesidad de haber instalado un software específico.

No obstante, con las cámaras IP se adjunta un software de visualización de hasta 4 cámaras, permitiendo la visualización simultánea de las mismas, el control, la administración, y por supuesto la reproducción de los videos que se hayan grabado mediante grabación programada, o como consecuencia de alarmas.

Las cámaras IP y los servidores de vídeo solamente necesitan conectarse directamente a un PC mediante un cable de red cruzado cuando se instalan por primera vez. Una vez instalada, cualquier modificación de la configuración, de los ajustes de calidad de imagen, de las contraseñas de acceso, se realizará de forma remota desde cualquier punto del mundo, bastará con conectarse a la cámara en modo "Administrador".

2.2 Dispositivos de Red.

2.2.1 Switch Nexxt 8 puertos 10/100: Contiene 8 puertos 10/100 Fast Ethernet que están equipados con un sistema incorporado en la función de Auto-Negociación. Basta con conectar un dispositivo de red a cualquier puerto y que se ajusta automáticamente para funcionar a la mayor velocidad posible. Un Switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto (Untiveros, 2005).

Estos interruptores están diseñados para proporcionar gran cantidad de ancho de banda con un mínimo de molestias. Son 100% Plug & Play y no requiere configuración. Estos modelos cumplen totalmente con los estándares IEEE 802.3u y los estándares IEEE 802.3 Fast Ethernet y para las operaciones de Ethernet.

Especificaciones técnicas.

1. 8 puertos de 10/100Mbps TX Auto-Negociación.
2. Full / half-duplex en cada puerto TX.
3. Compatible con la interfaz TP Auto MDIX automático de TX / RX swap.
4. Fuente automática de direcciones MAC.
5. Compatible con las tiendas y en la arquitectura hacia delante y realiza el reenvío y filtrado.

6. El asalto a la función de filtro de difusión IEEE802.3x control de flujo para Full Dúplex.
7. Función de Back Pressure para Half-duplex.
8. Runt y filtrado CRC elimina paquetes erróneos para optimizar el ancho de banda
9. Apoyo para manejar hasta 1522 bytes de paquetes.
10. Rango de temperatura: 0 ° - 55 ° C.

2.2.2 Cable UTP categoría 5e: La categoría 5, es uno de los grados de cableado UTP descritos en el estándar EIA/TIA 568B el cual se utiliza para ejecutar CDDI y puede transmitir datos a velocidades de hasta 100 Mbps a frecuencias de hasta 100 MHz.

Está diseñado para señales de alta integridad. Estos cables pueden ser blindados o sin blindar. Este tipo de cables se utiliza a menudo en redes de ordenadores como Ethernet, y también se usa para llevar muchas otras señales como servicios básicos de telefonía Token Ring, y ATM (Groth, 2005).

Características:

1. 4 pares trenzados sección AWG24
2. Cada par de cable esta distinguido por colores, siendo estos naranja, verde, azul y marrón
3. Aislamiento del conductor de polietileno de alta densidad, de 1,5 mm de diámetro.
4. Cubierta de PVC gris
5. Disponible en cajas de 305 m

2.2.3 RJ-45 (registered Jack 45): Es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e, 6 y 6a). Es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho pines o conexiones

eléctricas, que normalmente se usan como extremos de cables de par trenzado. Es utilizada comúnmente con estándares como TIA/EIA-568-B (véase Figura 6), que define la disposición de los pines.

Una aplicación común es su uso en cables de red Ethernet, donde suelen usarse 8 pines (4 pares). Otras aplicaciones incluyen terminaciones de teléfonos (4 pines o 2 pares) por ejemplo en Francia y Alemania, otros servicios de red como RDSI y T1 e incluso RS-232.

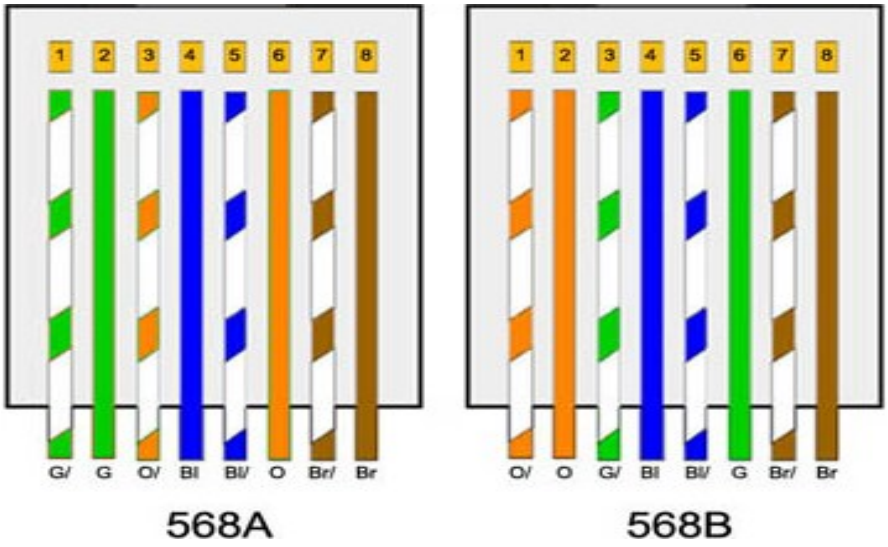


Figura 6. Estandares TIA/EIA.

2.2.4 IP pública: Las IP Públicas fijas actualmente en el mercado de acceso a Internet tienen un costo adicional mensual. Estas IP son asignadas por el usuario después de haber recibido la información del proveedor o bien asignadas por el proveedor en el momento de la primera conexión.

Esto permite al usuario montar servidores web, correo, FTP, etc. y dirigir un nombre de dominio a esta IP sin tener que mantener actualizado el servidor DNS cada vez que cambie la IP como ocurre con las IP Públicas dinámicas. En este proyecto se utilizó la dirección 200.62.73.203 como IP pública.

2.3 Dispositivos de monitoreo y vigilancia

2.3.1 Cámara web: Una cámara web (en inglés *webcam*) es una pequeña cámara digital conectada a una computadora, la cual puede capturar imágenes y transmitirlas a través de Internet, ya sea a una página web o a otra u otras computadoras de forma privada.

Las cámaras web necesitan una computadora para transmitir las imágenes. Sin embargo, existen otras cámaras autónomas que tan sólo necesitan un punto de acceso a la red informática, bien sea Ethernet o inalámbrico. Para diferenciarlas las cámaras web se las denomina cámaras de red.

Tecnología: Las cámaras web normalmente están formadas por una lente, un sensor de imagen y la circuitería necesaria para manejarlos.

Existen distintos tipos de lentes, siendo las lentes plásticas las más comunes. Los sensores de imagen pueden ser CCD (Charge Coupled Device) o CMOS (Complementary metal oxide semiconductor). Este último suele ser el habitual en cámaras de bajo coste, aunque eso no signifique necesariamente que cualquier cámara CCD sea mejor que cualquiera CMOS.

Las cámaras web para usuarios medios suelen ofrecer una resolución VGA (640x480) con una tasa de unos 30 fotogramas por segundo, si bien en la actualidad están ofreciendo resoluciones medias de 1 a 1,3 MP, actualmente las cámaras de gama alta cuentan con 3, 5, 8 y hasta 10 megapíxeles y son de alta definición.

La circuitería electrónica es la encargada de leer la imagen del sensor y transmitirla a la computadora. Algunas cámaras usan un sensor CMOS integrado con la circuitería en un único chip de silicio para ahorrar espacio y costos. El modo en que funciona el sensor es equivalente al de una cámara digital normal. También puede captar sonido, con una calidad mucho menor a la normal (Wawro, 2011).

2.3.2 Sensores CCD y CMOS: Hoy en día existen dos tipos de tecnologías utilizadas para la fabricación de sensores de cámaras digitales, ya sean compactas o réflex. Se trata de los CCD (Charge Coupled Device) o CMOS (Complementary Metal Oxide Semiconductor) figura 10. Ambos tipos de sensores están formados en su esencia por semiconductores de metal-óxido (MOS) y están distribuidos en forma de matriz.

Su función es la de acumular una carga eléctrica en cada una de las celdas de esta matriz. Estas celdas son los llamados píxeles. La carga eléctrica almacenada en cada píxel, dependerá en todo momento de la cantidad de luz que incida sobre el mismo, cuanta más luz incida sobre el píxel, mayor será la carga que este adquiera.

Aunque en su esencia, los CCD y CMOS funcionan de una manera muy similar, hay algunas diferencias que diferencian ambas tecnologías.

En el caso del CCD (véase Figura 7), éste convierte las cargas de las celdas de la matriz en voltajes y entrega una señal analógica en la salida, que será posteriormente digitalizada por la cámara. En los sensores CCD, se hace una lectura de cada uno de los valores correspondientes a cada una de las celdas. Entonces, es esta información la que un convertidor analógico-digital traduce en forma de datos.

En este caso, la estructura interna del sensor es muy simple, pero tenemos como inconveniente la necesidad de un chip adicional que se encargue del tratamiento de la información proporcionada por el sensor, lo que se traduce en un gasto mayor y equipos más grandes.

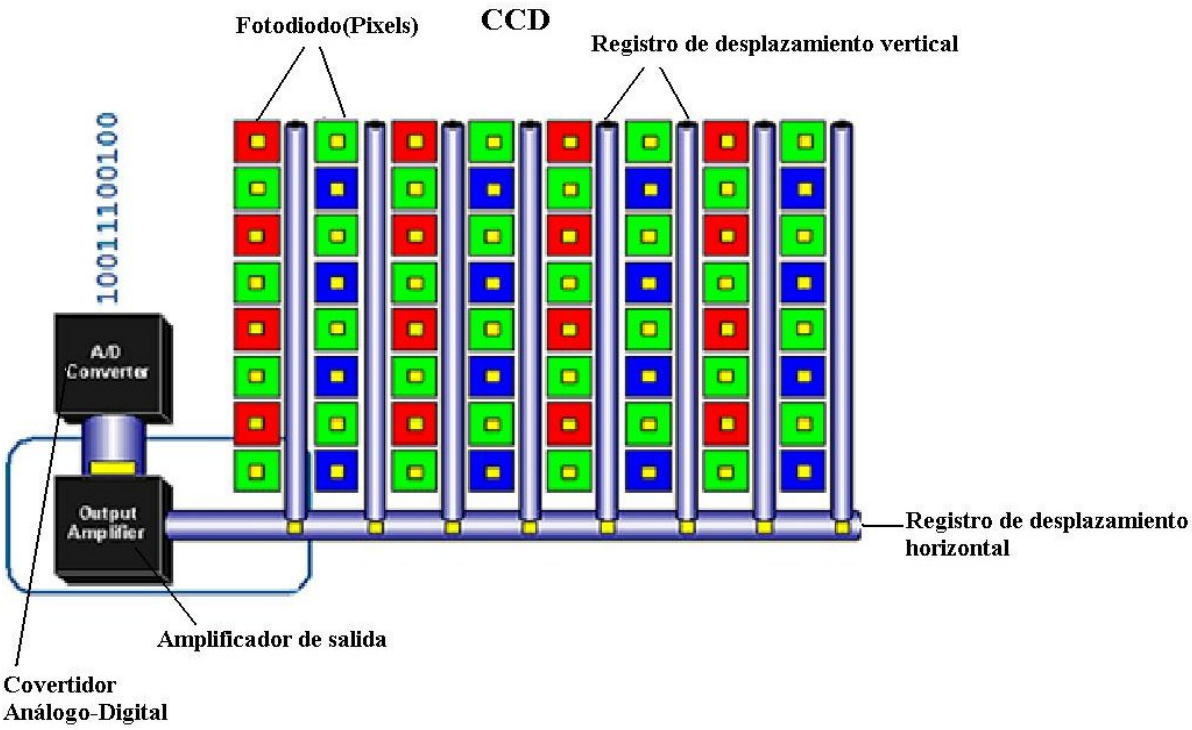


Figura 7. Sensor CCD

En el aspecto del rango dinámico, es el sensor CCD el ganador absoluto, pues supera al CMOS en un rango de dos. El rango dinámico es el coeficiente entre la saturación de los píxeles y el umbral por debajo del cual no captan señal. En este caso el CCD, al ser menos sensible, los extremos de luz los tolera mucho mejor.

En cuanto al ruido, también son superiores a los CMOS. Esto es debido a que el procesado de la señal se lleva a cabo en un chip externo, el cual puede optimizarse mejor para realizar esta función. En cambio, en el CMOS (véase la figura 8), al realizarse todo el proceso de la señal dentro del mismo sensor, los resultados serán peores, pues hay menos espacio para colocar los fotodiodos encargados de recoger la luz.

La respuesta uniforme es el resultado que se espera de un píxel sometido al mismo nivel de excitación que los demás, y que éste no presente cambios apreciables en la señal obtenida. En este aspecto, el que un sensor CMOS esté constituido por píxeles individuales, le hace más propenso a sufrir fallos. En el CCD, al ser toda la matriz

de píxeles uniforme, tiene un mejor comportamiento. A pesar de todo, la adición de circuitos con realimentación nos permite subsanar este problema en los CMOS, los CCD están un poquito por encima igualmente.

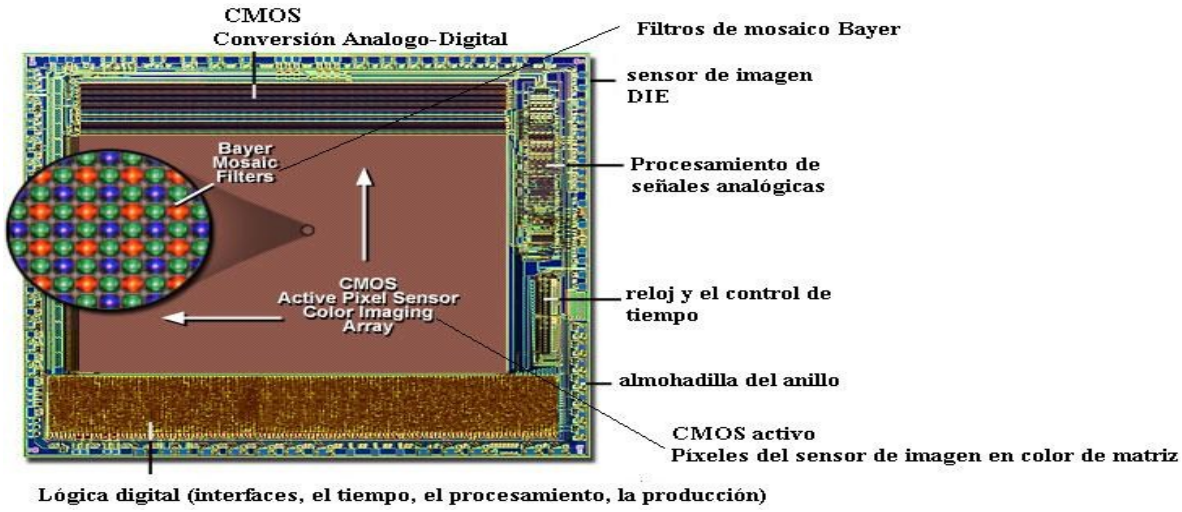


Figura 8. Sensor CMOS

En el caso del CMOS, aquí cada celda es independiente. La diferencia principal es que aquí la digitalización de los píxeles se realiza internamente en unos transistores que lleva cada celda, por lo que todo el trabajo se lleva a cabo dentro del sensor y no se hace necesario un chip externo encargado de esta función. Con esto se consigue reducir costes y equipos más pequeños.

Además de ofrecernos más calidad, los CMOS son más baratos de fabricar precisamente por lo que comentábamos arriba. Otra de las grandes ventajas es que los sensores CMOS son más sensibles a la luz, por lo que en condiciones pobres de iluminación se comportan mucho mejor. Esto se debe principalmente a que los amplificadores de señal se encuentran en la propia celda, por lo que hay un menor consumo a igualdad de alimentación. Todo lo contrario que ocurría en los CCD.

En cuanto a la velocidad, el CMOS es claramente superior al CCD debido a que todo el procesado se realiza dentro del propio sensor, ofreciendo mayor velocidad. Es esta una de las principales razones por las que empezaron a imponer los sensores

CMOS en sus cámaras y por la cual éstas permiten grabar vídeos a velocidades de hasta 1000 fps.

Otro aspecto en el que los sensores CMOS son superiores a los CCD es en el blooming. Este fenómeno se produce cuando un píxel se satura por la luz que incide sobre él y a continuación empieza a saturar a los que están a su alrededor. Aunque este defecto puede subsanarse gracias a algunos trucos en la construcción, en el caso de los CMOS nos olvidamos del problema.

2.3.3 ZoneMinder: Es un conjunto de aplicaciones que conjuntamente proporcionan una completa solución de video vigilancia permitiendo capturar, analizar, grabar y monitorizar cualquier cámara CCTV, Cámaras IP, Webcam, etc (véase Figura 9) conectada a una máquina basada en Linux. Está diseñado para ejecutarse en distribuciones de Linux que soporten la interfaz Video For Linux (V4L) y puede soportar múltiples cámaras sin pérdida aparente de rendimiento (Melin, 2009). ZoneMinder requiere MySQL y PHP y se apoya en un servidor web como Apache.

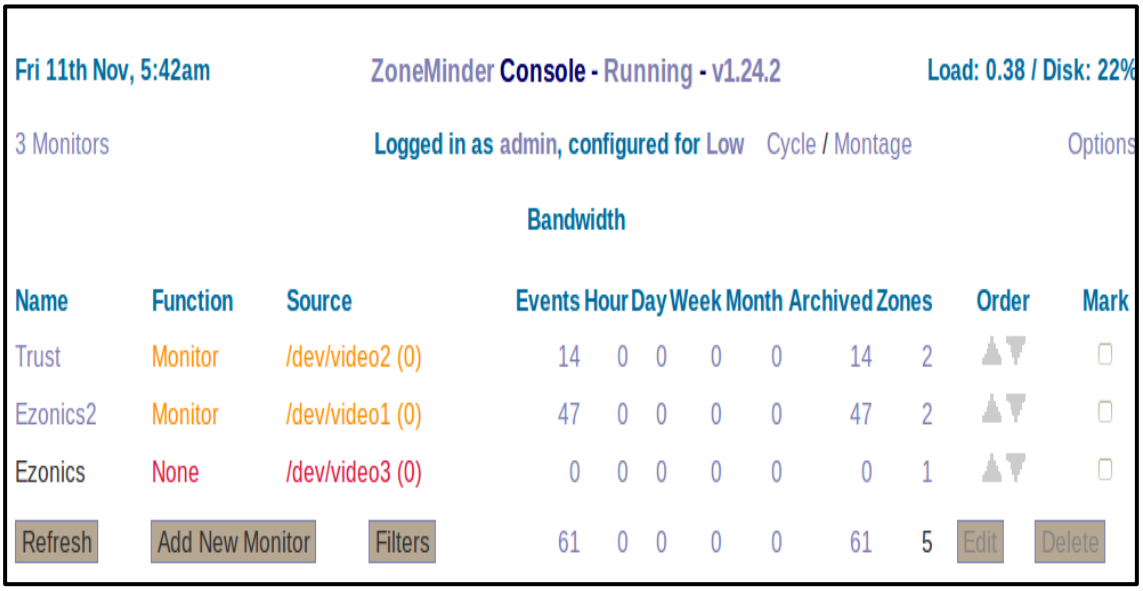


Figura 9. Interfaz Web del ZoneMinder

2.4 Sistemas Operativos Linux

2.4.1 SUSE Linux Enterprise Server (SLES): Es una distribución Linux proporcionada por SUSE y dirigido al mercado empresarial. Está dirigido a servidores, mainframes y estaciones de trabajo, pero se puede instalar en las computadoras de escritorio para las pruebas. Nuevas versiones son liberadas en un intervalo de 3-4 años, mientras que las versiones menores (llamados Service packs) son liberadas cada 6 meses.

La versión actual es SLES 11 SP1 (Figura 10), publicado 19 de mayo 2010, que se desarrolló a partir de una base de código común con SUSE Linux Enterprise Desktop y otros productos SUSE Linux Enterprise (Novell 1982).

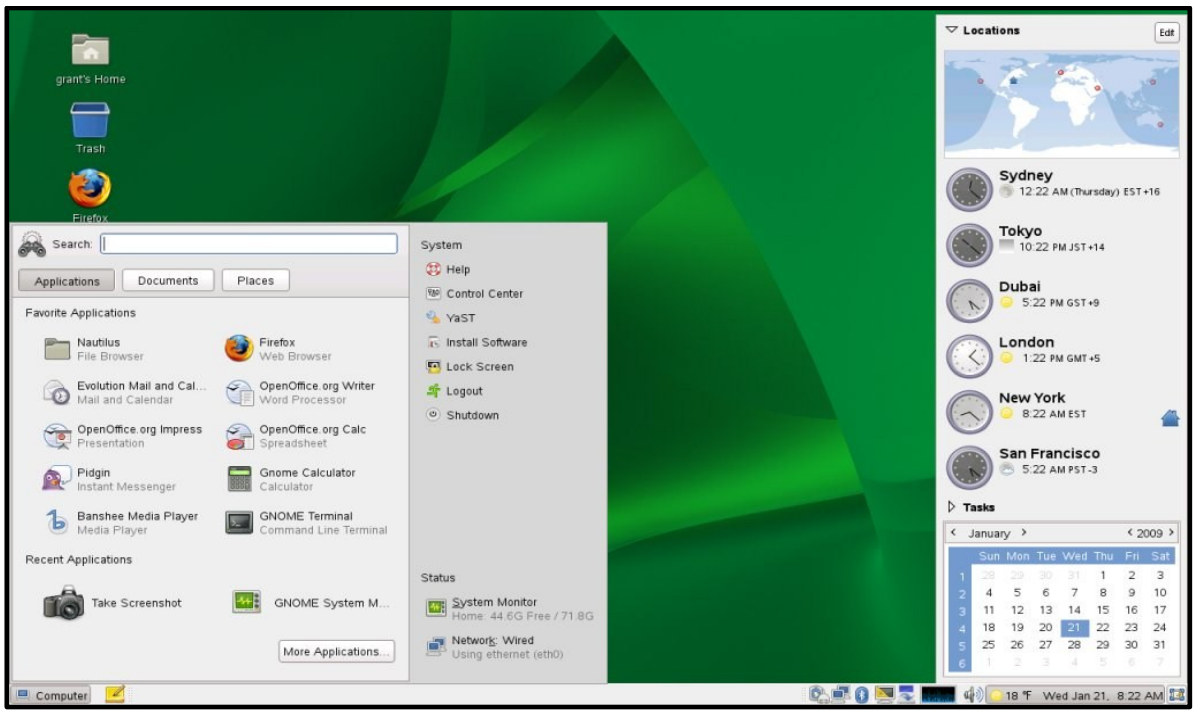


Figura 10. Interfaz de SLES 11.0 KDE

SLES es también una parte importante de Novell Open Enterprise Server, que ofrece todos los servicios de redes que antes sólo estaban disponibles en NetWare a la plataforma Linux.

Características:

- Fiabilidad, disponibilidad y capacidad de servicio
- Seguridad avanzada
- Virtualización multiplataforma
- Administración, desarrollo y gestión de sistemas simplificados
- Interoperabilidad con otras plataformas
- Informática de alto rendimiento
- Extensiones modulares con capacidades avanzadas.
- Asistencia técnica de prestigio en todo el mundo proporcionada por Novell.
- Características destacadas.

2.4.2 Ubuntu: Ubuntu es un sistema operativo mantenido por Canonical y la comunidad de desarrolladores. Utiliza un núcleo Linux, y su origen está basado en Debían. Ubuntu está orientado en el usuario promedio, con un fuerte enfoque en la facilidad de uso y mejorar la experiencia de usuario. Está compuesto de múltiple software normalmente distribuido bajo una licencia libre o de código abierto. Estadísticas web sugieren que el porcentaje de mercado de Ubuntu dentro de "distribuciones Linux" es de aproximadamente 49%, y con una tendencia a subir como servidor web. Posee una gran colección de aplicaciones para la configuración de todo el sistema, valiéndose principalmente de interfaces gráficas (Canonical 2010).

El entorno de escritorio predeterminado de Ubuntu es GNOME y se sincroniza con sus liberaciones. Existen otras dos versiones oficiales de la distribución, una con el entorno KDE, llamada Kubuntu, y otra con el entorno Xfce, llamada Xubuntu; existen otros escritorios disponibles, que pueden ser instalados en cualquier sistema Ubuntu independientemente del entorno de escritorio instalado por defecto.

Aplicaciones de Ubuntu: Ubuntu es conocido por su facilidad de uso y las aplicaciones orientadas al usuario final. Las principales aplicaciones que trae Ubuntu son: navegador web Mozilla Firefox, cliente de mensajería instantánea

Empathy, cliente de redes sociales Gwibber, cliente de correo Thunderbird, reproductor multimedia Totem, reproductor de música Banshee, gestor y editor de fotos Shotwell, cliente de torrents Transmisión, grabador de discos Brasero, suite ofimática Libre Office, y el instalador central para buscar e instalar aplicaciones Centro de software de Ubuntu.

Seguridad y accesibilidad: El sistema incluye funciones avanzadas de seguridad y entre sus políticas se encuentra el no activar, de forma predeterminada, procesos latentes al momento de instalarse. Por eso mismo, no hay un corta fuegos predeterminado, ya que no existen servicios que puedan atentar a la seguridad del sistema. Para labores o tareas administrativas en la línea de comandos incluye una herramienta llamada sudo (de las siglas en inglés de Súper User do), con la que se evita el uso del usuario administrador. Posee accesibilidad e internacionalización, de modo que el sistema esté disponible para tanta gente como sea posible. Desde la versión 5.04, se utiliza UTF-8 como codificación de caracteres predeterminado.

Interfaz: La actual interfaz de usuario de Ubuntu (véase figura 11), está compuesta por tres importantes elementos: un panel superior para indicadores de sistema y menús, un lanzador de aplicaciones al costado izquierdo, y un tablero que despliega lugares y aplicaciones. Ubuntu además de la interfaz Unity, utiliza las herramientas de GNOME que forman el resto del escritorio, el gestor de ventanas Compiz para las transiciones de efectos visuales, y varios elementos visuales diseñados por Canonical; tales como barras de desplazamiento Overlay Scrollbars, varios indicadores de sistema como el menú de sonido, el menú de mensajería, y el menú de estado de usuario, iconos Ubuntu Mono e Humanity, temas light-themes, las burbujas de notificación OSD, y los menús de aplicaciones globales.

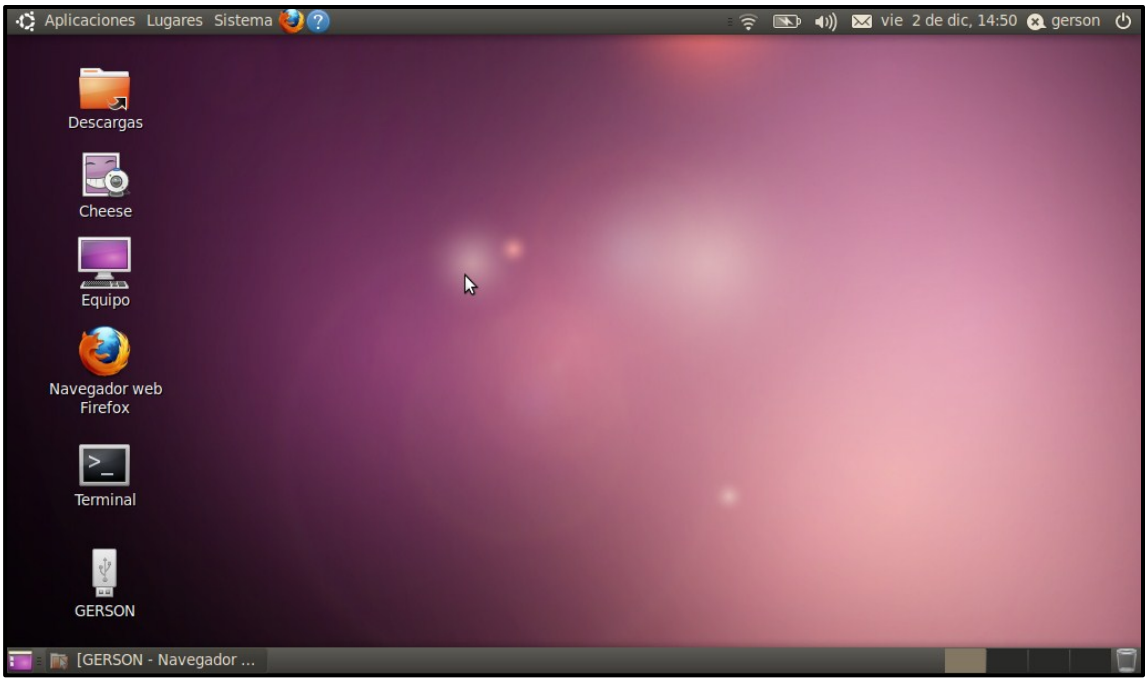


Figura 11. Interfaz de Ubuntu 10.04

2.5 Servicios y protocolos.

2.5.1 BIND (servidor DNS): (Berkeley Internet Name Domain, anteriormente: Berkeley Internet Name Daemon) es el servidor de DNS más comúnmente usado en Internet, especialmente en sistemas Unix, en los cuales es un estándar de facto. Es patrocinado por la Internet Systems Consortium. BIND fue creado originalmente por cuatro estudiantes de grado en la University of California, Berkeley y liberado por primera vez en el 4.3BSD. Paul Vixie comenzó a mantenerlo en 1988 mientras trabajaba para la DEC.

Una nueva versión de BIND (BIND 9) fue escrita desde cero en parte para superar las dificultades arquitectónicas presentes anteriormente para auditar el código en las primeras versiones de BIND, y también para incorporar DNSSEC (DNS Security Extensions). BIND 9 incluye entre otras características importantes: TSIG, notificación DNS, nsupdate, IPv6, rndc flush, vistas, procesamiento en paralelo, y

una arquitectura mejorada en cuanto a portabilidad. Es comúnmente usado en sistemas GNU/Linux (Ballester, 2003).

2.5.2 Servidor HTTP Apache: Es un servidor web HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.1y la noción de sitio virtual.

Apache es usado principalmente para enviar páginas web estáticas y dinámicas en la World Wide Web (www). Muchas aplicaciones web están diseñadas asumiendo como ambiente de implantación a Apache, o que utilizarán características propias de este servidor web.

Apache es el componente de servidor web en la popular plataforma de aplicaciones LAMP, junto a MySQL y los lenguajes de programación PHP/Perl/Python (y ahora también Ruby).

Apache es usado para muchas otras tareas donde el contenido necesita ser puesto a disposición en una forma segura y confiable. Un ejemplo es al momento de compartir archivos desde una computadora personal hacia Internet. Un usuario que tiene Apache instalado en su escritorio puede colocar arbitrariamente archivos en la raíz de documentos de Apache, desde donde pueden ser compartidos. Los programadores de aplicaciones web a veces utilizan una versión local de Apache con el fin de pre visualizar y probar código mientras éste es desarrollado.

2.5.3 Secure Shell: SSH (Secure Shell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo.

Además de la conexión a otros dispositivos, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH (Gómez, 2004).

Seguridad: SSH trabaja de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión; aunque es posible atacar este tipo de sistemas por medio de ataques de REPLAY y manipular así la información entre destinos.

2.5.4 NAT (Network Address Translation - Traducción de Dirección de Red): Es un mecanismo utilizado por enrutadores IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

Su uso más común es permitir utilizar direcciones privadas (definidas en el RFC 1918) para acceder a Internet. Existen rangos de direcciones privadas que pueden usarse libremente y en la cantidad que se quiera dentro de una red privada. Si el número de direcciones privadas es muy grande puede usarse solo una parte de direcciones públicas para salir a Internet desde la red privada. De esta manera simultáneamente sólo pueden salir a Internet con una dirección IP tantos equipos como direcciones públicas se hayan contratado. Esto es necesario debido al progresivo agotamiento de las direcciones IPv4. Se espera que con el advenimiento de IPv6 no sea necesario continuar con esta práctica.

Una pasarela NAT cambia la dirección origen en cada paquete de salida y, dependiendo del método, también el puerto origen para que sea único. Estas traducciones de dirección se almacenan en una tabla, para recordar qué dirección y puerto le corresponde a cada dispositivo cliente y así saber dónde deben regresar los paquetes de respuesta. Si un paquete que intenta ingresar a la red interna no existe en la tabla de en un determinado puerto y dirección se pueda acceder a un determinado dispositivo, como por ejemplo un servidor web, lo que se denomina NAT inverso o DNAT (Destinación NAT).

Tipos de NAT.

NAT estático: Consiste básicamente en un tipo de NAT en el cuál se mapea una dirección IP privada con una dirección IP pública de forma estática. De esta manera, cada equipo en la red privada debe tener su correspondiente IP pública asignada para poder acceder a Internet.

NAT dinámico Este tipo de NAT pretende mejorar varios aspectos del NAT estático dado que utiliza un pool de IPs públicas para un pool de IPs privadas que serán mapeadas de forma dinámica y a demanda.

NAT con sobrecarga: El caso de NAT con sobrecarga o PAT (Port Address Translation) es el más común de todos y el más usado en los hogares. Consiste en utilizar una única dirección IP pública para mapear múltiples direcciones IPs privadas. Las ventajas que brinda tienen dos enfoques: por un lado, el cliente necesita contratar una sola dirección IP pública para que las máquinas de su red tengan acceso a Internet, lo que supone un importante ahorro económico; por otro lado se ahorra un número importante de IPs públicas, lo que demora el agotamiento de las mismas (Di Tommaso, 2007).

2.5.5 Protocolo TCP

El fin de TCP es proveer un flujo de bytes confiable de extremo a extremo sobre una red de internet no confiable. TCP puede adaptarse dinámicamente a las propiedades del internet y manejar fallas de muchas clases. La entidad de transporte de TCP puede estar en un proceso de usuario o en el kernel. Parte un flujo de bytes en trozos y los mande como datagramas de IP.

Las conexiones de TCP son punto-a-punto y full dúplex. No preservan los límites de mensajes. Cuando una aplicación manda datos a TCP, TCP puede mandarlos inmediatamente o almacenarlos (para acumular más). Una aplicación puede solicitar que TCP manda los datos inmediatamente a través del flag de PUSH (empujar). TCP también apoya los datos urgentes. TCP manda datos con el flag URGENT inmediatamente. En el destino TCP interrumpe la aplicación (la manda una señal), que permite que la aplicación pueda encontrar los datos urgentes.

La cabecera TCP se muestra en la siguiente figura:

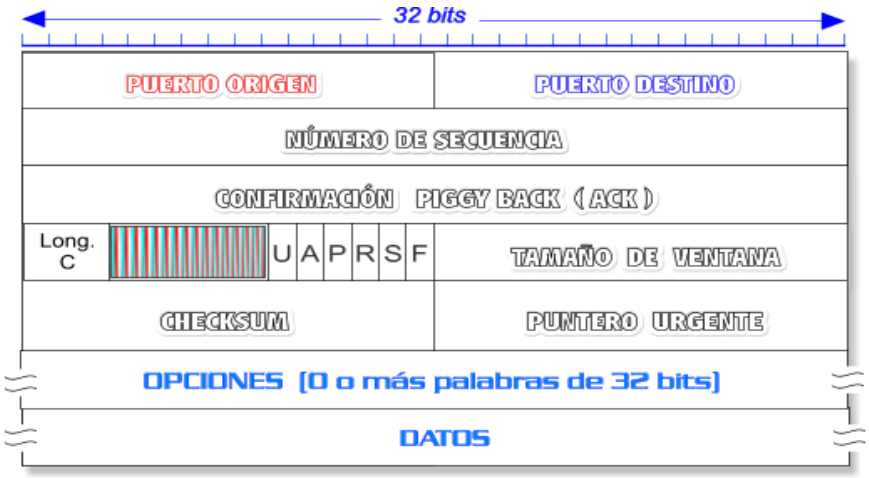


Figura 12. Cabecera TCP

2.5.6 IP (Internet Protocol) : Es un protocolo no orientado a conexión, usado tanto por el origen como por el destino para la comunicación de datos, a través de una red de paquetes conmutados no fiable y de mejor entrega posible sin garantías.

Los datos en una red basada en IP son enviados en bloques (véase figura 13) conocidos como paquetes o datagramas (en el protocolo IP estos términos se suelen usar indistintamente). En particular, en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

IP provee un servicio de datagramas no fiable (también llamado del mejor esfuerzo, lo hará lo mejor posible pero garantizando poco). IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad (mediante checksums o sumas de comprobación) de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP.

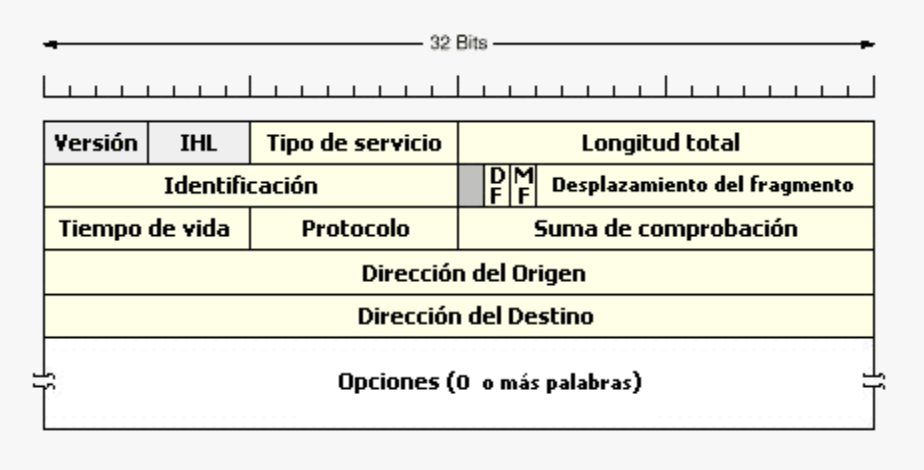


Figura 13. Cabecera IP

2.5.7 UDP (User Datagram Protocol): Es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 Modelo OSI). Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera (Poster, 1981). Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a

otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción.

Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

UDP sólo añade multiplexado de aplicación y suma de verificación de la cabecera (véase figura 14), y la carga útil. Cualquier tipo de garantías para la transmisión de la información deben ser implementadas en capas superiores.

La cabecera UDP consta de 4 campos de los cuales 2 son opcionales (con fondo rojo en la tabla). Los campos de los puertos fuente y destino son campos de 16 bits que identifican el proceso de origen y recepción. Ya que UDP carece de un servidor de estado y el origen UDP no solicita respuestas, el puerto origen es opcional. En caso de no ser utilizado, el puerto origen debe ser puesto a cero.

A los campos del puerto destino le sigue un campo obligatorio que indica el tamaño en bytes del datagrama UDP incluidos los datos. El valor mínimo es de 8 bytes. El campo de la cabecera restante es una suma de comprobación de 16 bits que abarca una cabecera IP (con las IP origen y destino, el protocolo y la longitud del paquete UDP), la cabecera UDP, los datos y 0's hasta completar un múltiplo de 16.

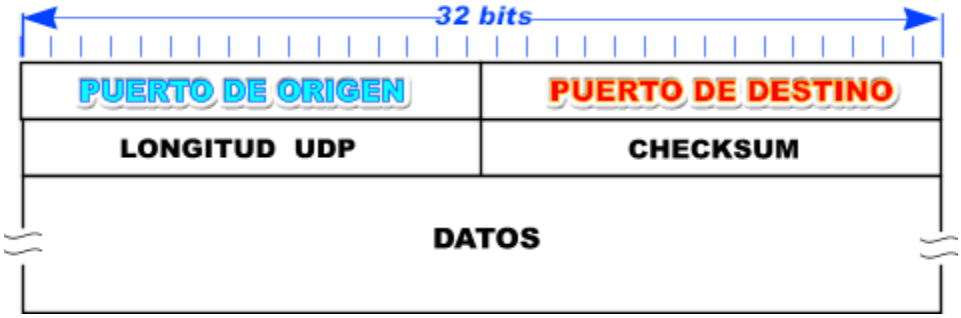


Figura 14. Cabecera UDP

2.5.8 Protocolo TCP/IP: Tiene la capacidad de generar varias conexiones simultáneas con un dispositivo remoto. Para realizar esto, dentro de la cabecera de un paquete IP, existen campos en los que se indica la dirección origen y destino. Esta combinación de números define una única conexión (Socolofsky, 1991).

El modelo TCP/IP es un modelo de descripción de protocolos de red creado en la década de 1970 por DARPA, una agencia del Departamento de Defensa de los Estados Unidos. Evolucionó de ARPANET. El modelo TCP/IP (ver figura 15), describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que una computadora pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando como los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario. Existen protocolos para los diferentes tipos de servicios de comunicación entre computadoras.

TCP/IP tiene cuatro capas de abstracción según se define en el RFC 1122. Esta arquitectura de capas a menudo es comparada con el Modelo OSI de siete capas. EL modelo TCP/IP y los protocolos relacionados son mantenidos por la Internet Engineering Task Force (IETF).

Para conseguir un intercambio fiable de datos entre dos computadoras, se deben llevar a cabo muchos procedimientos separados. El resultado es que el software de comunicaciones es complejo. Con un modelo en capas o niveles resulta más sencillo agrupar funciones relacionadas e implementar el software de comunicaciones modular.

Las capas están jerarquizadas. Cada capa se construye sobre su predecesora. El número de capas y, en cada una de ellas, sus servicios y funciones son variables con cada tipo de red. Sin embargo, en cualquier red, la misión de cada capa es proveer servicios a las capas superiores haciéndoles transparentes el modo en que esos servicios se llevan a cabo. De esta manera, cada capa debe ocuparse exclusivamente

de su nivel inmediatamente inferior, a quien solicita servicios, y del nivel inmediatamente superior, a quien devuelve resultados.

Figura 15

- **Capa 4** o **capa de aplicación**: Aplicación, asimilable a las capas 5 (sesión), 6 (presentación) y 7 (aplicación) del modelo OSI. La capa de aplicación debía incluir los detalles de las capas de sesión y presentación OSI. Crearon una capa de aplicación que maneja aspectos de representación, codificación y control de diálogo.

- **Capa 3** o **capa de transporte**: Transporte, asimilable a la capa 4 (transporte) del modelo OSI.

- **Capa 2** o **capa de red**: Internet, asimilable a la capa 3 (red) del modelo OSI.

- **Capa 1** o **capa de enlace**: Acceso al Medio, asimilable a la capa 1 (física) y 2 (enlace de datos) del modelo OSI.

2.6 Gestor de contenidos y lenguajes de programación.

2.6.1 Joomla 1.5: Es un sistema de gestión de contenidos y un framework para aplicaciones web que también puede ser utilizado independientemente. Entre sus principales virtudes está la de permitir editar el contenido de un sitio web de manera sencilla (véase Figura 16). Es una aplicación de código abierto programada mayoritariamente en PHP bajo una licencia GPL (Miro, 2005).

Este administrador de contenidos puede trabajar en Internet o intranets y requiere de una base de datos MySQL, así como, preferiblemente, de un servidor HTTP Apache. En Joomla se incluyen características como: mejorar el rendimiento web, versiones imprimibles de páginas, flash con noticias, blogs, foros, polls (encuestas), calendarios, búsqueda en el sitio web e internacionalización del lenguaje.

Figura 16. Panel de control de Joomla

Extensiones: Una de las mayores potencialidades que tiene este CMS es la gran cantidad de extensiones existentes programadas por su comunidad de usuarios que aumentan las posibilidades de Joomla! con nuevas características y que se integran fácilmente en él.

Existen cientos de extensiones disponibles y con diversas funcionalidades como por Ejemplo:

- Generadores de formularios dinámicos
- Directorios de empresas u organizaciones
- Gestores de documentos
- Galerías de imágenes multimedia
- Motores de comercio y venta electrónica
- Software de foros y chats
- Calendarios
- Software para blogs
- Servicios de directorio
- Boletines de noticias
- Herramientas de registro de datos
- Sistemas de publicación de anuncios
- Servicios de suscripción

A su vez estas extensiones se agrupan en:

- Componentes
- Módulos
- Plantillas
- Plugins

2.6.2 Firebug: Es una extensión de Firefox creada y diseñada especialmente para desarrolladores y programadores web. Es un paquete de utilidades con el que se puede analizar (revisar velocidad de carga, estructura DOM), editar, monitorizar y depurar el código fuente, CSS, HTML y JavaScript de una página web de manera instantánea u online.

Firebug no es un simple inspector como DOM Inspector, además edita y permite guardar los cambios, un paso por delante del conocido Web Developer. Su atractiva e intuitiva interfaz, con solapas específicas para el análisis de cada tipo de elemento (consola, HTML, CSS, Script, DOM y red), permite al usuario un manejo fácil y rápido. Firebug está encapsulado en forma de plug-in o complemento de Mozilla, es Open Source, libre y de distribución gratuita.

2.6.3 Adobe Dreamweaver: Es una aplicación en forma de estudio (basada en la forma de estudio de Adobe Flash) que está destinada a la construcción y edición de sitios y aplicaciones Web basados en estándares. Creado inicialmente por Macromedia (actualmente producido por Adobe Systems) es el programa de este tipo más utilizado en el sector del diseño y la programación web (ver figura 17), por sus funcionalidades, su integración con otras herramientas como Adobe Flash y, recientemente, por su soporte de los estándares del World Wide Web Consortium.

Su principal competidor es Microsoft Expression Web y tiene soporte tanto para edición de imágenes como para animación a través de su integración con otras. Hasta la versión MX, fue duramente criticado por su escaso soporte de los estándares de la web, ya que el código que generaba era con frecuencia sólo válido para Internet Explorer, y no validaba como HTML estándar. Esto se ha ido corrigiendo en las versiones recientes.

La gran ventaja de este editor sobre otros es su gran poder de ampliación y personalización del mismo, puesto que en este programa, sus rutinas (como la de insertar un hipervínculo, una imagen o añadir un comportamiento) están hechas en Javascript-C, lo que le ofrece una gran flexibilidad en estas materias. Esto hace que los archivos del programa no sean instrucciones de C++ sino, rutinas de Javascript que hace que sea un programa muy fluido, que todo ello hace, que programadores y editores web hagan extensiones para su programa y lo ponga a su gusto.

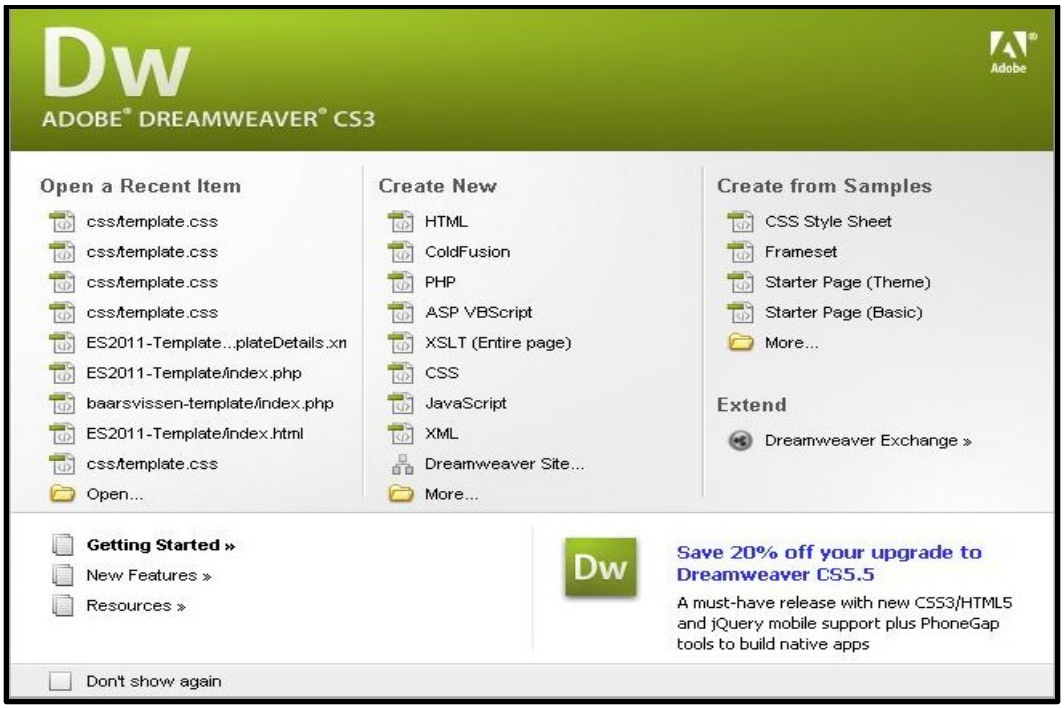


Figura 17. Interfaz de Adobe Dreamweaver.

2.6.4 CSS: El nombre hojas de estilo en cascada viene del inglés Cascading Style Sheets, del que toma sus siglas. CSS es un lenguaje usado para definir la presentación de un documento estructurado escrito en HTML o XML (y por extensión en XHTML). El W3C (World Wide Web Consortium) es el encargado de formular la especificación de las hojas de estilo que servirán de estándar para los agentes de usuario o navegadores.

La idea que se encuentra detrás del desarrollo de CSS es separar la estructura de un documento de su presentación.

Los tres tipos de estilos son:

CSS proporciona tres caminos diferentes para aplicar las reglas de estilo a una página Web:

- **Una hoja de estilo externa**, es una hoja de estilo que está almacenada en un

archivo diferente al archivo donde se almacena el código HTML de la página Web. Esta es la manera de programar más potente, porque separa completamente las reglas de formateo para la página HTML de la estructura básica de la página.

- **Una hoja de estilo interna**, que es una hoja de estilo que está incrustada dentro de un documento HTML. (Va a la derecha dentro del elemento <head>.) De esta manera se obtiene el beneficio de separar la información del estilo del código HTML propiamente dicho. Se puede optar por copiar la hoja de estilo incrustada de una página a otra (esta posibilidad es difícil de ejecutar si se desea para guardar las copias sincronizadas). En general, la única vez que se usa una hoja de estilo interna, es cuando se quiere proporcionar alguna característica a una página Web en un simple fichero, por ejemplo, si se está enviando algo a la página Web.

- **Un estilo en línea** (inline) es un método para insertar el lenguaje de estilo de página directamente dentro de una etiqueta HTML. Esta manera de proceder no es totalmente adecuada. El incrustar la descripción del formateo dentro del documento de la página Web, a nivel de código, se convierte en una manera larga, tediosa y poco elegante de resolver el problema de la programación de la página. Este modo de trabajo se podría usar de manera ocasional si se pretende aplicar un formateo con prisa, al vuelo. No es todo lo claro o estructurado que debería ser, pero funciona. Éste es el método recomendado para maquetar correos electrónicos en HTML.

Las ventajas de utilizar CSS (u otro lenguaje de estilo) son:

- Control centralizado de la presentación de un sitio web completo con lo que se agiliza de forma considerable la actualización del mismo.

- Los navegadores permiten a los usuarios especificar su propia hoja de estilo local, que será aplicada a un sitio web, con lo que aumenta considerablemente la

accesibilidad. Por ejemplo, personas con deficiencias visuales pueden configurar su propia hoja de estilo para aumentar el tamaño del texto o remarcar más los enlaces.

- Una página puede disponer de diferentes hojas de estilo según el dispositivo que la muestre o, incluso, a elección del usuario. Por ejemplo, para ser impresa, mostrada en un dispositivo móvil o ser "leída" por un sintetizador de voz.

- El documento HTML en sí mismo es más claro de entender y se consigue reducir considerablemente su tamaño (siempre y cuando no se utilice estilo en línea).

2.6.5 Página Web: Una página web es un documento o información electrónica adaptada para la World Wide Web y que puede ser accedida mediante un navegador para mostrarse en un monitor de computadora o dispositivo móvil. Esta información se encuentra generalmente en formato HTML o XHTML, y puede proporcionar navegación a otras páginas web mediante enlaces de hipertexto. Las páginas web frecuentemente incluyen otros recursos como hojas de estilo en cascada, guiones (scripts) e imágenes digitales, entre otros.

Las páginas web (véase figura 18), pueden estar almacenadas en un equipo local o un servidor web remoto. El servidor web puede restringir el acceso únicamente para redes privadas, ejemplo: En una intranet corporativa, o puede publicar las páginas en la World Wide Web. El acceso a las páginas web es realizado mediante su transferencia desde servidores.

Una página web está compuesta principalmente por información (sólo texto o módulos multimedia) así como por hiperenlaces; además puede contener o asociar datos de estilo para especificar cómo debe visualizarse, y también aplicaciones embebidas para así hacerla interactiva. Las páginas web son escritas en un lenguaje

de marcado que provee la capacidad de manejar e insertar hiperenlaces, generalmente HTML.

El contenido de la página puede ser predeterminado («página web estática») o generado al momento de visualizarla o solicitarla a un servidor web («página web dinámica»). Las páginas dinámicas que se generan al momento de la visualización, se especifican a través de algún lenguaje interpretado, generalmente JavaScript, y la aplicación encargada de visualizar el contenido es la que realmente debe generarlo. Las páginas dinámicas que se generan, al ser solicitadas, son creadas por una aplicación en el servidor web que alberga las mismas.

Figura 18 Página Web Electronicsecurity

2.6.6 HTML: Siglas de HyperText Markup Language («lenguaje de marcado de hipertexto»), es el lenguaje de marcado predominante para la elaboración de páginas web. Es usado para describir la estructura y el contenido en forma de texto, así como

para complementar el texto con objetos tales como imágenes. HTML se escribe en forma de «etiquetas», rodeadas por corchetes angulares (<,>). HTML también puede describir, hasta un cierto punto, la apariencia de un documento, y puede incluir un script (por ejemplo JavaScript), el cual puede afectar el comportamiento de navegadores web y otros procesadores de HTML.

HTML también es usado para referirse al contenido del tipo de MIME text/html o todavía más ampliamente como un término genérico para el HTML, ya sea en forma descendida del XML (como XHTML 1.0 y posteriores) o en forma descendida directamente de SGML (como HTML 4.01 y anteriores).

2.6.7 XML: Siglas en inglés de extensible Markup Language ('lenguaje de marcas extensible'), es un metalenguaje extensible de etiquetas desarrollado por el World Wide Web Consortium (W3C). Es una simplificación y adaptación del SGML y permite definir la gramática de lenguajes específicos (de la misma manera que HTML es a su vez un lenguaje definido por SGML).

Por lo tanto XML no es realmente un lenguaje en particular, sino una manera de definir lenguajes para diferentes necesidades. Algunos de estos lenguajes que usan XML para su definición son XHTML, SVG, MathML, Android.

XML no ha nacido sólo para su aplicación en Internet, sino que se propone como un estándar para el intercambio de información estructurada entre diferentes plataformas. Se puede usar en bases de datos, editores de texto, hojas de cálculo y casi cualquier cosa imaginable.

XML es una tecnología sencilla que tiene a su alrededor otras que la complementan y la hacen mucho más grande y con unas posibilidades mucho mayores. Tiene un papel muy importante en la actualidad ya que permite la compatibilidad entre sistemas para compartir la información de una manera segura, fiable y fácil.

2.6.8 PHP: Es un lenguaje de programación interpretado, diseñado originalmente para la creación de páginas web dinámicas. Se usa principalmente para la interpretación del lado del servidor (server-side scripting) pero actualmente puede ser utilizado desde una interfaz de línea de comandos o en la creación de otros tipos de programas incluyendo aplicaciones con interfaz gráfica usando las bibliotecas Qt o GTK+.

Características:

- Es un lenguaje multiplataforma.
- Orientado al desarrollo de aplicaciones web dinámicas con acceso a información almacenada en una base de datos.
- El código fuente escrito en PHP es invisible al navegador web y al cliente ya que es el servidor el que se encarga de ejecutar el código y enviar su resultado HTML al navegador.
- Esto hace que la programación en PHP sea segura y confiable.
- Capacidad de conexión con la mayoría de los motores de base de datos que se utilizan en la actualidad, destaca su conectividad con MySQL y PostgreSQL.
- Capacidad de expandir su potencial utilizando módulos (llamados ext's o extensiones).
- Posee una amplia documentación en su sitio web oficial, entre la cual se destaca que todas las funciones del sistema están explicadas y ejemplificadas en un único archivo de ayuda.
- Es libre, por lo que se presenta como una alternativa de fácil acceso para todos.
- Permite aplicar técnicas de programación orientada a objetos.
- Biblioteca nativa de funciones sumamente amplia e incluida.
- No requiere definición de tipos de variables aunque sus variables se pueden evaluar también por el tipo que estén manejando en tiempo de ejecución.
- Tiene manejo de excepciones (desde PHP5).

Si bien PHP no obliga a quien lo usa a seguir una determinada metodología a la hora de programar (muchos otros lenguajes tampoco lo hacen), aun haciéndolo, el programador puede aplicar en su trabajo cualquier técnica de programación o de desarrollo que le permita escribir código ordenado, estructurado y manejable. Un ejemplo de esto son los desarrollos que en PHP se han hecho del patrón de diseño Modelo Vista Controlador (MVC), que permiten separar el tratamiento y acceso a los datos, la lógica de control y la interfaz de usuario en tres componentes independientes.

Inconvenientes

Como es un lenguaje que se interpreta en ejecución, para ciertos usos puede resultar un inconveniente que el código fuente no pueda ser ocultado. La ofuscación es una técnica que puede dificultar la lectura del código pero no la impide y, en ciertos casos, representa un costo en tiempos de ejecución.

2.6.9 MySQL: Es un sistema de gestión de bases de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones. MySQL AB desde enero de 2008 una subsidiaria de Sun Microsystems y ésta a su vez de Oracle Corporation desde abril de 2009 desarrolla MySQL como software libre en un esquema de licenciamiento dual.

Por un lado se ofrece bajo la GNU GPL para cualquier uso compatible con esta licencia, pero para aquellas empresas que quieran incorporarlo en productos privativos deben comprar a la empresa una licencia específica que les permita este uso. Está desarrollado en su mayor parte en ANSI C.

Al contrario de proyectos como Apache, donde el software es desarrollado por una comunidad pública y los derechos de autor del código están en poder del autor individual, MySQL es patrocinado por una empresa privada, que posee el copyright de la mayor parte del código (Flores, 2006).

MySQL es muy utilizado en aplicaciones web, como Drupal o phpBB, en plataformas (Linux/Windows-Apache-MySQL-PHP/Perl/Python), y por herramientas de seguimiento de errores como Bugzilla. Su popularidad como aplicación web está muy ligada a PHP, que a menudo aparece en combinación con MySQL. MySQL es una base de datos muy rápida en la lectura cuando utiliza el motor no transaccional MyISAM, pero puede provocar problemas de integridad en entornos de alta concurrencia en la modificación.

En aplicaciones web hay baja concurrencia en la modificación de datos y en cambio el entorno es intensivo en lectura de datos, lo que hace a MySQL ideal para este tipo de aplicaciones. Sea cual sea el entorno en el que va a utilizar MySQL, es importante monitorizar de antemano el rendimiento para detectar y corregir errores tanto de SQL como de programación.

Capítulo III

DESARROLLO

Este proyecto de seminario de graduación fue desarrollado en una casa residencial del departamento de Managua, ubicada en el Bo. Venezuela, donde se implementó un sistema de vigilancia y seguridad con cámaras Web e IP a través de un servidor Web SLES, la elección de este local fue debido a que el dueño de la vivienda tenía interés de implementar un sistema de vigilancia que le permitiera el monitoreo y la supervisión de sus bienes y además que contaba con una dirección IP publica, la cual facilito el desarrollo e implementación de este proyecto. En el siguiente diagrama se muestra la estructura del desarrollo.

Configuraciones que se realizaran en el Sistema de Vigilancia y Seguridad.

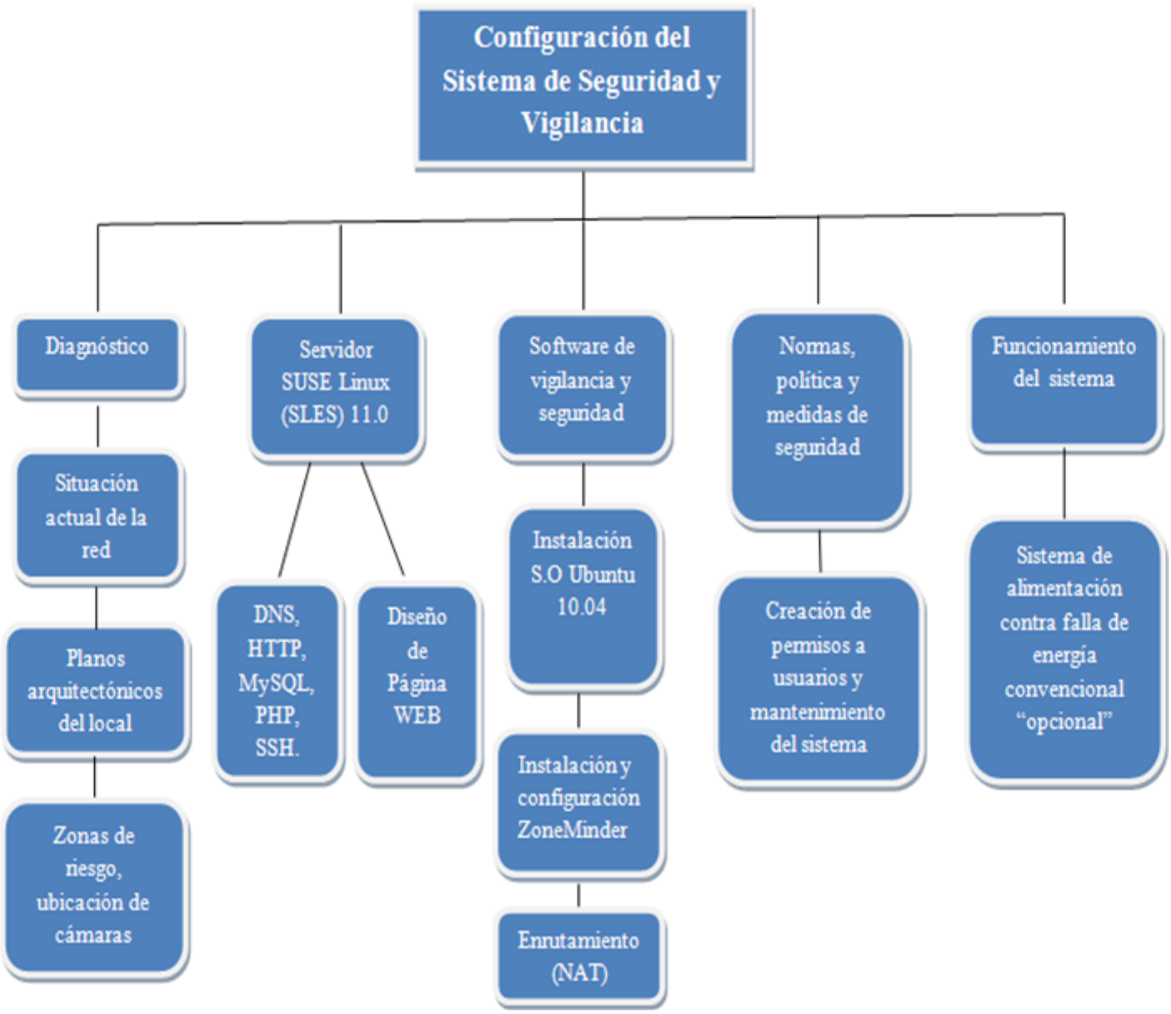


Figura 19. Estructura del desarrollo del sistema.

3.1 Diagnostico

La red doméstica del domicilio está compuesta por un Router Thomson TG585 v7 el cual fue asignado por el ISP Turbonett con un ancho de banda de 256 Kbits y un servicio de IP publica 200.62.73.203, las características del Router son las siguientes:

- Alimentación de 110 VCA a 6 VDC.
- Wireless Multi-User ADSL2 + Gateway
- Acceso inalámbrico con un alcance de más de 120 metros con su antena externa.
- Cuenta con modem ADSL. Compatible con cualquier dispositivo WiFi.

Interfaces:

LAN:

- 802.11g 54Mb/s Wi-Fi CERTIRED gateway.
- 4 puertos Ethernet.

WAN:

- ADSL, ADSL2, ADSL2 + (POTS/ISDN)

Gestión:

- Configurable por navegador web vía HTTP(s). Asistente de configuración Easy Setup.
- **Seguridad:**
  Servidor de seguridad integrado. WEP, WPA y WPA2 seguridad de red inalámbrico.

En la red doméstica están conectados una computadora personal y un servidor de Testing el cual es un servicio brindado por la empresa SIGOS de origen Alemán en el cual realizan pruebas de rendimiento de las redes en Nicaragua, todos esto conectados a la red doméstica a través de cable UTP (Directo) categoría 5e, utilizando la norma 568B.

3.1.1 Estructura anterior de la Red.

La red doméstica está estructurada según la siguiente figura:

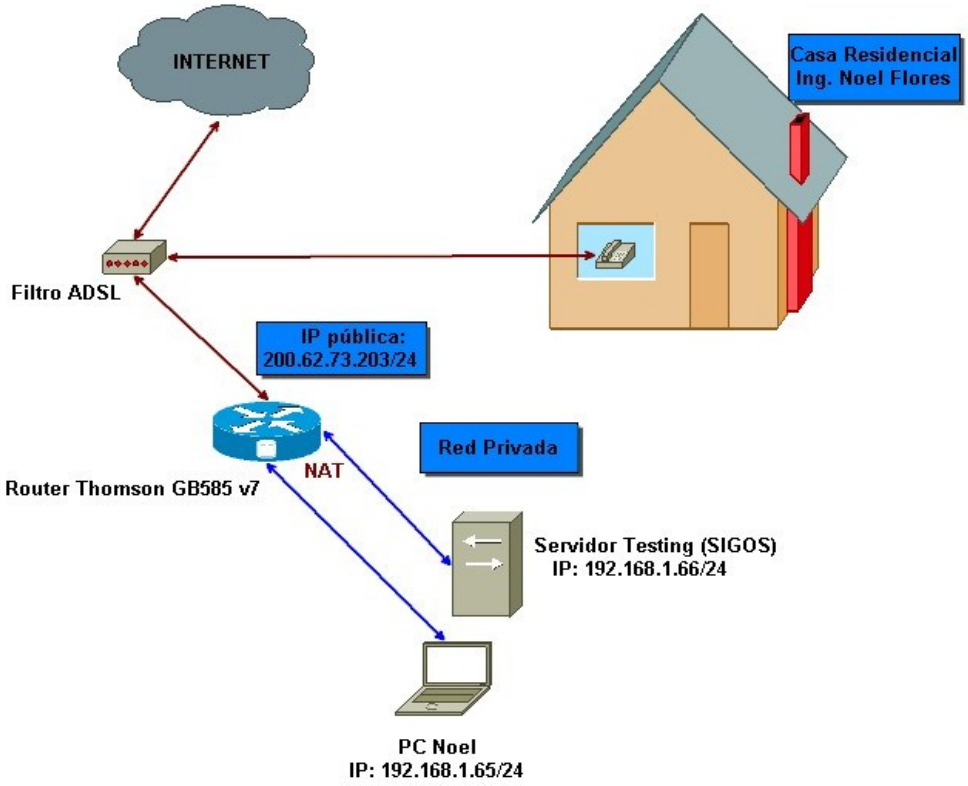


Figura 20. Red local anterior al sistema de vigilancia.

Los cambios que se realizaran en la red son los siguientes:

- Switch Nexxt de 8 puertos fastethernet.
- PC de escritorio CLON con sistema operativo SLES (servidor).
- Notebook Toshiba N505 con sistema operático Ubuntu.
- 1 Cámara IP tipo Panasonic BLC 1A.
- 2 Webcam marca Ezonics 307.
- 2 Webcam Klip Extreme 300.

Una vez integrados estos dispositivos en el sistema, la red quedó estructurada de la siguiente manera:

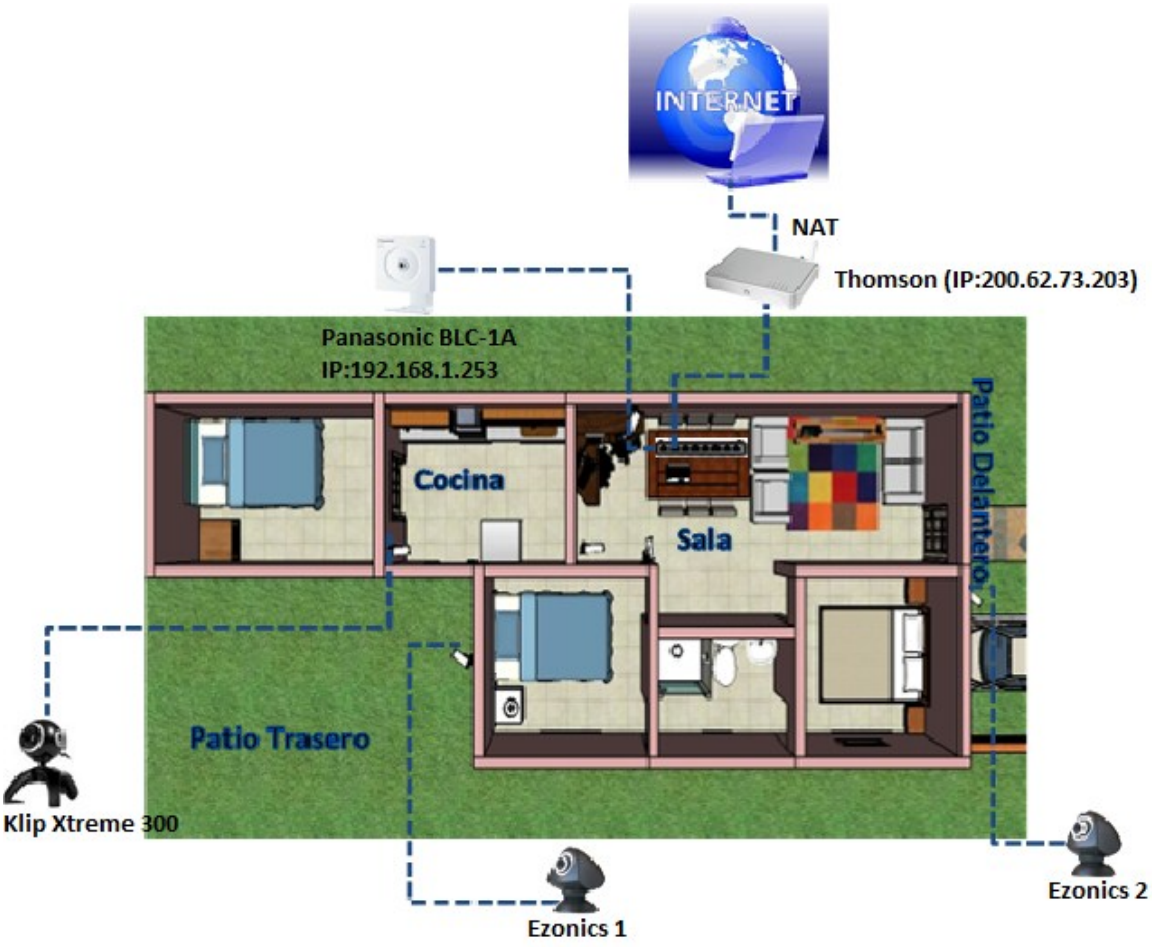


Figura 21. Red actual del local

3.1.2 Planos arquitectónicos del local: A continuación se muestran los planos del domicilio (véase Figura 22) en donde estará instalado todo el sistema de vigilancia y seguridad. Este es una casa Particular ubicada en Bo. Venezuela, con dirección Clínica Don Bosco 5 c al Este, 2 c al Sur y ½ al Este. El propietario del local es el Ing. Noel Flores

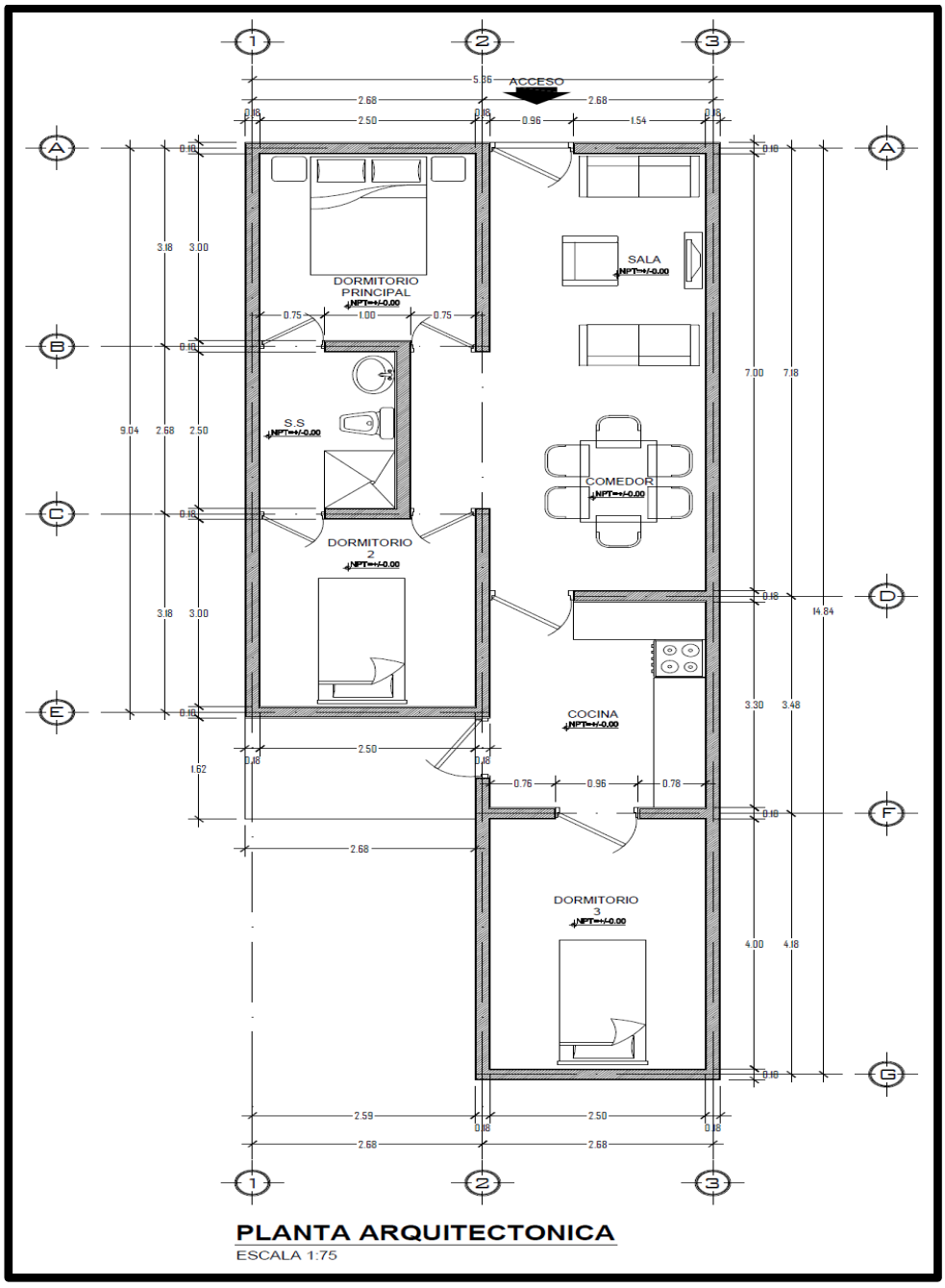


Figura 22. Plano arquitectónico a escala del domicilio.

3.1.3 Zonas de riesgo y ubicación de las cámaras.

La ubicación de las cámaras estará de acuerdo a la necesidad de cubrir aquellas áreas donde existen objetos de valor que pueden ser objetivo de robo y espacios abiertos

vulnerable a la incursión de personas no deseadas o ajenas al círculo de los habitantes del domicilio.

Parámetros de ubicación.

Las cámaras de seguridad se deben colocar en soportes estables para minimizar el efecto de distorsión debido al movimiento. Las cámaras exteriores deben fijarse a una altura de al menos 3,5 m para dificultar su acceso pero permitiendo no distorsionar la imagen y acceder a su mantenimiento. Conviene protegerlas con una "jaula" metálica, en el caso de las cámaras en interiores utilizando los parámetros de ubicación se recomienda ubicarlas a una distancia mínima de 2 m.

El campo de visión es la medida de cuán grande es el área que una cámara es capaz de observar el FOV está basado en la cámara y el lente. En aplicaciones donde una visualización más cercana es necesaria una lente de 8mm o 12 mm resulta una mejor opción.

Al incrementar la distancia focal de la lente disminuye la distancia percibida al área visualizada pero también disminuye el área que la cámara es capaz de observar. El FOV puede ser calculado de la siguiente manera:

$$\frac{h}{H} = \frac{f}{L}$$

h= Peso del formato: Formato de ½ es igual a 6.4 mm, formato de 1/3 es igual a 3.6 mm y el formato de ¼ igual a 2.7 mm.

H= Altura de objeto.

f= Distancia focal.

L= Distancia al objeto.

Para la ubicación de la cámara IP se ubicó tratando de lograr la captura de una persona de cuerpo completo, con un reconocimiento del rostro. Tomando una altura promedio de 1.8 m.

h= 1/4 =2.7 mm $\quad$ $\mathbf{H} = \frac{h}{f} * L$

L= 6 m= 6000 mm $\quad$ **H**= 2025 mm= 2.025 m

f= 8 mm

Según los resultados obtenidos anteriormente se necesitan una cámara con una distancia focal (f) de 8 mm, la cual es una característica de la BLC-C1A Panasonic, el ángulo de captura para este tipo de lente con respecto a su distancia focal es el siguiente:

- Angulo Horizontal: 53 grados.
- Angulo vertical: 41 grados.

Zonas de riesgo

1. Sala: En esta zona se encuentran una serie de artículos de gran valor (TV LCD, Muebles, Minicomponente, Computadoras, etc, además de la vista al acceso principal de la vivienda y acceso a dormitorios.

Figura 23. Vista 3D de la sala del domicilio.

2. Patio delantero: Esta es la zona de mayor riesgo ya que colinda con la calle principal, además existen antecedentes delincuenciales previos, donde delincuentes han penetrado desde este acceso a la vivienda.

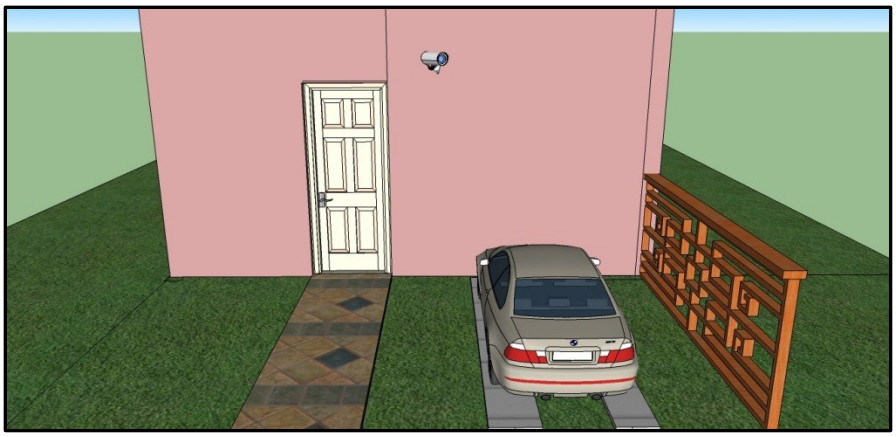


Figura 24. Vista 3D del patio delantero.

3. Patio trasero: Esta mantiene el mismo nivel de riesgo que la anterior, ya que es la zona donde existe menos concurrencia de los habitantes del domicilio.

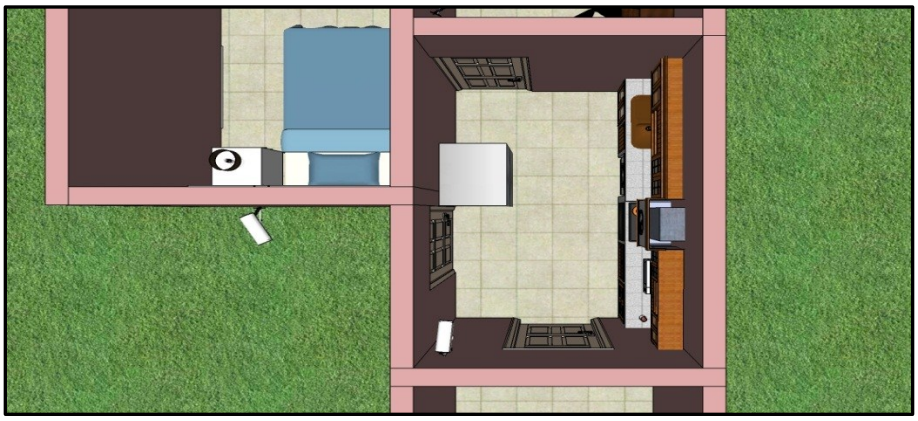


Figura 25. Vista 3D del patio trasero.

4. Cocina: Esto debido a que se puede acceder a la misma a través del patio trasero, su riesgo será menor ya que existirá una cámara previa, que cubrirá este acceso desde el patio. Sin embargo en esta zona se encuentra artículos de gran valor (Cocina, Lavadora, Refrigeradora, etc).

Figura 26. Vista 3D de la cocina

5. Servidor Testing: Dado su gran valor económico, se decidió implementar una medida de seguridad adicional a través de webcam que cubrirá únicamente la zona donde se ubica este equipo.

Figura 27. Vista 3D de la sala desde otro ángulo

6. Servidor SLES y Ubuntu: Para la protección del equipo de seguridad y el acceso de usuarios no autorizados, se implementará el uso de otra Webcam que cubrirá el sitio específico donde se encuentran los equipos. El equipo está ubicado en la sala de la vivienda, debido a que este es un punto estratégico con respecto al ahorro de cableado y conectores de alimentación AC.

A continuación les mostramos una vista panorámica de todo el domicilio de donde se observa todo el sistema de vigilancia y seguridad.

Figura 28. Vista 3D de todo el local

3.2 Servidor SUSE Linux (SLES) 11.0

La instalación del sistema operativo se hizo de forma típica, siguiendo paso a paso el asistente de instalación, se instalaron los servicios que necesarios para el buen funcionamiento del sistema. A continuación se muestran las características mínimas necesarias para instalar SLES 11.0 64 bits según el manual de usuario disponible en Novell, Inc.

- Procesador Pentium* III a 500 MHz o superior (se recomienda Pentium 4 a 2,4 GHz o superior o cualquier procesador AMD64 o Intel* EM64T).
- 512 MB de RAM física (se recomienda 1 GB).
- 2 GB de espacio disponible en disco (se recomienda una cantidad superior).
- Resolución de pantalla de 800 x 600 (se recomienda 1.024 x 768 o superior).

En este proyecto se utilizó una computadora de escritorio CLON con las siguientes especificaciones:

- Procesador Intel ® Core ™ Dúo E7400 2.80 GHz

- 2 GB de RAM
- 250 GB de HDD.
- Resolución de pantalla de 1024 x 768.
- LCD 14”

Una vez instalado el sistema operativo en la PC, se confirmó si se instalaron los servicios a través del gestor de software Yast se localiza mediante el botón de menú, aplicaciones, sistema (véase Figura 29), también se puede acceder al Yast utilizando el lanzador rápido de escritorio (pulsando Alt + F2) y escribiendo en él, Yast.

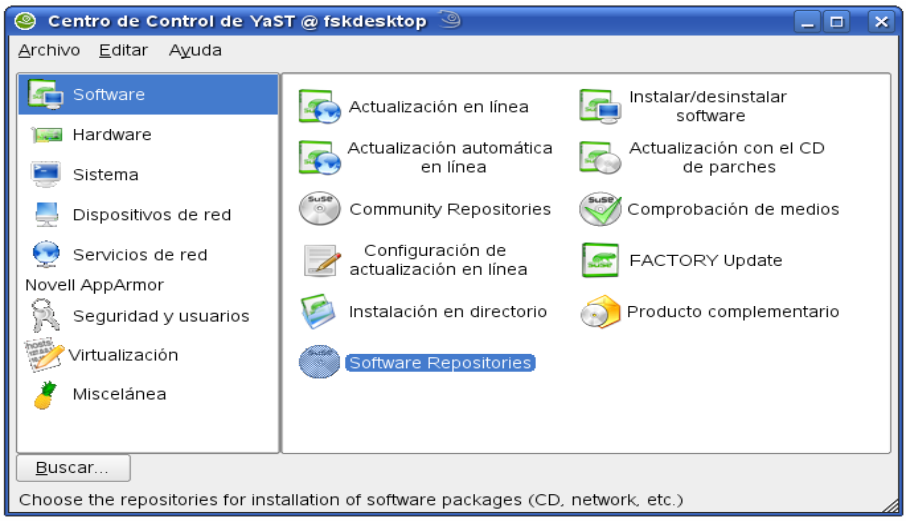


Figura 29. Panel de control Yast

Una vez dentro de Yast se debe verificar si están instalados los servicios que se necesitan, que son el servidor DNS y HTTP ya que los demás servicios los instalan de forma manual (MySQL, SSH) en la consola o terminal.

Configuración Servicios DNS, HTTP, MySQL y SSH.

Las configuraciones de los servicios se llevaran a cabo a través de modificaciones en algunos archivos presentes por defecto en el sistema. A continuación se detalla cada uno de los comandos y rutas de archivos utilizados para la configuración de todos los servicios del servidor Suse.

3.2.1 DNS (Servidor de nombres de dominio).

El DNS permitirá que la web sea localizada desde cualquier lugar del mundo mediante un nombre de dominio el cual es www.electronicsecurity.com que corresponde a la IP pública 200.62.73.203.

Un cliente DNS no almacena información DNS. Este casi siempre hace referencia a un Servidor DNS donde obtener la información que requiere. La única configuración para un Cliente DNS es la que se hace en el archivo /etc/resolv.conf, en el cual se define la dirección IP del servidor DNS que se debería usar.

Los DNS se utilizan para distintos propósitos:

- Resolución de nombres.
- Resolución inversa de direcciones.
- Resolución de servidores de correo.

Existen varios tipos de servidores DNS como Bind, Power DNS, djbddns y todos trabajan sobre el puerto 53 protocolo TCP/UDP. En este caso se utilizó Bind que viene por defecto en SLES 11.0.

Existen 4 tipos de servidores DNS, los más importantes son:

Maestro: El servidor se comporta como un auténtico servidor DNS ya que atenderá las peticiones de resolución de nombre. Así mismo responde a consultas de otros servidores DNS.

Esclavo: Este tipo de servidor solamente sirve como espejo de un servidor DNS maestro , cuando el servidor DNS maestro tiene alguna modificación se verá reflejado en el servidor DNS esclavo ya que esta sincronizados.

Lo primero que se debe hacer es configurar el DNS cliente para esto se debe editar el archivo resolv.conf que se encuentra en /etc/resolv.conf a través de la terminal utilizando el editor **vi** (véaseeditar el archivo named.conf que se encuentra en etc/named.conf este es un enlace simbólico a /var/lib/named.

Lo más importante del archivo named.conf es la definición de las zonas. Se configuró una Zona de tipo Master, además en named.conf se observan algunas zonas definidas ya por defecto en el sistema (véase figura 31), la primera zona definida por defecto hace referencia a los servidores de Raíz y las otras dos hacen referencia al local hosts.

A continuación se define la zona, esta se nombró electronicsecurity.com, y se determinó el nombre del archivo en donde se alojó la zona principal, aquí se debe declarar la configuración de los dominios que el servidor DNS alojará.

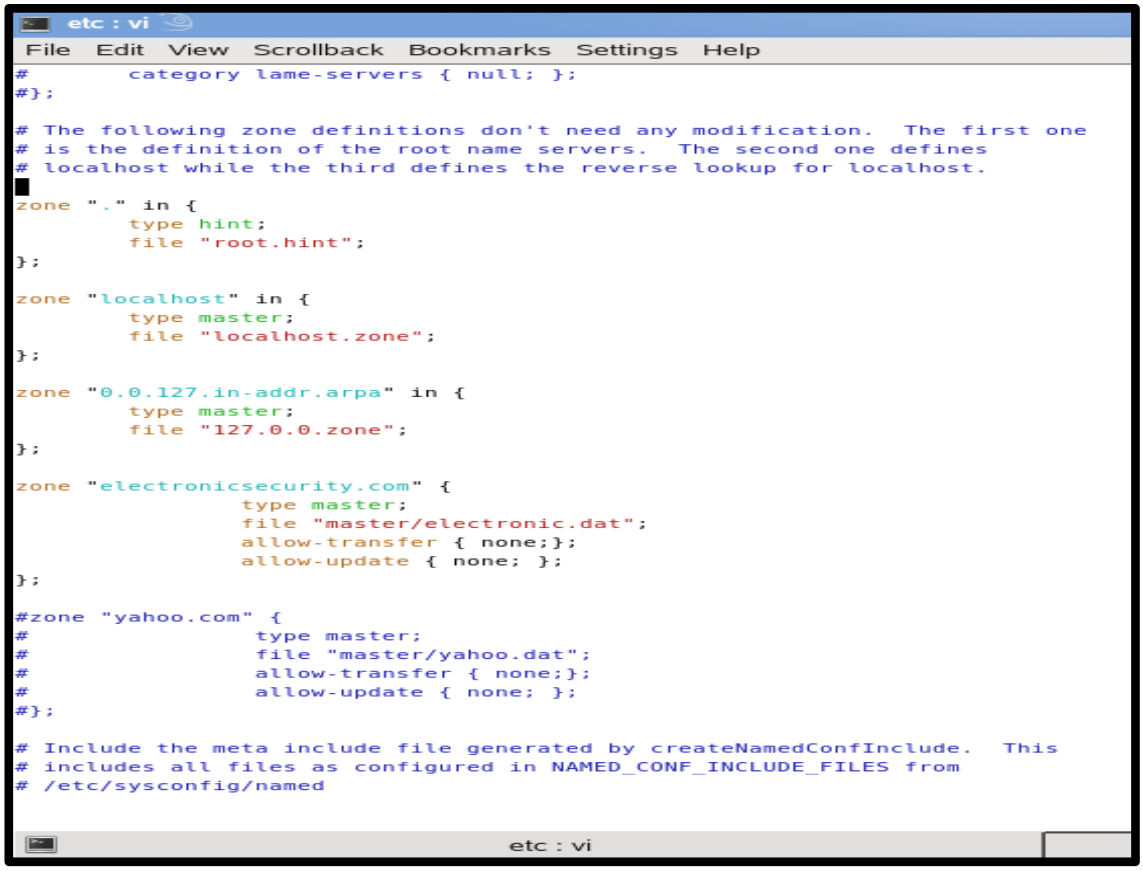


Figura 31. Archivo de configuración de las Zonas.

Una vez que configurada la zona el archivo quedó de la siguiente manera:

```
};
    zone "electronicsecurity.com" {
            type master;
            file "master/electronic.dat";
            allow-transfer {none;};
            allow-update{none; };
    };
```

Lo siguiente será crear un archivo de configuraciones de la zona, este se debe crear en /var/lib/named/master y se le debe asignar el nombre que se definió en named.conf el cual es electronic.dat.

En la configuración de los archivos de Zona se dividen por columna de datos y separadas por espacio que definen todos los registros del recurso de las zonas asociadas. A continuación les muestran los tipos de registros más frecuentes (véase Tabla 2).

Tipo de registro	Descripción
A	Registro de dirección IP que se le asigna un nombre.
AAAA	Registro de dirección IPv6 que se le asigna a un nombre, en este caso también se puede ocupar el tipo de registro A6.
CNAME	Registro del nombre canónico que dice al servidor de nombres que otros nombres son conocidos hacia un registro. Permite la creación de nombres, alias hacia nombres de dominio.
MX	Registro de servidor de correos electrónicos, que indica a donde se tiene que dirigir el correo.
PTR	Registro que sirve sobre todo para la resolución inversa de nombres, se orienta a través de la dirección IP.
NS	Registro de servidor de nombres que permite definir una lista de nombres

	con autoridad a un dominio.
SOA	Registro que proclama información importante sobre la autoridad de determinados servidores, sobre determinados espacios de nombres. Este registro los datos de correos electrónicos, números de series y parámetros de expiración.
TXT	Registro de texto que permite al administrador insertar texto arbitrariamente en un registro DNS

Figura 2. Tipos de registros

Se debe utilizar el registro de tipo A, El archivo de configuración quedara de la siguiente manera:

$TTL 86400

@ SOA electronicsecurity.com. admin.electronicsecurity.com. (

2011230201 3600 1200 604800 7200)

	IN	NS	server.electronicsecurity.com.
server.electronicsecurity.com.	IN	A	200.62.73.203
electronicsecurity.com.	IN	A	200.62.73.203
www.electronicsecurity.com.	IN	A	200.62.73.203

Una vez realizadas todas las configuraciones anteriores se tendrá listo el servidor DNS, se puede probar haciendo ping a cada una de las direcciones especificadas en el archivo de configuraciones (electronic.dat). Otra forma de probar su buen funcionamiento es:

nslookup server (nombre de host)

nslookup electronicsecurity (dominio)

nslookup www (Web)

nslookup 200.62.73.203 (dirección ip)

3.2.2 HTTP (Protocolo de transferencia de hipertexto)

Ahora que ya se tiene configurado el servidor DNS, se debe configurar un Servidor Web, el cual nos permitirá alojar la página web. En este sistema se utilizó Apache. Este servidor HTTP es usado principalmente para enviar páginas web estáticas y dinámicas en la World Wide Web. Muchas aplicaciones web están diseñadas asumiendo como ambiente de implantación a Apache, o que utilizan características propias de este servidor web.

Apache es un componente de servidor web en la popular plataforma de aplicaciones LAMP, junto a MySQL y los lenguajes de programación PHP/Perl/Python (y ahora también Ruby). Este sitio necesitara soporte de php y de una base de datos cuya instalación se explicará más adelante. Al igual que Bind, Apache viene incluido en el SLES 11.0, de lo contrario se debe instalar de forma manual a través de la línea de comandos (Consola) o a través del Yast.

El servidor web Apache ya viene configurado por defecto y utiliza el puerto 80, en este caso, lo que más más interesa es conocer la ruta en donde se debe alojar los archivos de las página web. Si se necesita hacer algún cambio en la configuración, se editan los archivos que se encuentran en /etc/Apache2 los cuales son:

- httpd.conf
- listen.conf
- vhosts.d

La ruta donde se debe alojar el sitio web es /srv/www/htdocs, esta ruta se encuentra en el archivo httpd.conf. Para comprobar el buen funcionamiento del servidor Web se editó en el navegador www.electronicsecurity.com y donde aparecerá el siguiente mensaje It Works!.

Esto es debido a que en la carpeta httdocs viene por defecto un **index.html** que contiene dicho mensaje. Si se tiene problemas con el Servidor DNS y HTTP se pueden iniciar con el comando *service named start* (para el DNS) y *service apache2 start* (para HTTP).

Si lo que se necesita es reiniciar los servicios se utiliza el mismo comando pero con *restart.* Lo más conveniente es que todo los servicios se inicien automáticamente cuando se encienda el servidor, para esto se utiliza el comando *chkconfig named on* y *chconfig apache2 on*, estos comandos son válidos para SLES, OpenSuse y cualquier otra distribución Linux basada en SUSE.

Una vez configurado el servidor web, es necesario un gestor de bases de datos para el sitio web, Al igual que Bind y Apache, MySQL es parte del paquete de SLES 11.0 de lo contrario se debe instalar desde el Yast.

3.2.3 Gestor de Base de Datos MySQL.

A continuación se explica paso a paso como entrar a MySQL y crear una nueva base datos:

1. Se accede a través de *Mysql*
2. *Show DATABASES;* este permite visualizar las bases de datos que se han creado.
3. Para crear la base de datos se utiliza *create DATABASES nuevabd;*
4. *Use nuevavabd*
5. *GRANT ALL ON joomla.* TO `userjoomla@`localhost` INDENTIFIED BY `password`;* Con este comando se define el nombre de la base de datos, la cual se llamó Joomla que será el administrador de contenidos de la web, el usuario y la contraseña.
6. Para salir de MySQL se usa *quit.*

Una vez creada la base de datos, se reinician los servicios de MySQL para que se hagan efectivos los cambios realizados, a través de *service mysql restart.*

Lenguaje de programación PHP

En la actualidad PHP es un lenguaje de programación orientado al desarrollo de aplicaciones web dinámicas con acceso a información almacenada en una base de datos, además algunos administradores de contenidos como Joomla necesitan soporte de PHP para sus aplicaciones.

Para que la web trabaje eficientemente se deben instalar en el servidor algunos complementos PHP. A continuación se presenta una lista detallada de los estos complementos, los cuales pueden ser instalados muy fácilmente desde el Yast (véase Figura 32).

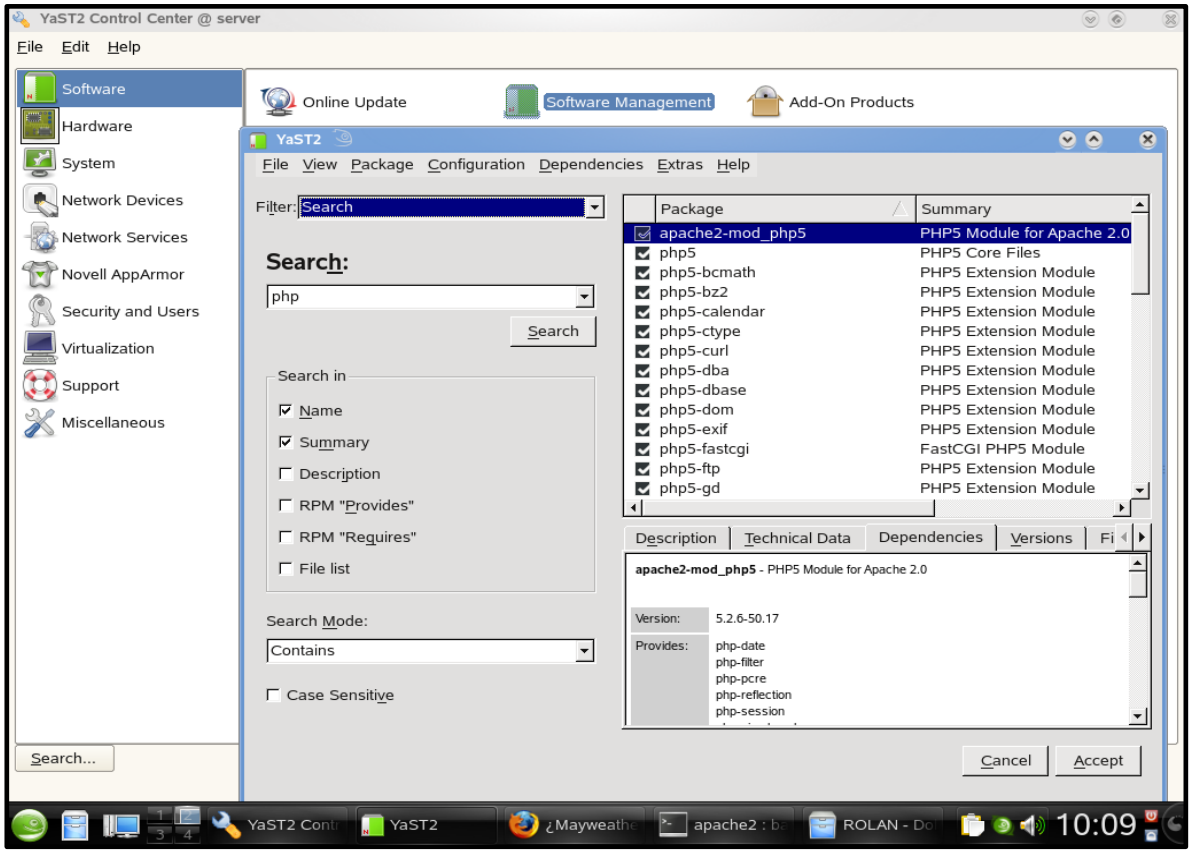


Figura 32. Instalación de PHP mediante Yast

3.2.4 Interprete de Órdenes Seguras SSH.

Una de las mayores ventajas de este sistema de vigilancia es que se le brindara al usuario un servicio de soporte técnico de forma remota, a través del protocolo SSH que sirve para acceder a máquinas remotas a través de una red, utilizando el puerto 22. Este permitirá tener control total del servidor. En la actualidad existen una gran variedad de programas en Windows que permite este servicio, los más utilizados son Putty y SSH Secure Shell Client (véase Pagina 33), en este caso se utilizó el segundo, debido a su agradable interfaz y fácil manipulación.

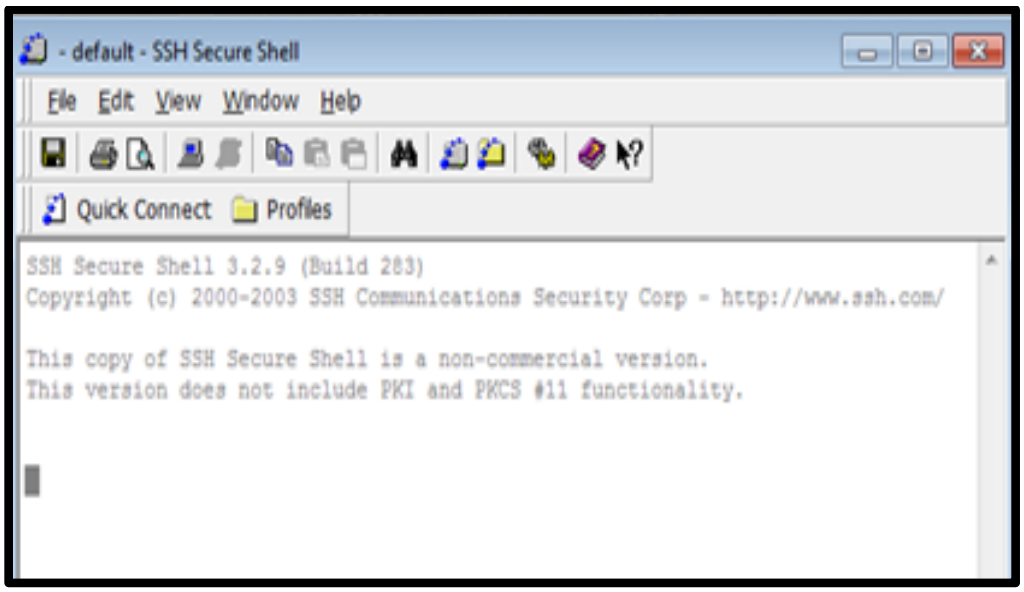


Figura 33. Interfaz de SSH

Para acceder al servidor Suse desde cualquier PC con Windows por medio de SSH Secure Shell Client, se debe abrir la interfaz del programa y con un Intro se accede a la pestaña Connect to Remote Host (véase Figura 34), donde se debe digitalizar la dirección IP del host (200.62.73.203), el nombre del usuario (root), y el número del puerto que se está utilizando (24).

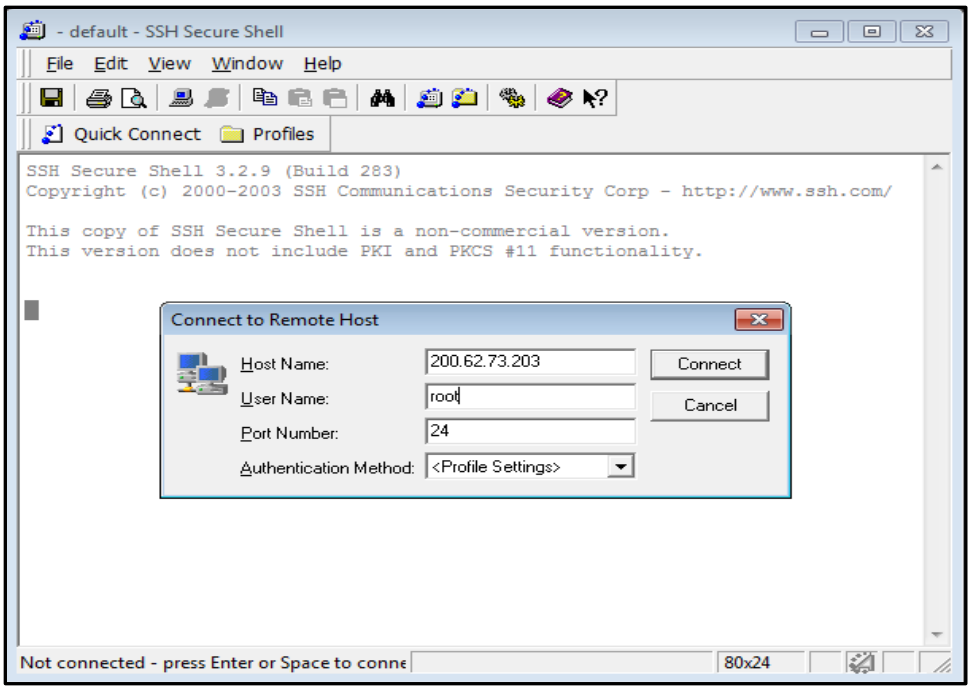


Figura 34. Conexión a un host remoto.

Una vez introducidos estos datos aparecerá una pequeña pestaña solicitando la contraseña del servidor (véase Figura 35). Después de esto el administrador podrá realizar todas las configuraciones o soporte técnico necesario para el buen funcionamiento del sistema.

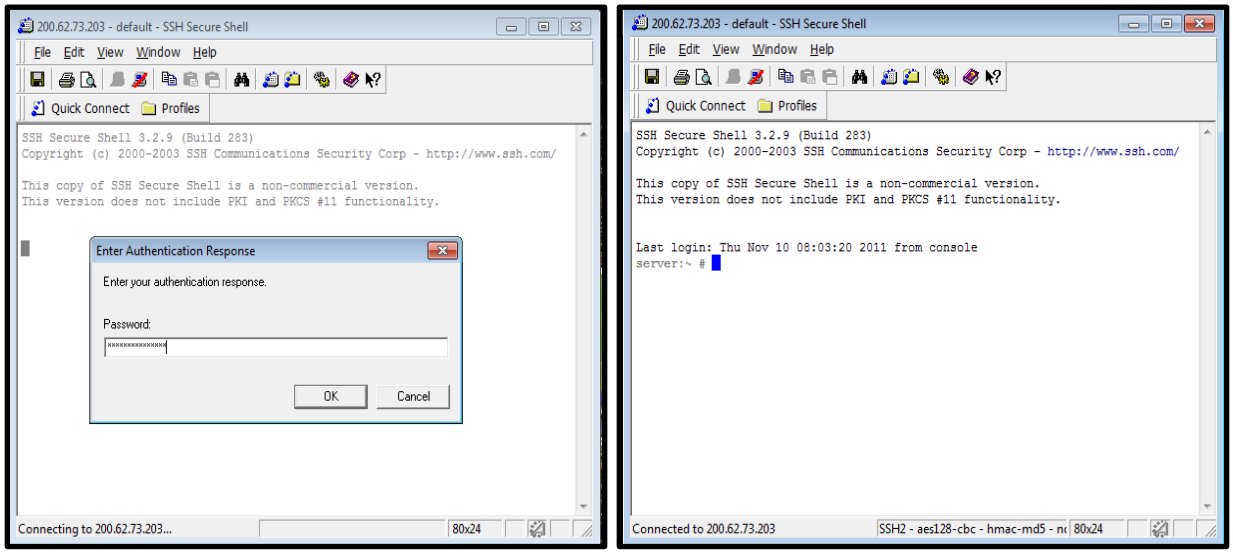


Figura 35. Conexión del servidor SLES mediante SSH.

También existen aplicaciones en Linux como es el caso de SSH Server, el cual se puede instalar desde la terminal o consola, esto es válido cuando el usuario se conecta al servidor desde una PC con sistema operativo Linux. Para configurar este servicio se debe instalar openssh-server a través del comando *apt-get install openssh-server*, una vez instalado el programa se puede conectar a la interfaz del servidor a través de *ssh "ip del host"* y luego se debe digitalizar la contraseña al recibir esta petición. Este ejemplo es válido solo para sistemas operativo Ubuntu.

3.3 Diseño de Página Web

Para desarrollar de una manera óptima el sistema vigilancia y seguridad fue necesaria la creación de una página Web que permitirá de una manera sencilla ofrecer servicios e interactuar con el usuario, además de la visualización de contenidos e información relacionada con este proyecto.

A través de la Web dinámica el usuario podrá acceder al software de seguridad (ZoneMinder), en donde podrá visualizar imágenes en tiempo real captadas por las cámaras ubicadas en su domicilio de forma segura y rápida. Así como estar en constataste comunicación con el administrador del sistema por medio de los formularios de contactos.

El diseño de la página fue realizado sobre Photoshop (CS3) y su programación se hizo en Adobe Dreamweaver y se utilizaron lenguajes de programación tales como HTML, CSS, PHP y XML con soporte de una base de datos creada en MySQL. Para convertir la Web estática en dinámica utilizamos el administrador de contenidos Joomla 1.5 (véase Figura 36). Para acceder a Joomla se debe editar en el navegador de preferencia, la dirección URL de la Web y agregarle **/administrator** donde se debe digitar usuario y contraseña. El acceso a este es permitido únicamente para el administrador del sistema en caso de cambios y mejoras a la Web.

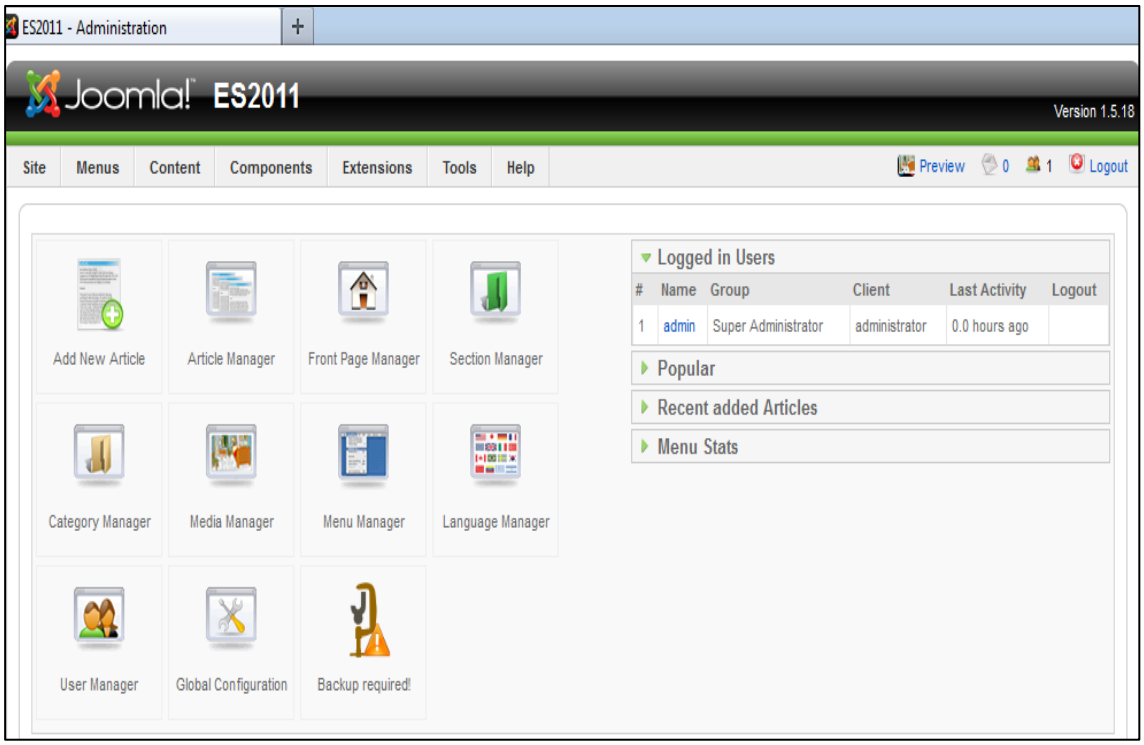
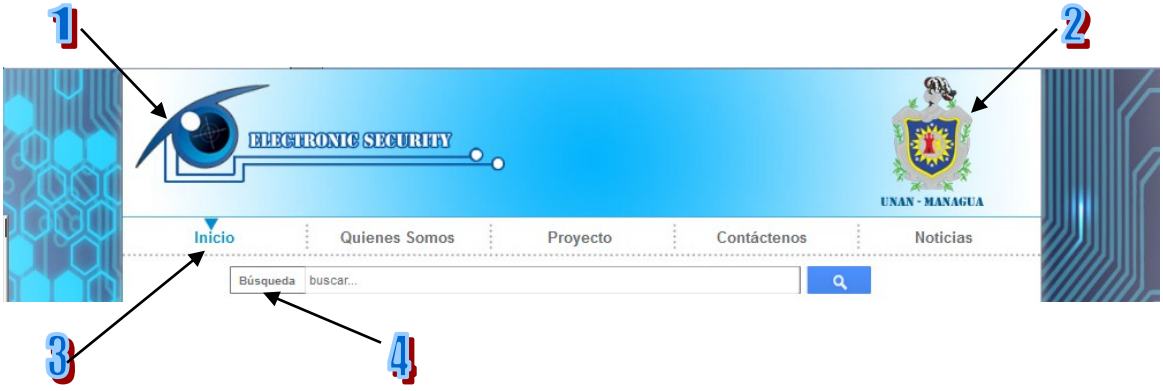


Figura 36. Panel de control de Joomla.

Este administrador de contenidos ofrece la siguientes funcionalidades como por ejemplo: Generadores de formularios dinámicos, galerías de imágenes multimedia, servicios de directorios, gestores de documentos, motores de comercio y venta electrónica, software de foros y chats, boletines de noticias, entre otros.

A continuación se explica a detalle la estructura de la página web:



1. **Logo:** Este fue creado para dar una imagen corporativa, mostrando este proyecto de una forma empresarial que brinde servicios de vigilancia y seguridad con cámaras IP.

2. **Banner:** En este se presenta el logotipo de la UNAN-Managua, el cual al dar clic se enlazará (vinculo) al sitio Web de la UNAN en una nueva pestaña.

3. **Menú Horizontal:** Este es un menú dinámico compuesto por 5 botones (Inicio, Quienes Somos, Proyecto, Contáctenos, Noticias). Al hacer clic sobre cada uno de ellos se accederá a cada uno de los contenidos presentes en la página Web.

4. **Motor de búsqueda:** Esta facilitará la localización de contenidos o textos a través de una palabra clave, la cual una vez digitada el motor de búsqueda presentara todos aquellos contenidos en donde esté presente dicha palabra.

5. **Banner 2:** Este es una breve descripción del proyecto para que el usuario tenga una idea de los servicios que ofrecemos como Electronic Security.

6. **Sub Menú:** Está compuesto por 5 botones que definen la ubicación de las cámaras en su domicilio, no es más que un enlace directo al software de seguridad ZoneMinder.

7. **Content:** Aquí se visualizara el contenido correspondiente a cada botón del Menú principal.

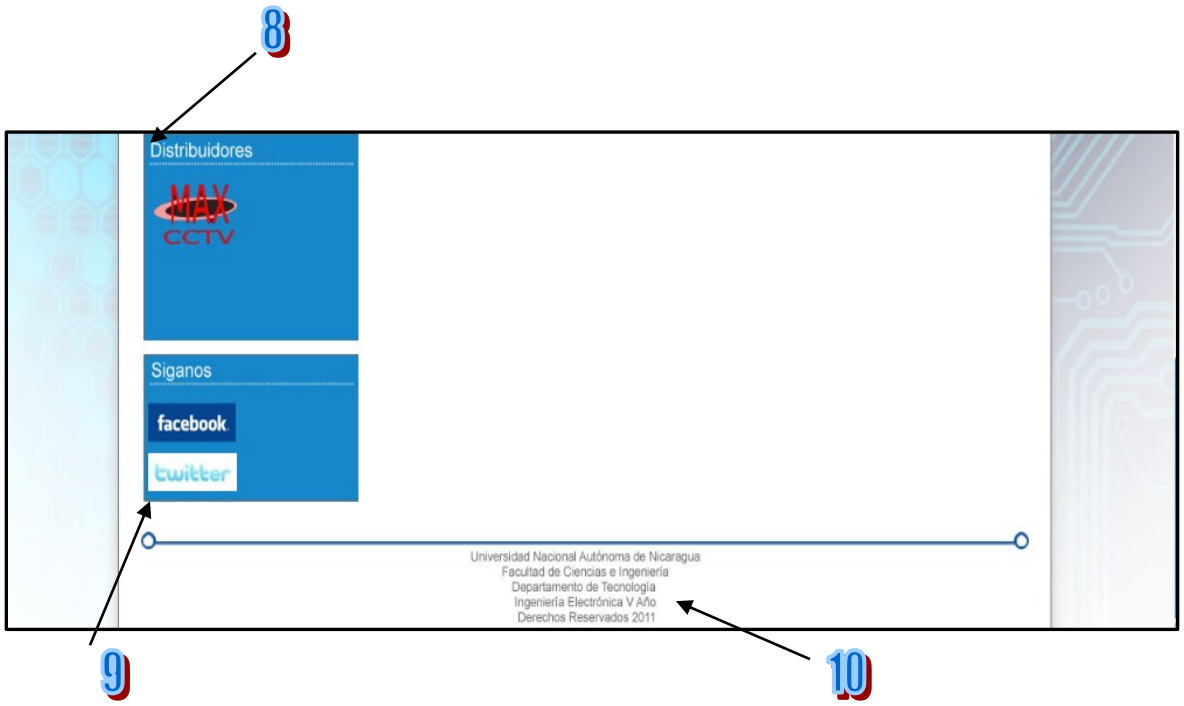
   Botón Inicio: Este cargará por defecto cada vez que el usuario acceda al sitio Web, permitiendo visualizar en el content la interfaz del software de vigilancia y seguridad ZoneMinder.

   Botón Quienes Somos: Se visualizará a través del content una pequeña descripción personal de los creadores del sistema de vigilancia y seguridad.

   Botón Proyecto: En este se mostrara un resumen del trabajo escrito con un vínculo, que permitirá al usuario descargar el trabajo completo en formato PDF.

   Botón Contáctenos: Ofrecerá un formulario de contactos en donde el usuario podrá contactarse con los administradores del sistema, en caso de alguna solicitud de soporte técnico o consulta en general.

   Botón Noticia: A través de él se tendrá acceso a artículos externos relacionados a sistemas de seguridad publicados en otros sitios web para una mayor información.



8. **Distribuidores:** Este espacio abierto para todos aquellos distribuidores o empresas en que se publiquen su servicios en la Web, esto implicara un costo económico, su función será que cuando el usuario de un clic al logotipo de su preferencia sea enlazado a la página oficial de los proveedores.

9. **Sociales:** Desde aquí el usuario tendrá un acceso directo a las cuentas de redes sociales que tiene Electronic Security, donde podrán dejar comentarios, consultas, sugerencias y dudas sobre el sistema de vigilancia y seguridad, además de publicar sus propios artículos y compartirlos en línea con los demás usuarios.

10. **Footer:** En este caso se utilizó para agregar créditos que hacen referencia a la estructura académica de la facultad, así como el nivel académico de los autores del proyecto y derechos de autor.

Una vez realizada la programación de la página Web se procedió a hacer el montaje de esta a través de XAMPP que es un servidor independiente de plataforma, software libre que consiste principalmente en la base de datos MySQL, servidor

Web apache y los interpretes para lenguajes de script: PHP y Perl. Este trabaja de la mano con Joomla y con el complemento de Firefox Firebug que son herramientas que facilitan la programación en HTML y CSS. Para importar la Web de XAMPP a srv/www/htdocs (ruta en donde se debe alojar la web en el SLES), se debe utilizar un componente de Joomla llamado Akeeba Backup el cual hará un respaldo total de la Web (véase Figura 37).

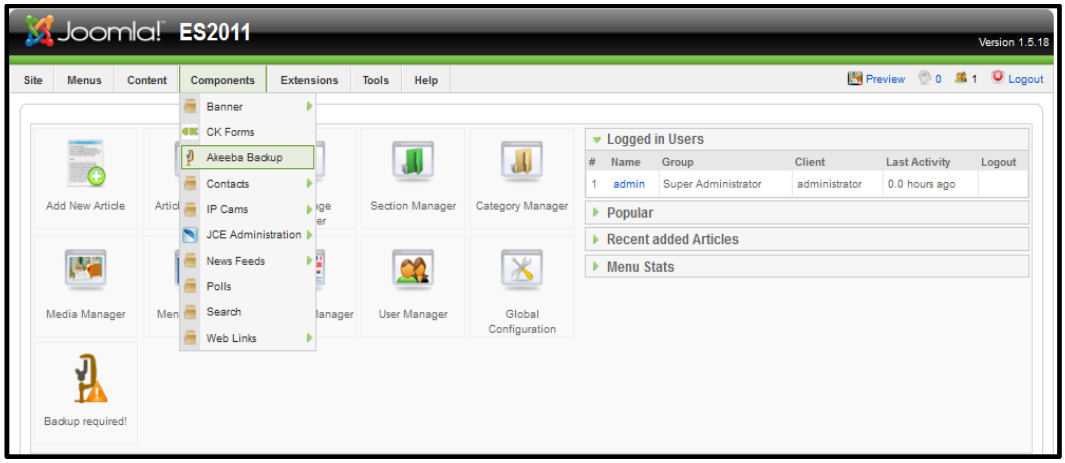


Figura 37. Selección de complemento Akeeba.

El Akeeba Backup creará un archivo site-localhost-20111110-165530.jpa, el cual se debe descomprimir con la ayuda del programa Akeeba Extract Wizard. Este generara una serie de archivos que se deben trasladar a /srv/www/htdocs.

Para montar la Web en el servidor apache instalado en SLES se debe digitar en el navegador de preferencia **localhost**, en donde cargara un asistente de instalación de Akeeba donde se deben rellenar los datos de la Web como se muestran en las siguientes figuras (véase figura 38, 39, 40, 41). Se debe de tomar en cuenta que la carpeta **htdocs** debe de tener permisos de lectura, escritura y ejecución, esto se hace con el comando *chmod –R 777 "nombre del directorio"*.

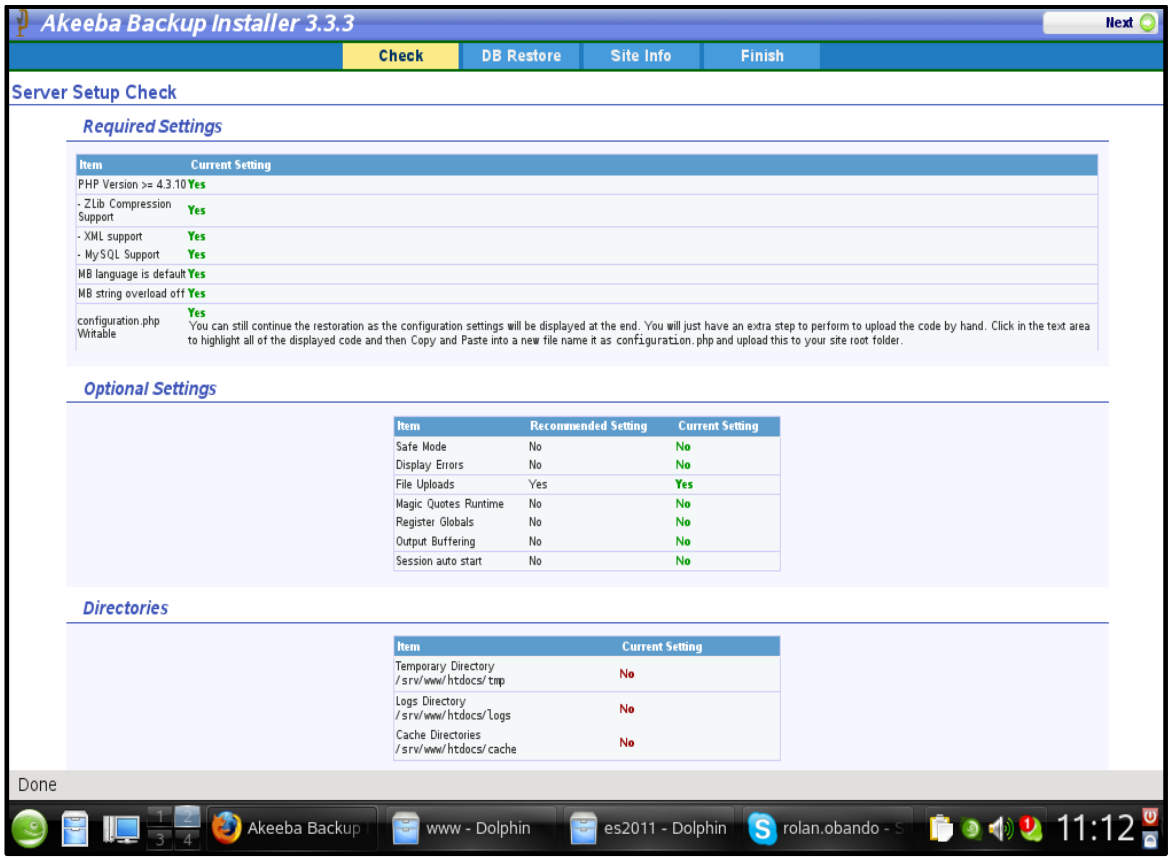


Figura 38. Dependencias necesarias para el funcionamiento de Akkeba.

Figura 39. Configuración de base de datos.

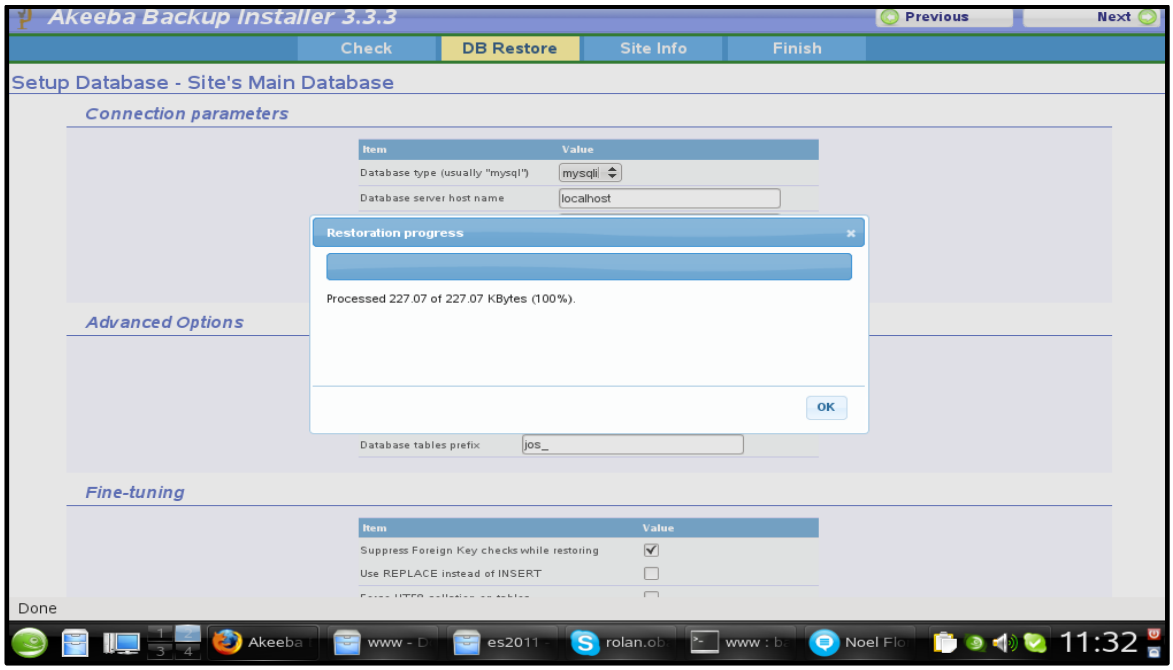


Figura 40. Comprobación de la base de datos.

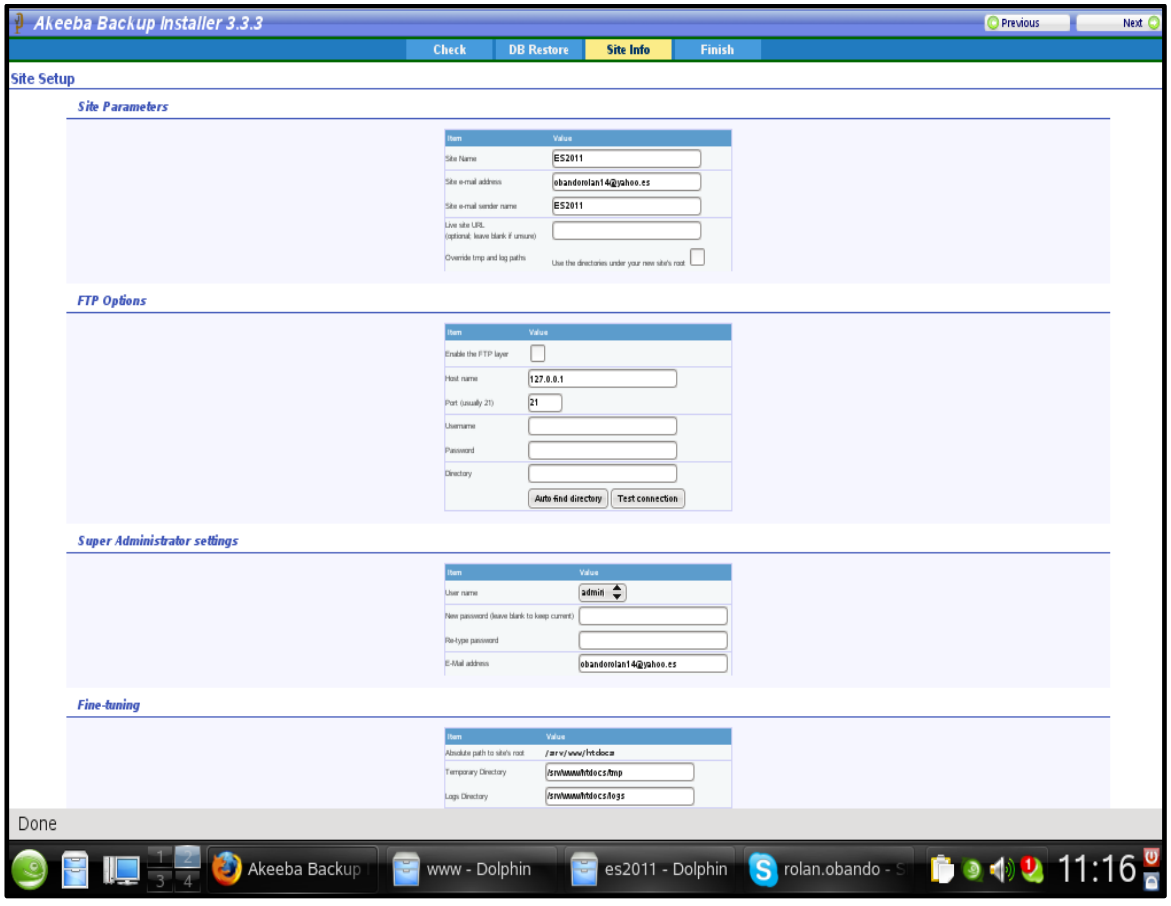


Figura 41. Información del sitio Web

El último paso es eliminar la carpeta installations y después hacer clic en el botón previous para cargar en el navegador la Web dinámica con todas sus aplicaciones e información.

3.4 Software de vigilancia y seguridad:

ZoneMinder es un conjunto de aplicaciones que conjuntamente proporcionan una completa solución de video vigilancia permitiendo capturar, analizar, grabar y monitorizar cualquier cámara CCTV, Cámaras IP, Webcam, conectada a un ordenador basado en Linux. Está diseñado para ejecutarse en distribuciones de Linux que soporten la interfaz Video For Linux (V4L) y puede soportar múltiples cámaras sin pérdida aparente de rendimiento. ZoneMinder requiere MySQL, PHP y se apoya en un servidor web como Apache.

Como inconveniente se puede decir que su instalación y mantenimiento no son aptos para personas sin una mínima base de conocimiento de Linux, y tecnologías web como Apache o PHP. El acceso se realiza mediante un navegador web incluso aunque se esté de forma local.

Las principales características que el software ZoneMinder proporciona son:

- Gestión de cámaras IP independientemente del fabricante.
- Administración de las grabaciones.
- Detección de movimiento.
- Gestión de la detección de movimiento.
- Gestión de varias fuentes de vídeo simultáneas.
- Agrupación de fuentes de vídeo por grupos lógicos, por ejemplo Múltiples zonas de riesgo.
- Gestión de usuarios.
- Acceso remoto o local vía explorador web.
- Envío de emails.

- Creación de eventos en función de un calendario.
- Creación de vídeo en formato MPEG, WMV, AVI, 3GP.
- Creación de logs comprimidos en formato Zip o Tar.
- Control del ancho de banda.
- Acceso desde dispositivos de interfaz reducida como PDA o teléfonos de última generación.

3.4.1 Instalación S.O Ubuntu 10.04

Debido a que se utilizó como servidor Suse Linux Enterprise Server 11.0 (SLES), el cual es una de las últimas versiones de Suse desarrollado por Novell, Inc. En la actualidad no se ha creado dependencia del ZoneMinder para esta versión de Linux, ya que solo existen dependencias para SLES 10.1, el cual en la actualidad se encuentra obsoleto. Para solucionar este problema se instaló ZoneMinder 1.24 en Ubuntu 10.04 ya que este es uno del S.O Linux más popular en la actualidad debido a una serie de ventajas:

- Fuerte enfoque en la facilidad de uso e instalación.
- Los drivers para hardware se descargan desde sitios seguros.
- Es estable, liviano y es compatible con la mayoría del hardware disponible.
- El soporte proporcionado por los foros te da soluciones e información en el menor tiempo.
- Las actualizaciones resuelven los posibles bugs que puedan surgir.
- Se puede utilizar en forma privada, pública o comercial sin tener que pagar licencias.

Los Requerimientos recomendados para la instalación de Ubuntu 10.04 se presentan a continuación:

- Procesador: 1.0 GHz.

- Memoria: 512 MB.
- Espacio libre en disco: 8 GB.

En este caso se utilizó una Notebook Toshiba modelo NB 505 con las siguientes especificaciones:

- Procesador: Intel ® Atom ™ CPU NS550 1.50 GHz.
- RAM: 2GB
- HDD: 320 GB
- LCD: 10.1 in.

Para la instalación de este sistema operativo se siguió paso a paso el asistente de instalación del sistema ya que los complementos se instalaron de forma manual a través de la Terminal (línea de comandos).

Una vez instalado el S.O Ubuntu se debe ejecutar las actualizaciones y complementos necesarios, para proceder a instalar el ZoneMinder, Esto se hizo por medio del Gestor de actualizaciones, este se localiza en **Sistema>Administración>Gestor de actualizaciones** (véase Figura 42) a través de él, se instalan Plugins adicionales y complementos del sistema, que permitirán el buen funcionamiento del software.

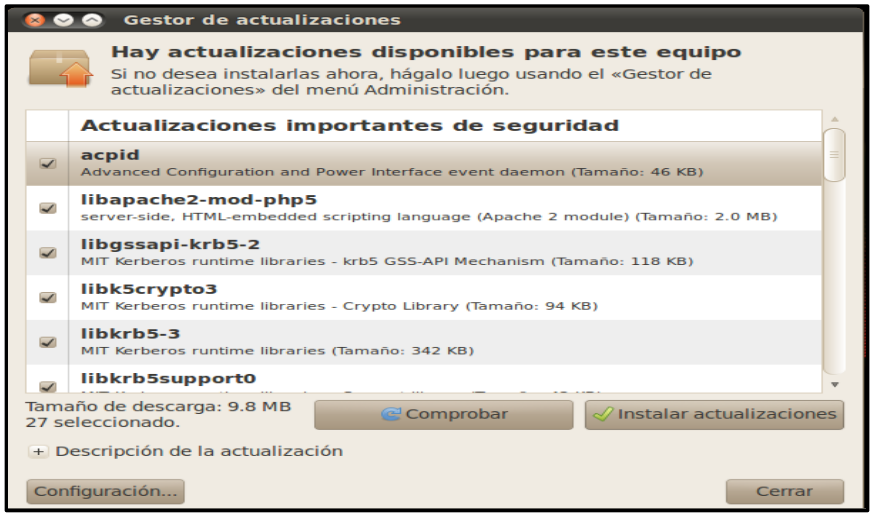


Figura 42. Gestor de actualización de software.

También se debe utilizar el gestor de paquetes Synaptic que se localiza en **Sistema>Administración>Gestor de paquetes Synaptic**, para instalar los soportes php (véase figura 43).

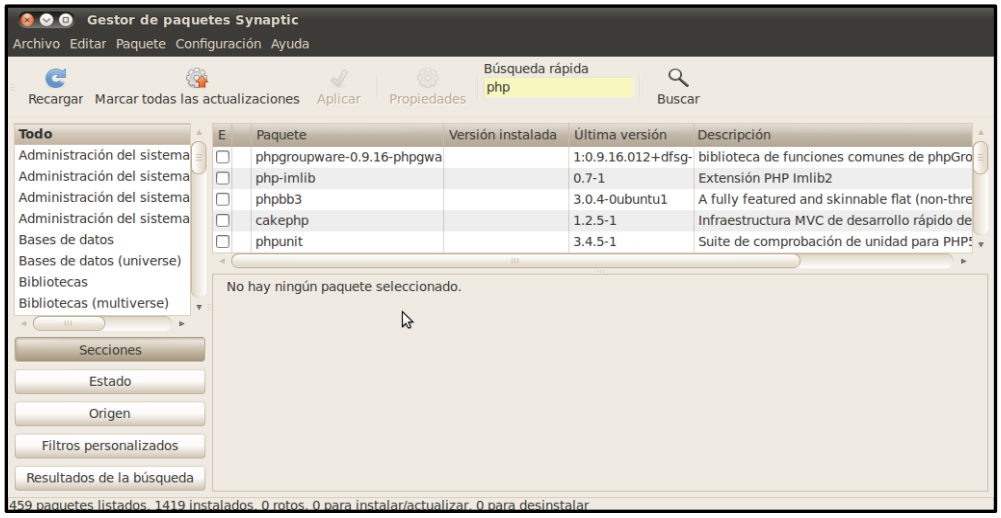


Figura 43. Gestor de paquetes synaptic

3.4.2 Instalación del ZoneMinder

Los requerimientos para la instalación del ZoneMinder en una computadora son los siguientes:

- CPU a más de 2.0 GHZ.
- Memoria RAM: 512 Mb.
- Tarjeta de captura de video: Solo en los casos en la que se utilicen cámaras de Tv de circuito cerrado.
- Tarjeta de Red.
- Manejo de dispositivos USB 2.0, Requerimientos de Software.

Debido a que el ZoneMinder cuenta con una interfaz Web se debe instalar un servidor Apache y una base de datos MySQL con los siguientes comandos:

apt-get install apache2

apt-get install mysql-server mysql-client

La instalación del ZoneMinder se realiza a través de una línea de comandos, en Ubuntu se hace por medio de la Terminal que se encuentra en el Menú **Aplicaciones>Accesorios>Terminal.** Los comandos son los siguientes:

- *apt-get install zoneminder* (instalación zm)
- *ln -s /etc/zm/apache.conf /etc/apache2/conf.d/zoneminder.conf* (enlace simbólico del zm al apache y agregar un alias en apache para poder acceder a zm desde el servidor web)
- */etc/init.d/apache2 force-reload* (reinicia el Apache)
- *mysql -u root -p < /usr/share/zoneminder/db/zm_create.sql*
- *mysql -u root -p* (esto lleva a la línea de comandos de mysql)
- *> grant select,insert,update,delete on zm.* to 'zmuser'@localhost identified by 'zmpass';* (para crear usuario y contraseña de la base de datos y garantizar el acceso de zm a mysql)
- *> flush privileges;*
- *> quit* (para salir de la base de datos)
- *chmod 4755 /usr/bin/zmfix* (para asignar permisos de lectura, escritura y ejecución a zmfix).
- *zmfix -a*
- *adduser www-data video*
- *gedit /etc/sysctl.conf* (esto manda al editor gedit).
- desplácese hasta la parte inferior del archivo y pegar lo siguiente: (Nota: Esto sólo tiene efecto después de un reinicio).

  kernel.shmall = 134217728

  kernel.shmmax = 134217728

- *zmpkg.pl start* (para iniciar el zoneminder)

Los comandos anteriores son para aumentar la memoria compartida del ZoneMinder.

Para comprobar que se instaló correctamente el ZoneMinder se debe editar en nuestro navegador http://localhost/zm el cual cargara la interfaz Web de zm (véase figura 44).

Lo primero que se presenta es la vista inicial cuando se está ejecutando en modo no authenticated (por defecto). La autentificación es una opción que permite especificar para cada usuario que se registra en ZoneMinder los permisos para ejecutar ciertas tareas. Se recomienda la ejecución en modo "authenticated", si nuestro sistema está abierto a internet.

Durante la instalación se crea un usuario con todos los privilegios cuyo login y password son "admin". Se recomienda cambiar el password tan pronto como sea posible. Para crear usuarios accedemos al link "Options" en la esquina superior derecha en la pestaña "system" marcamos la casilla ZM_OPT_USE_AUTH. A continuación podemos añadir, eliminar y establecer permisos de usuarios en la nueva pestaña "User" dentro de "Options".

La ventana de ZoneMinder ajustará su tamaño para no ser demasiado agresiva con el escritorio. En la parte superior podemos ver varias informaciones básicas como el momento de la última actualización y la carga del servidor. También habrá una indicación del estado del sistema: "stopped" o "running".

La vista será similar a:

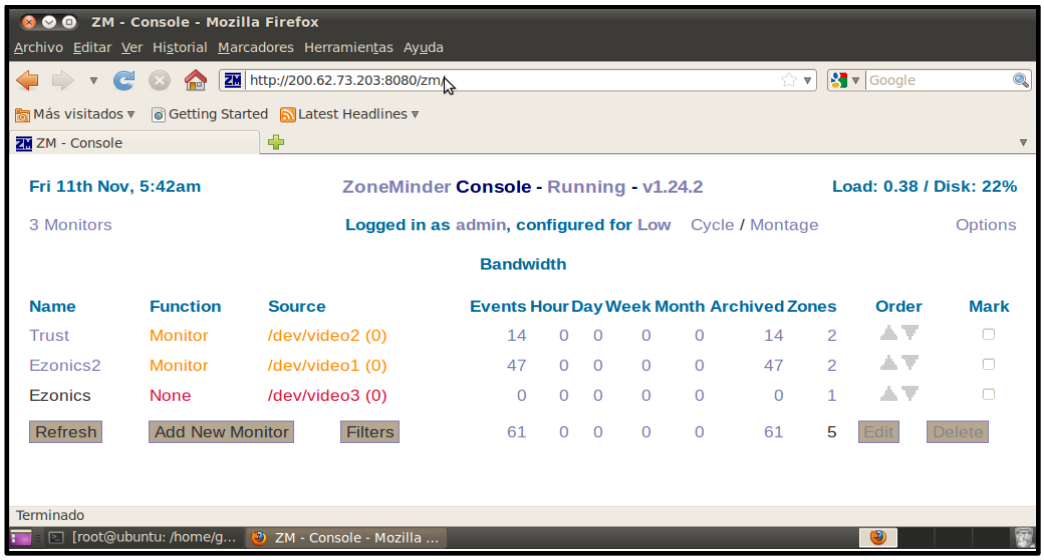


Figura 44. Panel de control del ZoneMinder

3.4.2.1 Definición de monitores

Para utilizar ZoneMinder es necesario definir al menos un Monitor. Un Monitor es básicamente una asociación con una cámara y puede realizar comprobaciones continuas de las imágenes captadas por esa cámara, como por ejemplo la detección de movimiento. Para crear un Monitor hacemos click en "Add New Monitor".

Es posible validar las cámaras mediante el comando "*zmu -d* <ruta del dispositivo> -q -v -U <usuario> -P <password>" (la ruta de las cámaras USB es normalmente /dev/video0, 1, 2, etc). De esta forma es posible además obtener valores útiles de configuración del dispositivo que sirven para completar los campos del panel "Add New Monitor". Si el comando *zmu* da un error lo más habitual es comprobar si poseemos todos los permisos, para esto ejecutamos "*zmfix -a*".

Las opciones están divididas en un conjunto de etiquetas. No es necesario salvar los cambios de una etiqueta, sino que se pueden rellenar los campos de todas ellas y luego salvarlas como un conjunto. Las opciones de cada etiqueta se describen brevemente a continuación.

Etiqueta "General":

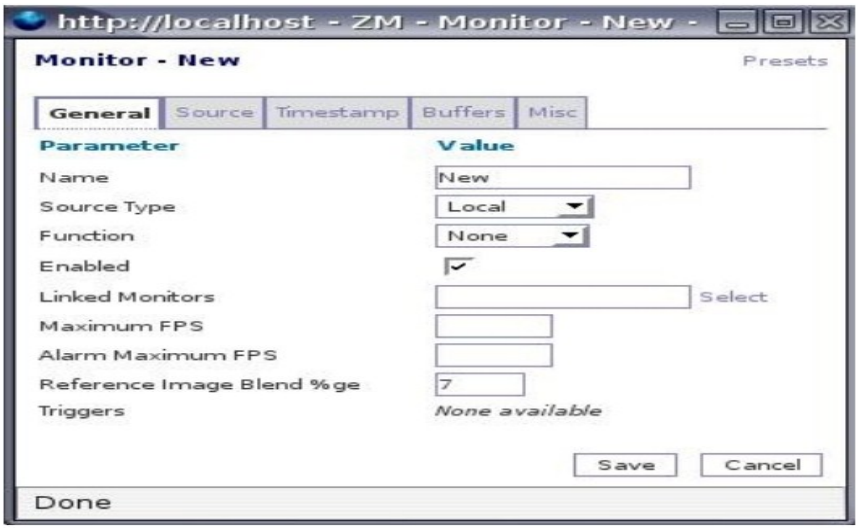


Figura 45

Name: El nombre del Monitor con caracteres sin espacios.

Source Type: Esta variable determina si la cámara está conectada de forma local, a un puerto USB de la máquina, si por el contrario es una cámara remota, o si es una fuente de imagen representada por un archivo. Seleccionar una opción u otra afectará al conjunto de opciones que se mostrará en la siguiente etiqueta.

Fuction: Esta variable define lo que el monitor hace. El estado puede ser uno de los siguientes:

- **None:** el monitor está actualmente desactivado y no es posible visualizar vídeo ni generar eventos.

- **Monitor:** El Monitor solo mostrará flujos de vídeo sin realizar un tratamiento de los mismos.

- **Modect (Motion Detection):** Todas las imágenes capturadas serán analizadas y se generará un evento cuando se detecte movimiento.

- **Record:** En este caso se generan continuamente eventos de una longitud determinada.

- **Mocord:** Es un estado entre Modect y Record, y el resultado son eventos de longitud fija con las zonas de detección de movimiento remarcadas dentro de esos eventos.

- **Nodect:** Este es un modo especial diseñado para ser usado con eventos externos.

Enabled: Indica si el monitor debe ser iniciado en modo activo o pasivo. Normalmente marcaremos esta opción salvo si queremos que la cámara sea activada o desactivada por acciones externas. Si no se activa el Monitor no generará ningún evento en respuesta a movimiento.

Linked Monitors: Este campo nos permite seleccionar otros monitores del sistema que actuaran como desencadenantes para activar este monitor. Por ejemplo, si tenemos varias cámaras supervisando una zona podemos hacer que todas empiecen a grabar si solo una de ellas detecta un movimiento. Hay que tener mucho cuidado de no crear dependencias circulares que nos llevarán a alarmas persistentes.

Máximum FPS: En algunas ocasiones podemos tener cámaras capaces de realizar altas tasas de captura, pero no normalmente no requeriremos tanto rendimiento para no sobrecargar el servidor. Esta opción nos permite limitar la máxima tasa de captura.

Alarm Máximum FPS: Si hemos especificado un nivel máximo de frames por segundo, quizás deseamos que este nivel sea sobrepasado ante una alarma. Este valor nos permite definir el número de frames (fotograma o capturas) por segundo generados (FPS) ante una alarma.

Reference Image Blend: Cada imagen analizada en ZoneMinder es una composición de las imágenes previas, normalmente formada aplicando la imagen actual con un cierto porcentaje de la imagen anterior de referencia. Este valor alrededor de 10, nos permite definir el porcentaje de imagen de referencia que se aplicará a la imagen actual.

Triggers: Esta sección nos permite seleccionar que eventos se aplicarán si el modo de ejecución ha sido establecido "Triggered". El evento más común es el generado por el estándar x10.

Etiqueta "Source" (para dispositivos locales)

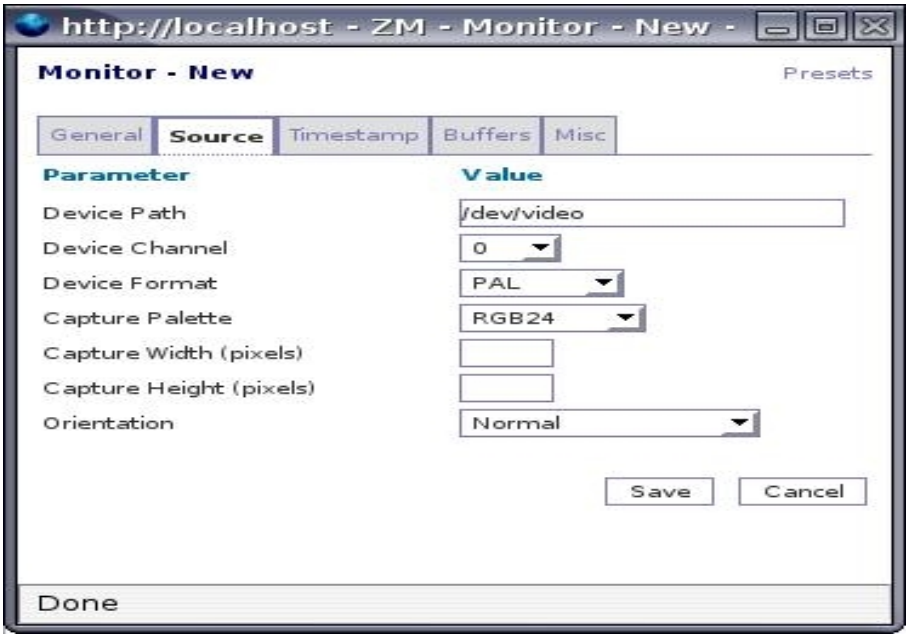


Figura 46

Device Path/Channel: Especifica la ruta completa donde se ubica el dispositivo, por ejemplo /dev/video0, 1, 2, etc. y Channel 0 para dispositivos USB.

Device Format: El formato del Streaming de video. Los más comunes son 0 para el sistema PAL y 1 para el NTSC.

Capture Palette: Indica la profundidad de color. Si tenemos dudas es interesante comenzar probando con escalas de grises, Grey, o colores de 24 bits.

Capture Width/Height: Especifica las dimensiones del Streaming de video que generará la cámara.

Orientation: S i por motivos de ubicación nuestra cámara se encuentra girada es posible "girar" el video para que la visualización sea correcta.

Etiqueta "Timestamp"

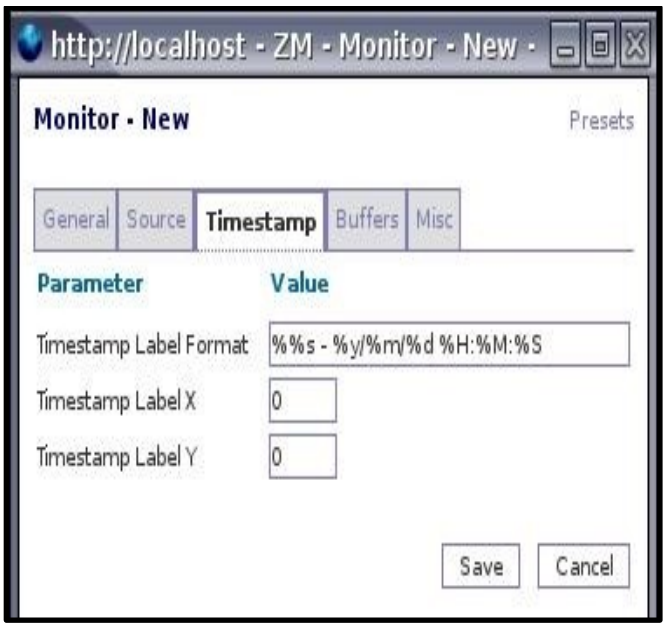


Figura 47

Timestamp Label Format: Indica el formato de la etiqueta de tiempo, fecha y hora, que se superpone al video generado. Por defecto especifica año/mes/día hora/minuto/segundo con el formato %y/%m/%d %H:%M:%S.

Timestamp Label X/Y: Indican la posición en coordenadas cartesianas dónde se ubicará la etiqueta. El punto 0,0 especifica la esquina superior izquierda de la pantalla.

Etiqueta "Buffers"

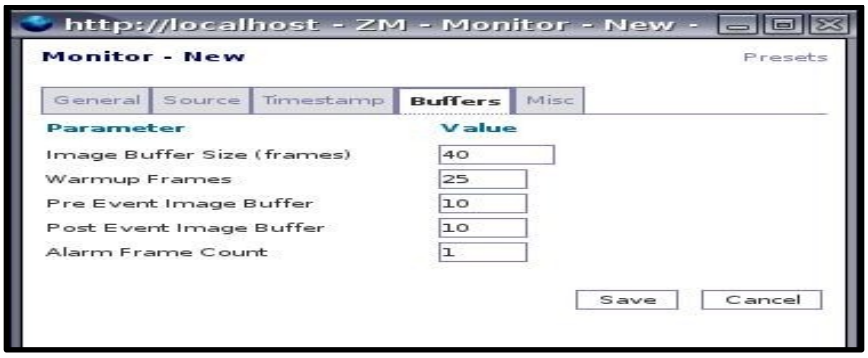


Figura 48

Image Buffer Size: Este es el tamaño del buffer de imágenes, donde se guardan las últimas imágenes captadas. Son imágenes que aún están esperando tratamiento. Estas imágenes se incluyen también como previas a la generación de una alarma, es decir, si se genera una alarma se presentan los frames que generaron la alarma y también algunas capturas previas que se obtienen de este buffer.

Warm-up Frames: Especifica cuantos frames procesará, pero no examinará el demonio de análisis al inicio. Esto permite generar una referencia precisa antes de buscar cambios en los frames para detectar alarmas.

Pre/Post Event Image Buffer: Indica cuantos frames deben conservarse antes y después de un evento para incluirlos en las capturas. Esto nos permitirá ver qué ocurrió antes y después de un evento concreto. Normalmente se utiliza el valor 10 para ambos, pero si deseamos generar un número menor de eventos pero más largos incrementaremos el buffer Post, ya que el Pre está limitado a la mitad de la variable Image Buffer Size.

Alarm Frame Count: Indica cuantos frames de alarma consecutivos deben ocurrir antes de que se genere un evento. Por defecto se utiliza el valor 1, aunque valores de 3 o 4 evitan las falsas alarmas generadas por fluctuaciones de luz o defectos de visualización.

Etiqueta Misc

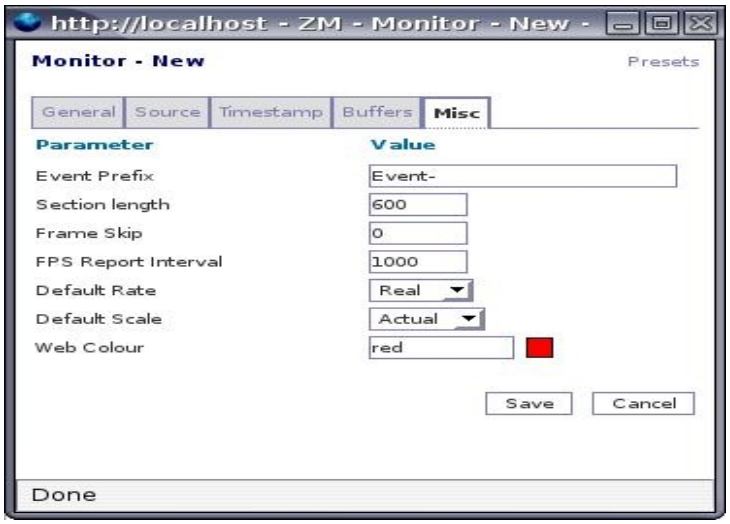


Figura 49

Event Prefix: Por defecto los eventos se llaman "Event- <id del evento>" pero se nos permite modificarlo para llamarlos como deseemos y así poder identificar, por ejemplo, que Monitor los generó.

Section Length: Especifica la longitud en segundos de los eventos de longitud fija generados cuando el Monitor está en modo Record o Mocord. Si el modo es cualquier otro, esta variable se ignora.

Frame Skip: Esta característica se aplica también si el Monitor se encuentra sólo en modo Record o Mocord, e indica cuantos frames se deben saltar al grabar los eventos. Un valor de 1 indica que se salta un Frame de cada uno grabado, 2 indica que se saltarán 2 frames por cada uno grabado, etc.

FPS Report Interval: Indica cada cuantos segundos se refresca la tasa de frames por segundo que ofrece la cámara.

Default Scale: Si hemos elegido un tamaño de imagen particularmente grande o pequeño, con esta variable podemos escalarlo.

Web Colour: Algunos elementos de ZoneMinder utilizan colores para diferenciar Monitores. Desde aquí se selecciona el color que identificará a este monitor.

Finalmente si hacemos click en "Save" ya tendremos perfectamente caracterizado nuestro Monitor.

3.4.2.2 Consola principal de ZoneMinder: Ahora, de vuelta a la consola principal, veremos algunas columnas con estadísticas vitales. La mayoría de las columnas son también links. De izquierda a derecha tenemos: Id, Name, Function, Source, Events, Hour, Day, Week, Month, Archive, Zones, Order y Mark (véase figura 50).

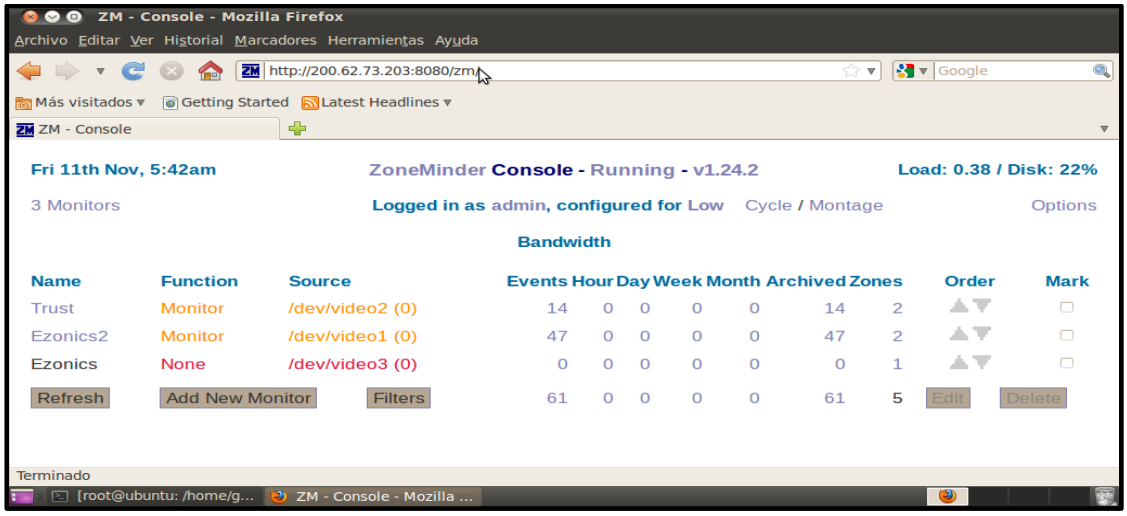


Figura 50. Menú de aplicaciones de ZoneMinder.

Function y Source: Estas dos columnas nos proporcionan información vital dependiendo del color en que se muestran. El rojo indica que el monitor no ha sido configurado para realizar ninguna acción y por lo tanto no existe ningún demonio de captura (*zmc*) ejecutándose en él.

Si el color es naranja significa que existe un demonio de captura ejecutándose (*zmc*) pero no uno de análisis (*zma*). En verde indica que ambos funciones se están

ejecutando. Para ejecutarlas podemos hacer click en una de las columnas y cambiar la funcionalidad del Monitor. Si tenemos varios Monitores apuntando a un mismo dispositivo, el color de estado del dispositivo indica el estado de todos los Monitores.

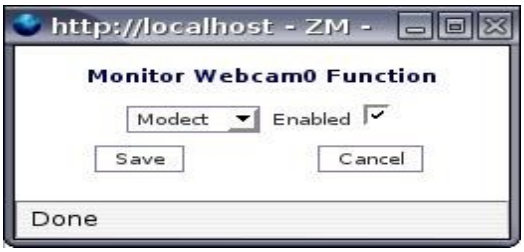


Figura 51. Funcionalidad del monitor.

Una vez que tenemos varios Monitores activos, la etiqueta "<n> Monitors" se convierte también en un link permitiéndonos asociarlos en grupos. También se activarán los links Cycle, que mostrará unos instantes de cada monitor del sistema en una nueva ventana, y Montaje (véase figura 52), que nos mostrará todos los monitores activos en una nueva ventana.

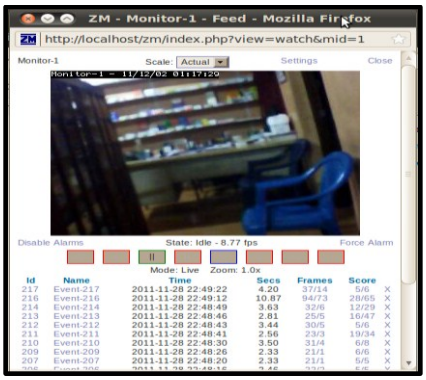


Figura 52. Visualización de un solo monitor.

Definición de zonas

El próximo paso importante a dar para trabajar con Monitores es configurar las "Zonas". Por defecto ya existe una zona que ocupa toda la imagen capturada pero se debe crear una Zona propia. Si hacemos click en la columna Zonas de un monitor veremos una nueva ventana que contendrá la imagen capturada por la cámara. Dicha imagen tendrá superpuesto un mallado representando las Zonas.

El color de la Zona determina de qué tipo se trata. La zona por defecto es una Zona Activa así que estará coloreada en rojo. Las Zonas Inclusivas aparecerán en naranja, las Exclusivas en púrpura, las pre exclusivas en azul y las Inactivas en blanco.

En principio no tendremos zonas seleccionadas debajo de la imagen donde se representan las zonas aparecerá un listado de las mismas. Haciendo click en cada una podremos editar las particularidades.

Para añadir una zona, haciendo click en "Add New Zone" o modificar las características de la misma accedemos a la ventana de configuración o pantalla de características.

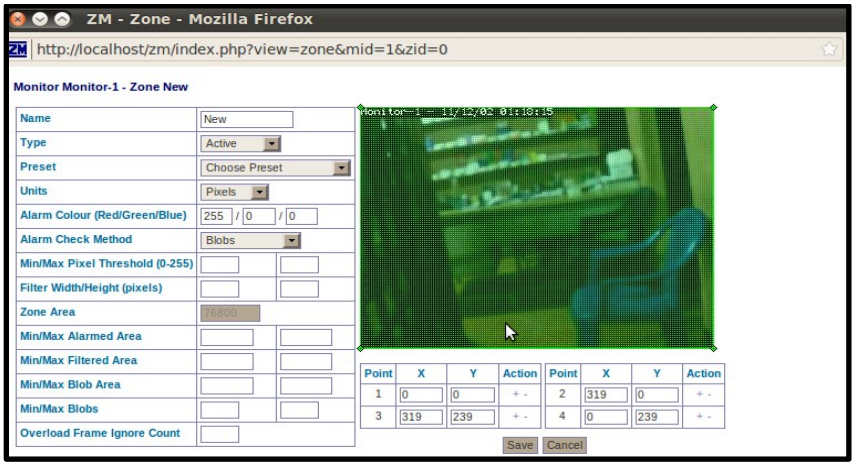


Figura 53. Definición de zonas.

La pantalla de características de cada Zona está dividida en dos áreas principales, a la izquierda está el área de opciones y a la derecha el área de dibujo. El área de la Zona puede ser definida completando la tabla de coordenadas o haciendo click en las esquinas de la Zona y haciendo click en su nueva ubicación. Para añadir nuevos puntos de dibujo utilizamos el signo "+" colocado al lado del punto detrás del que queremos añadir el nuevo punto. El símbolo "-" sirve para eliminar puntos y la "x" permite deseleccionar puntos.

Una vez que hemos seleccionado el tamaño y forma correctos para la zona, debemos rellenar el resto de la configuración. Las opciones son las siguientes:

Name: Se trata simplemente de la etiqueta con la que identificaremos la zona.

Type: Este es uno de los conceptos más importantes dentro de ZoneMinder. Tenemos cinco opciones entre las que elegir:

- **Active:** Es el tipo de zona más utilizada. Esta zona activará una alarma ante cualquier evento que ocurra en su interior y que cumpla un cierto criterio.

- **Inclusive:** Este tipo de zona se utiliza si queremos activar una alarma solo si al menos otra Zona Activa ha desencadenado ya otra alarma.
- **Exclusive:** En este caso las alarmas solo se activarán si no se activado ya una alarma de otra Zona Activa.

- **Preclusive:** Es relativamente reciente. Este tipo de Zona asegura que una alarma no se generará ante un evento en esta región de la imagen. Se utiliza para evitar que se generen alarmas ante cambios de luz que no se pueden excluir utilizando valores generales como número de pixeles de alarma, frames de alarma etc.

- **Inactive:** Es el tipo opuesto a Active. Nunca se generará una alarma en esta zona.

Es importante mencionar que se debe intentar superponer Zonas, lo que generaría una sobrecarga de procesamiento innecesaria.

Presets: Es una lista de características típicas. Seleccionar una rellenará algunos de los siguientes campos y nos ayudará a seleccionar los valores adecuados para nuestra zona.

Units: Indica si alguna de las siguientes características están expresadas en pixeles o porcentaje. El porcentaje se refiere respecto al área seleccionada, no a la imagen completa. En general las medidas en pixeles son más precisas, aunque más difíciles de utilizar.

Alarm Colour: Especifica el color con el que queremos marcar la zona de la imagen que ha generado la alarma.

Alarm Check Method: Se utiliza para especificar qué tipo de pruebas se aplican para determinar si un Frame representa una alarma o no. "*AlarmPixels*" indica que se realiza una cuenta individual de los pixeles activados. "*FilteredPixels*" indica que los pixeles serán filtrados para eliminar los elementos aislados antes de contarlos. "Blobs" utiliza un algoritmo más sofisticado de análisis que agrupa pixeles activados en grupos continuos o "blobs". Este último método es el elegido por defecto ya que es mucho más preciso.

Min/Maximum Pixel Threshold: Se utiliza para definir límites para los valores de los pixeles de una imagen y los predecesores de la imagen de referencia para decidir si se genera un evento.

Filter Width/Height: Para mejorar la detección de un evento válido en ZoneMinder se aplica otras funciones a los datos. La primera de estas funciones es un filtro que elimina todos los pixeles que no participan en un bloque continuo de cierto tamaño. Esta opción siempre se expresa en pixel y debe ser realmente pequeña y un número impar. Tres o cinco es un buen valor inicial.

Zone Área: Este campo no tiene por qué ser rellenado, es simplemente una referencia útil cuando se trabaja en pixeles del área seleccionada.

Min/Maximum Alarmed Área: Estos valores definen el mínimo y máximo número de pixeles que, si exceden su umbral, generarán una alarma. Si las unidades

están expresadas en porcentaje esta y las siguientes opciones se referirán al porcentaje de la imagen, no de la Zona. En general un valor de cero hace que la variable sea ignorada.

Min/Maximun Filtered Área: Son dos valores adicionales que especifican el límite de pixeles que causarán una alarma después del proceso de filtrado. No tiene sentido que esta área sea mayor que la "Alarmed Área".

Min/ Maximun Blob Área: En la fase de análisis los pixeles que generan alarmas se agrupan en conjunto o Blobs. Estos conjuntos pueden tener cualquier forma y cualquier tamaño. Esta variable nos permite definir el tamaño del blob que generará una alarma.

Min/ Maximum Blobs: Especifica los límites para el número de blobs detectados.

La configuración que hemos elegido cómo más óptima después de una multitud de ensayos ha sido la siguiente:

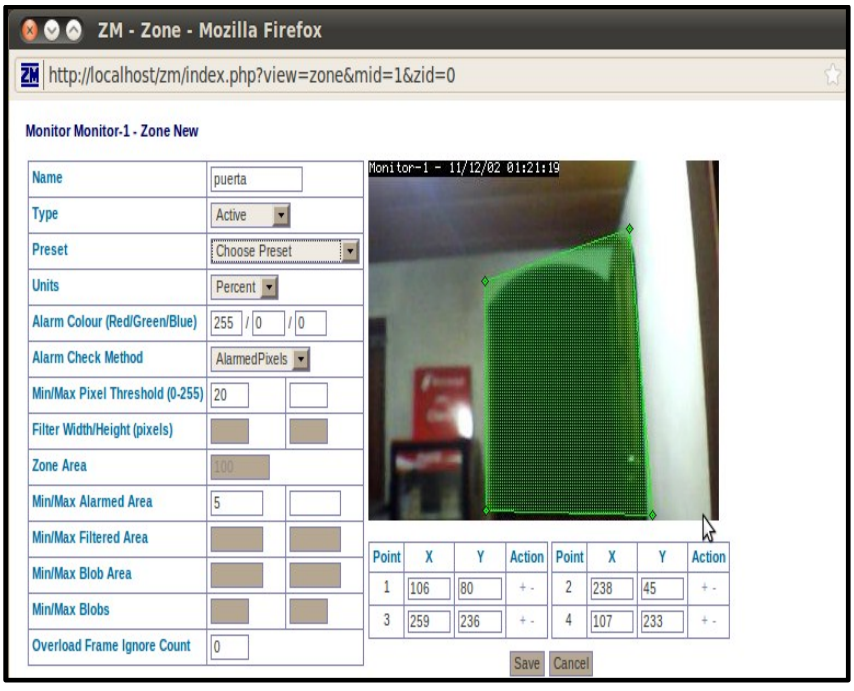


Figura 54. Configuración de Zonas

Visualización de monitores

Llegados a este punto ya deberíamos tener uno o varios monitores con una o varias Zonas cada uno. De vuelta a la ventana principal veremos una lista con monitores. Haciendo clic en un monitor concreto se nos mostrará una nueva ventana con una imagen en vivo de ese monitor y una lista de los últimos eventos capturados.

En el encabezado de esta nueva ventana también se nos permite seleccionar otras opciones como por ejemplo si deseamos ver un Streaming de vídeo o stills (secuencias de imágenes estáticas). También se nos permite cambiar la escala del vídeo, modificar las características de la imagen en dispositivos locales o cerrar la ventana.

Por defecto, si se ha minimizado la ventana, ante una alarma esta saltará a primer plano. Es posible también configurar sonidos para avisar de los eventos.
Bajo el estatus se encuentra una lista de eventos recientes, por defecto los diez últimos, pero haciendo clic en "All" se nos dará la lista completa, y en "Archive" se muestra una lista de los eventos archivados de este monitor. Haciendo clic en el encabezado de cualquier columna se ordenaran los eventos siguiendo ese criterio.

Desde aquí se puede borrar los eventos. Cada evento viene caracterizado por un Id, un nombre, el momento en el que ocurrió, la longitud del evento (incluyendo frames anteriores y posteriores), el número de frames que comprende el evento, el número de frames que contienen alarma, y finalmente una puntuación.

También es posible visualizar todos los monitores de la instalación de forma secuencial o al mismo tiempo seleccionando desde la ventana principal "Cycle" o "Montaje" respectivamente.

Filtrado de eventos

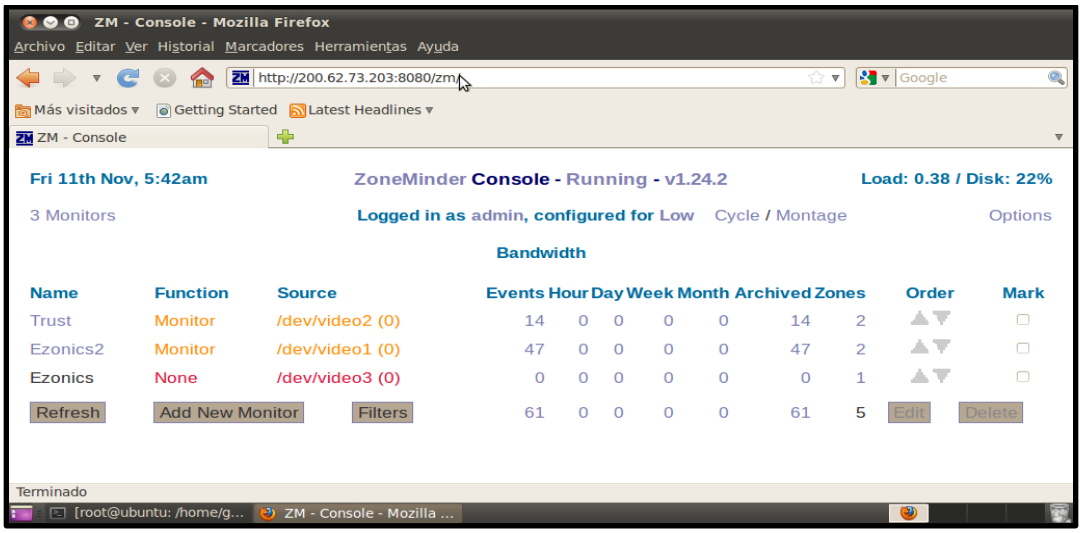


Figura 55. Registros de eventos.

Las otras columnas de la ventana principal contienen otros datos tales como la hora, día, semana y mes de los últimos eventos, así como el total de los eventos archivados. Al hacer click en cualquiera de los totales, en "All", o en "Archive" se muestra una nueva ventana con una lista de todos los eventos de acuerdo con un filtro. Por ejemplo si se hace click en el total de la columna "Archive" se muestra todos los eventos archivados.

En esta nueva ventana se debe hacer click en "Create New Filter", lo que permitirá crear un nuevo filtro o modificar los existentes.

Filtrar es realmente simple; lo primero que hay que hacer es seleccionar cuantas expresiones se van a utilizar. A continuación se selecciona lo que se quiere filtrar y de qué manera, incluyendo además una relación entre las cadenas de filtrado ("and" u "or").

Existen varios elementos diferentes relacionados con un evento que pueden ayudar a filtrar; por ejemplo la fecha, el número de pixeles con alarma, el score.

Si se hace click en "Save" el siguiente cuadro de dialogo se puede especificar las acciones a llevar a cabo ante un evento que cumpla este criterio de filtrado, tales como archivar el archivo de vídeo, enviar un e-mail, etc.

Figura 56. Creación de los filtros.

En este caso se creó un filtro que ante un evento con más de 10 frames de alarma realizará las siguientes acciones:

- Archivar los eventos.
- Generar un video para ellos.
- Enviar un email con los detalles y un link del video que se guardó tras la alarma (Configurado en el menú "options/email" de la ventana principal).

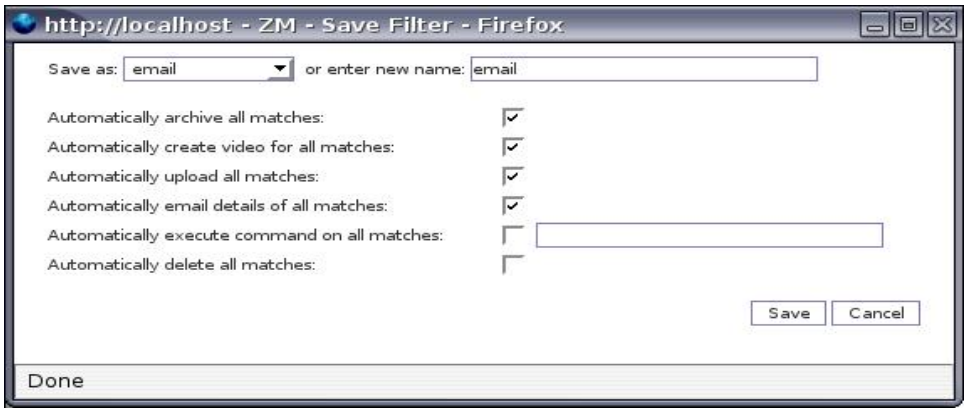


Figura 57. Definición de filtros.

Almacenamiento de eventos.

El tamaño del video dependerá del formato en que se realice la captura de los eventos puede ser en mpg, mpeg, wmv, avi, 3gp. La mejor calidad de video se obtiene mediante el formato avi. Esto equivale a 1.6 GB por cada hora de grabación continua.

Esto se obtuvo al realizar 1 hora de grabación continua almacenando la información en un disco duro de 80 GB, el cual se ocupo un 2% de su capacidad en ese tiempo.

A través de una regla de tres se hace el cálculo:

80 GB = 100 % X= (80GB*2%) / 100%
X GB = 2% X= 1.6 GB

Por lo tanto 24h de grabación continua equivale a 38.4 GB en formato AVI.

Existe otra forma de calcular el almacenamiento de los datos pero para esto se debe de calcular el ancho de banda consumido por cada cámara.

AB= Tamaño de la imagen x fps x canales.
AB (Panasonic) = 9Kb x 15 fps x 1
AB (Panasonic) = 135 Kps

AB= Tamaño de la imagen x fps x canales.
AB (Ezonics) = 10.6 x 30 fps x 1
AB (Ezonics) = 318 Kps

AB= Tamaño de la imagen x fps x canales.
AB (Klip) = 13 x 30 fps x 1
AB (Klip) = 390 Kps

Una vez que sea calculado el ancho de banda obtenemos los bytes por segundo. Este valor se debe de multiplicar por el tiempo que se grabará de forma continua (24 h) y se debe sumar un margen de 10 % de sobrecarga debido al sistema de archivo, la fórmula es la siguiente:

HDD= (AB x 60 s x 60 min x Tg) + 10%
HDD= (390 Kbps x 60 s x 60 min x 24 h) + 3.29
HDD= 32.90 GB + 3.29
HDD = 36.19 GB

De esta forma se puede observar que los datos de la formula son similares a los resultados reales obtenidos, según la regla de tres explicada anteriormente.

Para evitar que se llene el disco interminablemente de los eventos, en la pantalla inicial de la consola de ZoneMinder se debe escoger cualquier enlace de eventos (Hour, Day, Week, Month, etc). Se debe seleccionar la opción "Show Filter Windows" en la parte superior, se habilita en la lista desplegable superior "choose Filter" la opción **"Purgewhenfull**". Adicionalmente se selecciona la opción que se desea tomar cuando este al porcentaje deseado (Eliminar, Ejecutar, crear, etc).

3.4.2.3 Opciones avanzadas de ZoneMinder.

Una de las funciones que definimos en el filtro es enviar un correo electrónico al usuario con los detalles de los eventos que produjeron tras una alerta o alarma en el sistema de vigilancia, para esto se deben de rellenar algunos datos en el ZoneMinder lo hacemos mediante **Options>Email** (véase la figura 58).

Entre los datos más importantes que se deben de rellenar en esta pestaña son: El correo electrónico del usuario, la dirección de salida de correo del ISP de internet (Turbonett) la cual es *mail1.turbonett.com.ni* y la dirección IP donde se encuentra instalado la interfaz del ZoneMinder (200.62.73.203/ZM).

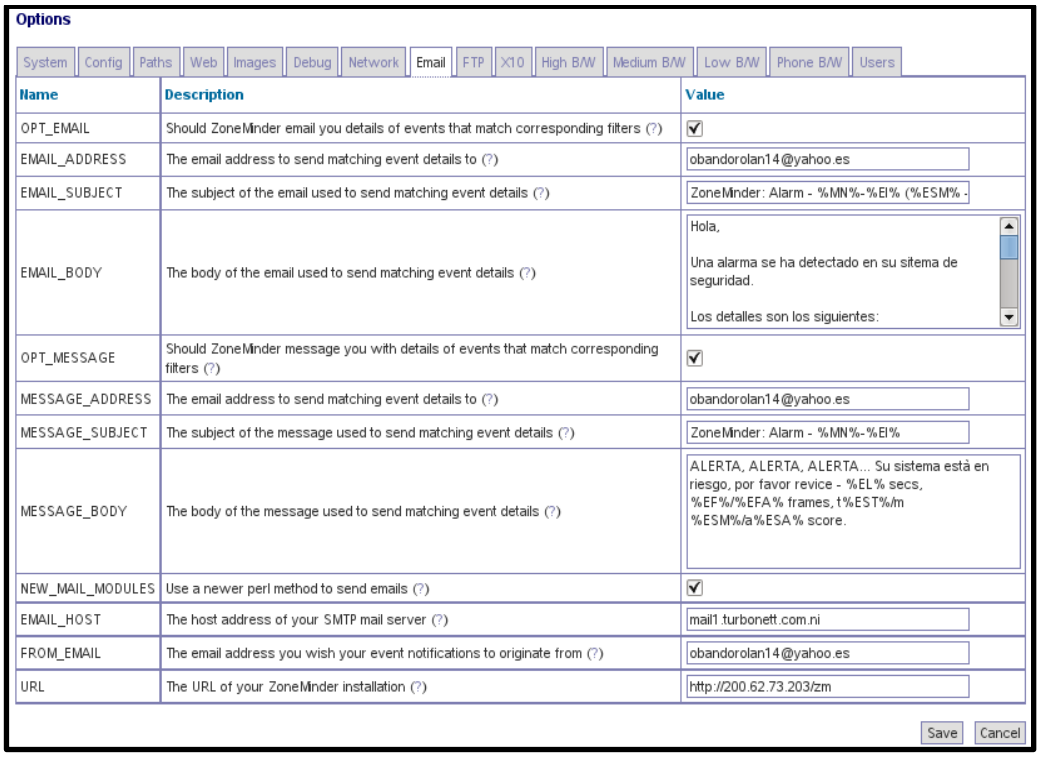


Figura 58. Configuración para envió de correo electrónico.

Para hacer el sistema más eficiente lo recomendable es agregar un tono alarma, esto se hace ubicando el archivo de sonido en usr/share/zoneminder/sounds y se debe declarar en **Options>Web>WEB_ALARM_SOUNDS>Nombre del archivo de sonido** (véase 59).

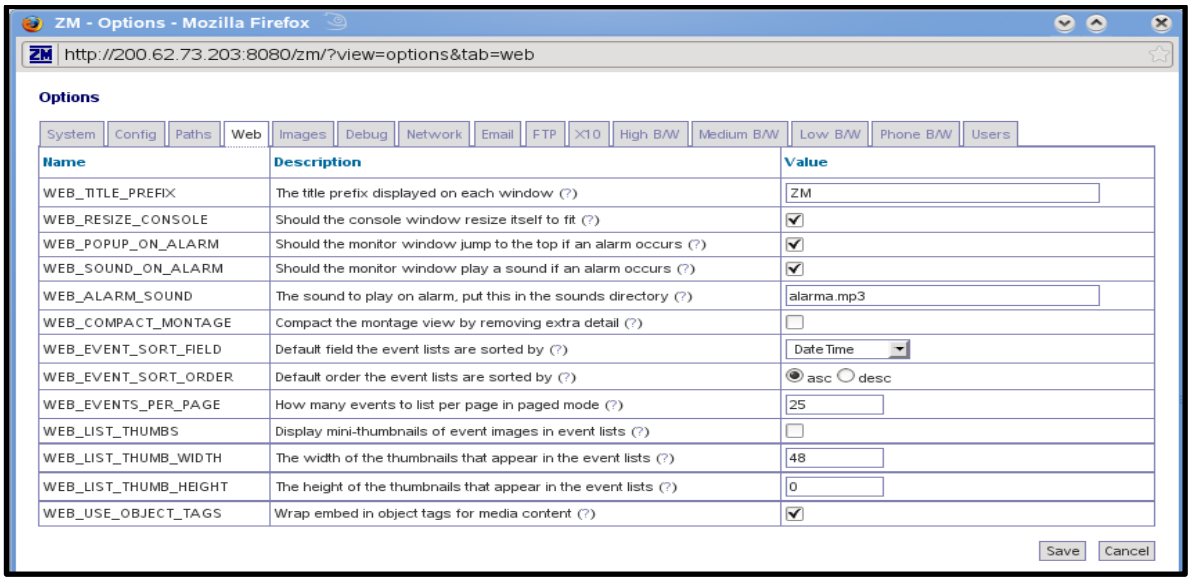


Figura 59. Configuración de tono de alarma.

3.4.2.4 Exportación de la interfaz del ZoneMinder al sitio Web Electronicsecurity.

El ZoneMinder cuenta con una interfaz Web independiente, para hacer que esta interfaz sea parte del sitio Web, utilizamos un módulo de Joomla llamado Wrapper el cual permite visualizar páginas Web externas dentro del propio sitio creado en Joomla. Estas páginas externas se muestran mediante un IFrame (marco en línea), insertado en el área de contenido del módulo. A continuación explicaremos como lo utilizamos.

1. Se accede a Joomla a través de un navegador digitando la URL de la página web más /administrator ejemplo: www.electronicsecurity.com:8081/administrator.
2. Una vez cargada la interfaz se accede a Menú>topmenu>Inicio (véase Figura 60), topmenu es el nombre que se le asignó al menú principal e Inicio es el nombre del primer botón del menú y que cargara automáticamente cuando se acceda a la web.

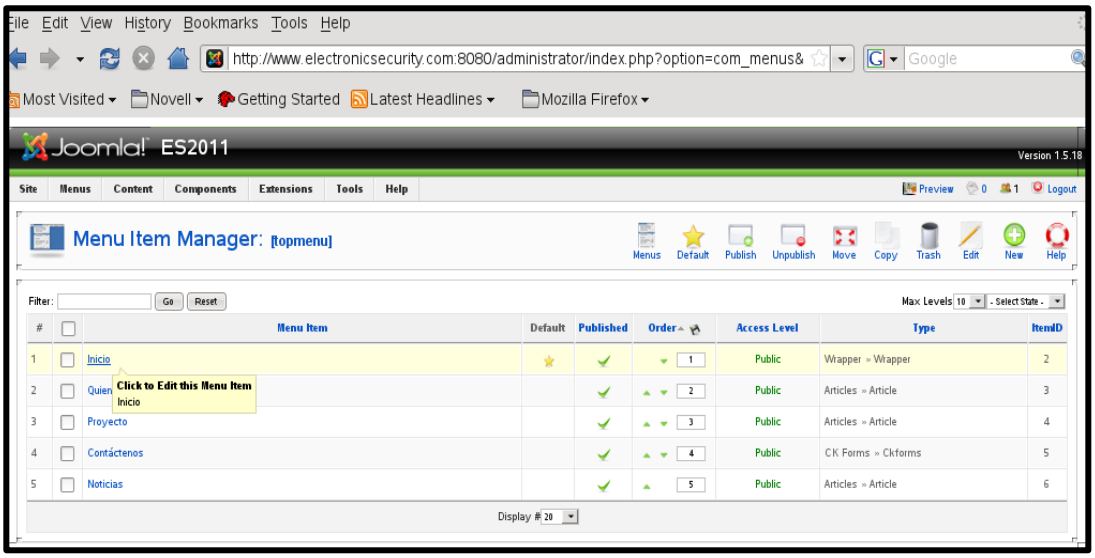


Figura 60. Opciones de menú de Joomla.

3. Una vez dentro de la configuración del botón inicio se debe especificar la función de este la cual será mostrar la interfaz del ZoneMinder en el

contenido de la Web. Esto será posible a través del módulo Wrapper dando clic en botón Change Type y se selecciona de la lista de opciones Wrapper (véase figura 61).

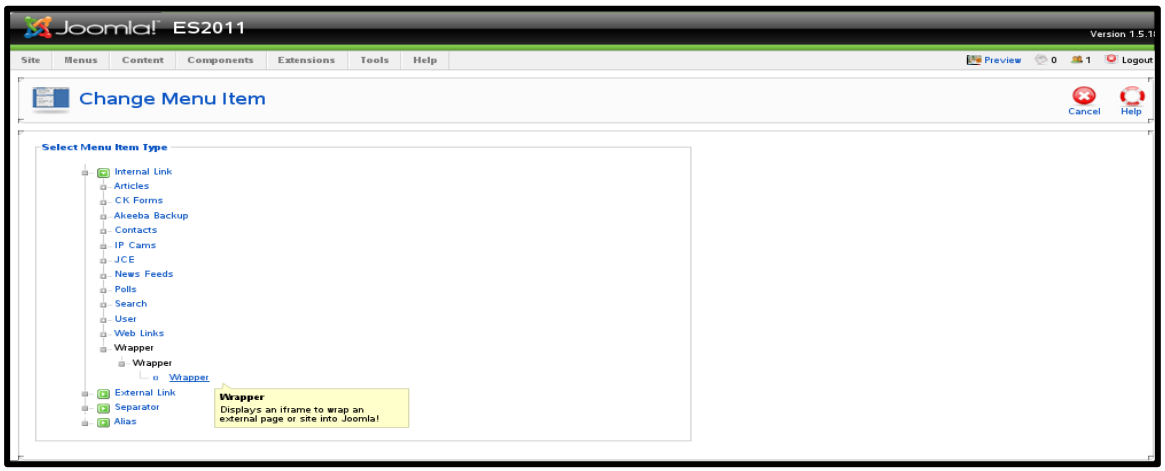


Figura 61. Cambio del tipo de menú de Joomla

4. Una vez seleccionado la opción Wrapper simplemente se edita la dirección URL de la Web de ZoneMinder en este caso es la www.electronicsecurity.com:8080/zm 0 200.62.73.203:8080/zm (véase figura 62).

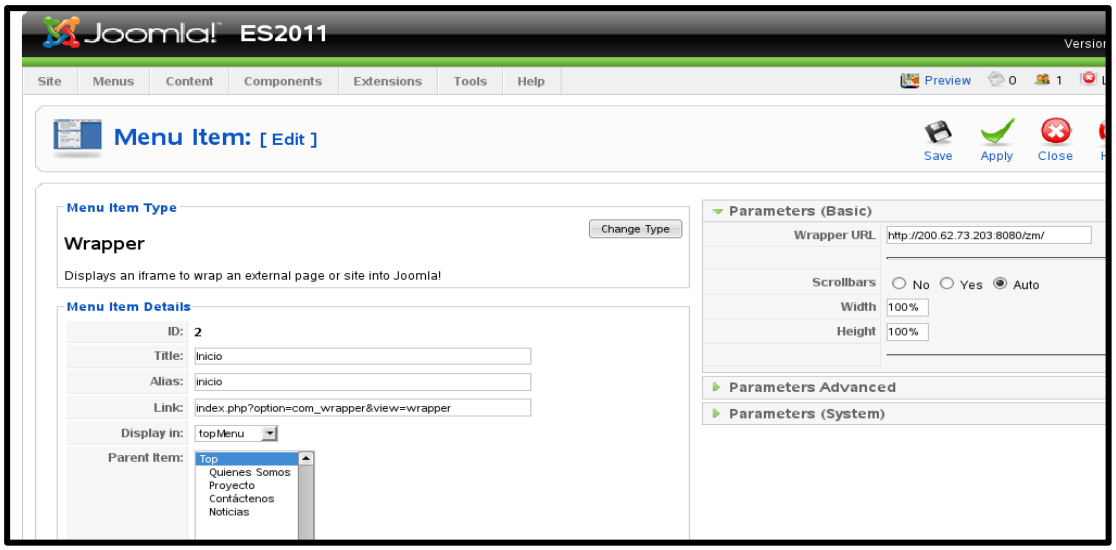


Figura 62. Opciones de Wrapper.

El resultado es el siguiente:

Figura 63. Interfaz web del ZoneMinder adherida a la Web.

3.4.3 Enrutamiento (NAT)

Es un Traductor de dirección de Redes, que permite traducir una IP privada de una red en una IP pública, para que esta pueda enviar paquetes al exterior (internet), y una vez que esta obtenga una respuesta la IP publica se re direccionará a la IP privada para que esta pueda recibirlo.

Debido a que uno de los objetivos del proyecto es permitir que los usuarios se conecten al sistema de forma remota se utiliza una IP publica 200.62.73.203 la cual debe re direccionarse a la IP privada de cada hosts 192.168.1.64 que es el servidor SLES donde se tienen alojados los servicios DNS y Web. Además se cuenta con un servidor Web instalado en Notebook con S.O Ubuntu que aloja la interfaz del ZoneMinder con una IP 192.168.1.65. El tipo de NAT utilizado es con sobrecarga ya que solo cuenta con una dirección IP públicas para re direccionar a distintas IP privada. Estas configuraciones se deben hacer en el Router, se utilizó un Router Thomson TG585 v7 ADSL (Figura 64). Aquí se debe definir los protocolos de transmisión de datos y los puertos de entrada y Salida.

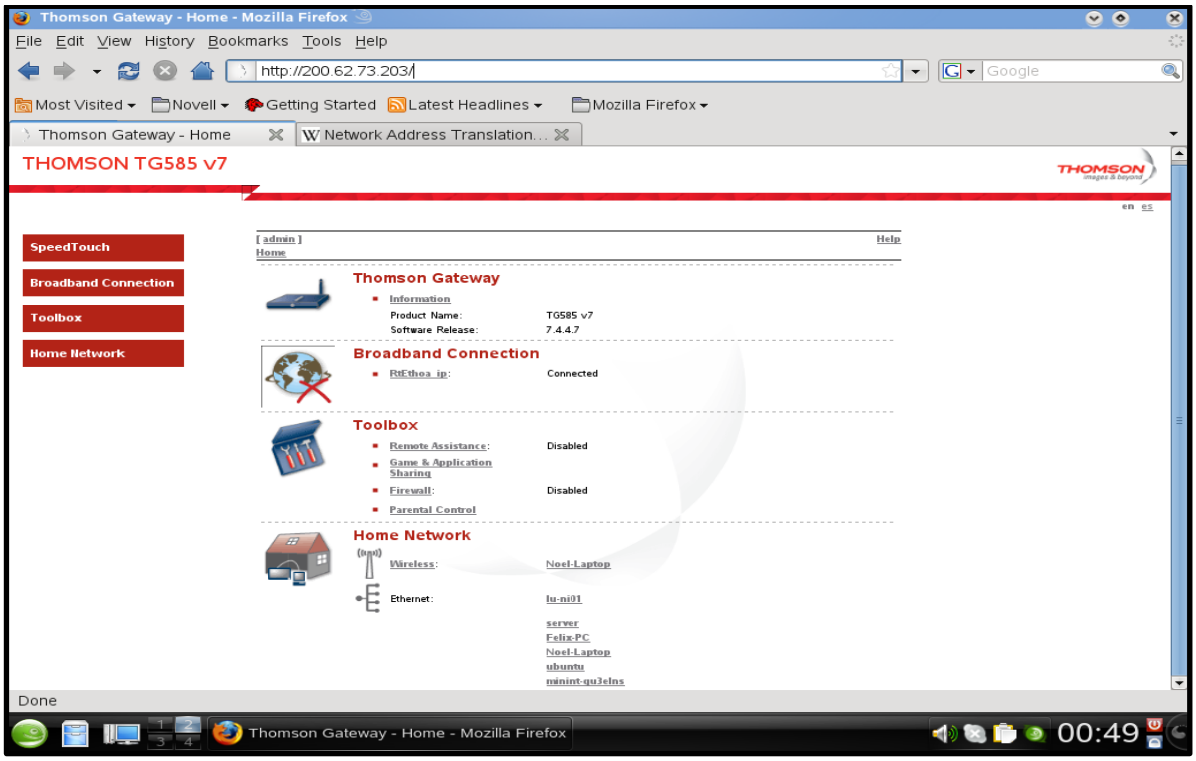


Figura 64. Interfaz del Router Thomson.

En la lista señalada en la figura anterior se puede observar el nombre de cada hosts conectados a la red doméstica, dando click en cada uno de ellos se visualiza información general (véase Figura 65), como por ejemplo su IP. En este caso, interesa únicamente server (SLES 11.0) y Ubuntu (10.04).

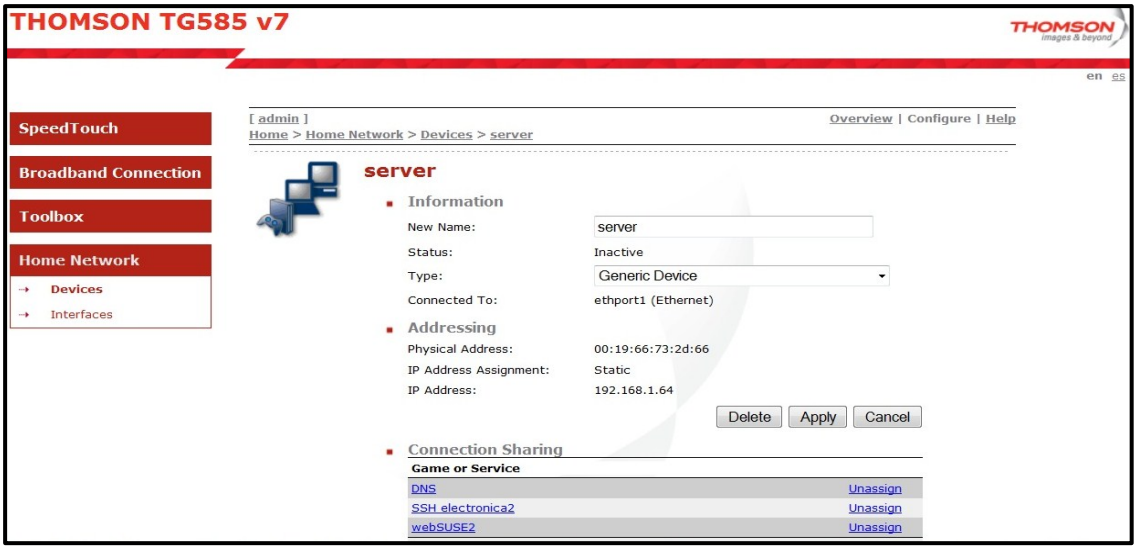


Figura 65. Especificaciones de cada equipo conectado.

Lo siguiente será asignar a cada hosts los protocolos de comunicación con que trabaja cada servicio configurado en el servidor. Para el servidor SLES se define los protocolos TCP/UDP que utilizara el servidor DNS a través del puerto 53 (véase Figura 66) y en el caso del servicio SSH se utiliza el protocolo TCP definiendo el puerto 24, debido a que el puerto 22 que originalmente trabaja SSH está siendo utilizado por otro host (véase Figura 67).

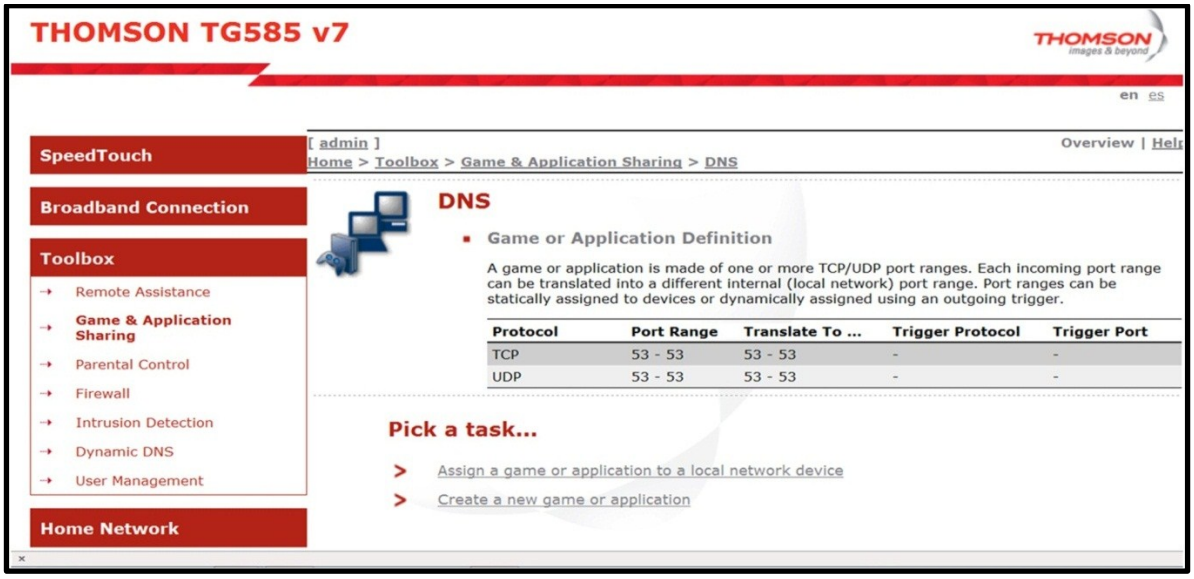


Figura 66. Definiciones de los protocolos de enrutamiento.

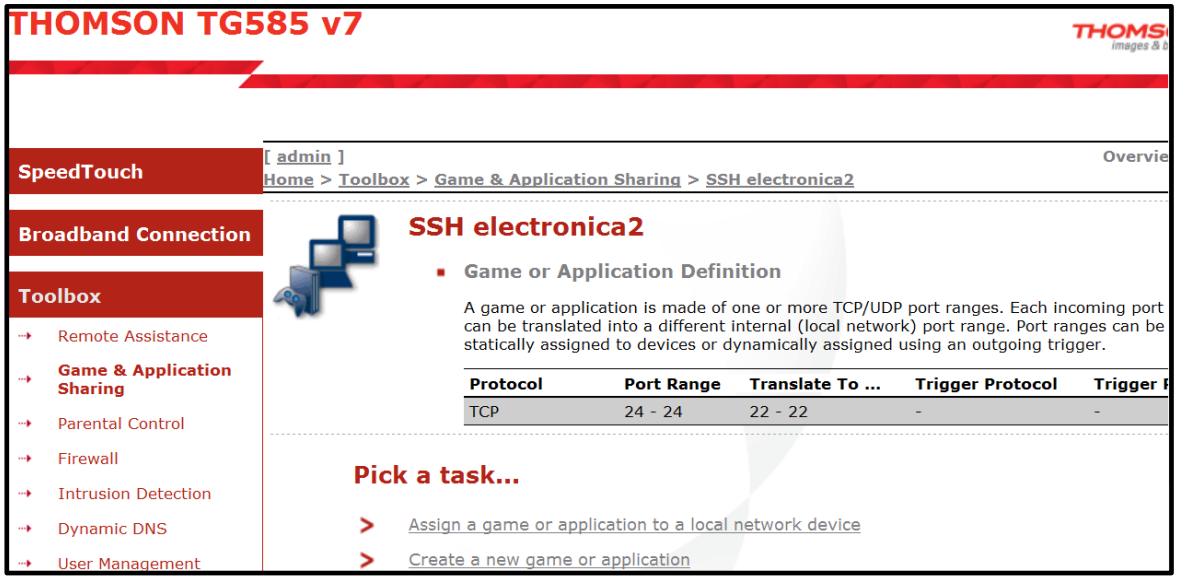


Figura 67. Definición de puerto para SSH

En el caso del host con Ubuntu se definió el protocolo TCP (véase Figura 68) para la interfaz Web del ZoneMinder utilizando el puerto 8080 debido a que el puerto 80 está siendo ocupado por el servicio ISP. A pesar de que se han establecidos puertos virtuales (24 y 8080), el traductor de dirección de redes se encargara de direccionar las solicitudes de estos puertos a los originales (22, 80).

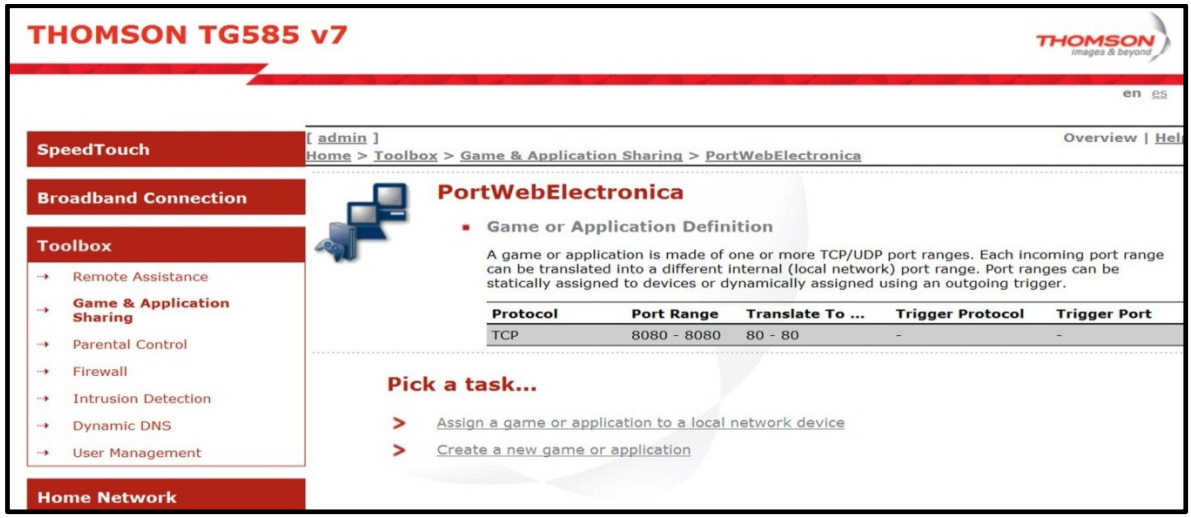


Figura 68. Asignación del puerto 8080

Si se necesita modificar, definir nuevos protocolos y puertos se puede hacer a través de la opción ***Assign a game or application to a local network device*** presente en el Router y señalado en la figura anterior.

3.5 Normas, política y medidas de seguridad

Debido a la inseguridad de internet se decidió realizar ciertas restricciones al ingresar al sistema por medio del navegador de preferencia, las cuales son:

1. El acceso a la web es restringido solamente el usuario y administrador conocerán el usuario y la contraseña de entrada a la Web.

2. De la misma manera el acceso al software de seguridad ZoneMinder se encuentra restringido. En Options>User el administrador podrá definir diferentes usuarios con privilegios. Cada cliente de nuestro sistema tendrá asignado un usuario y contraseña con la cual podrá tener acceso únicamente a las cámaras ubicadas en su propiedad, teniendo permisos solo de visualización. Solo el administrador tendrá acceso a todas las cámaras agregadas en el sistema y podrá hacer modificaciones necesarias para el buen funcionamiento del sistema.

3. El acceso al administrador de contenidos Joomla será exclusivo para el administrador del sistema en caso que se deben realizar mejorar o modificaciones en la página Web.

3.5.1 Creación de permisos a usuarios y mantenimiento del sistema

Desde la ventana principal se puede acceder a la etiqueta "Option", esta permite modificar la mayoría de las opciones de configuración de ZoneMinder.

Una de las opciones más utilizadas y que viene desactivada por defecto, es la opción de usuarios. Dentro de la etiqueta "System" si se activa la casilla ZM_OPT_USE_AUTH, se creará una nueva pestaña llamada "Users" que permitirá definir usuarios y sus privilegios (véase la figura 69).

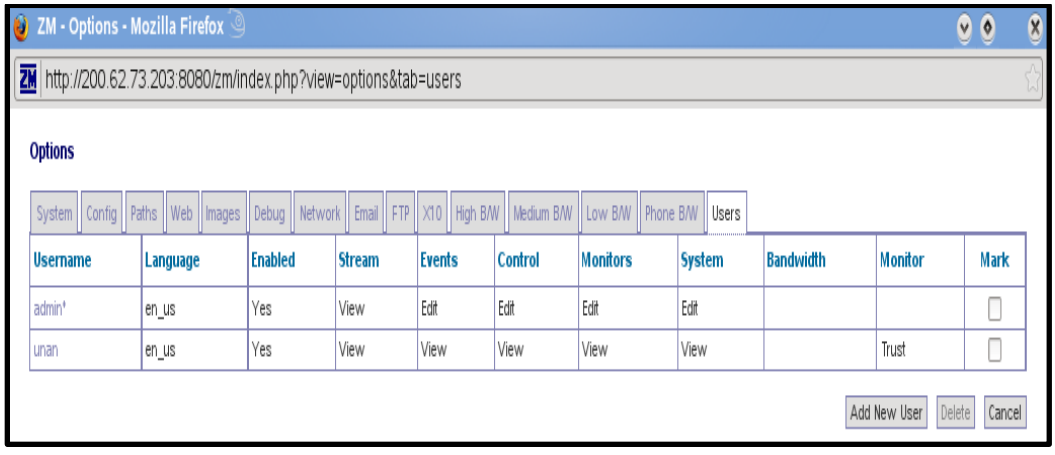


Figura 69. Opciones para definición de usuarios en ZoneMinder.

Para crear y administrar nuevas cuentas se debe abrir la ventana Add New User. La interfaz que permite crear y modificar nuevas cuentas de usuarios se indica un la figura siguiente (véase figura 70).

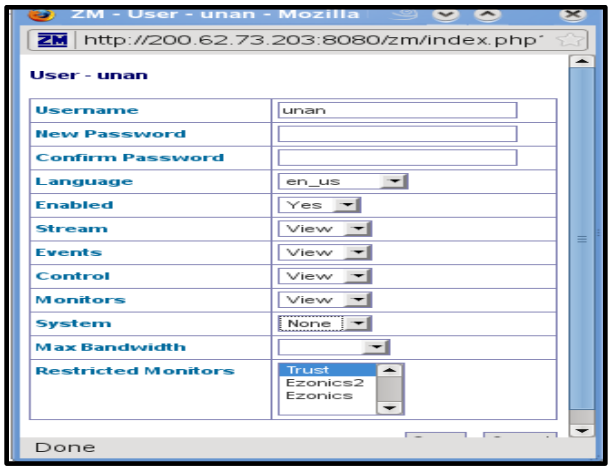


Figura 70. Asignación de privilegios a usuarios.

La ventana Add New User permite crear una infinidad de usuarios asignándoles diferentes niveles de acceso definidos por cada uno de los campos presentados continuación:

- **Language:** Este campo permite escoger el idioma de la interfaz Web.
- **Enabled:** Permite o niega habilitar dicha cuenta.
- **Stream:** Permite o niega la visualización del video.
- **Events:** Permite o niega el acceso a los eventos guardados.
- **Monitors:** Permite o niega la edición de monitores.
- **System:** Permite o niega el acceso a configuraciones avanzadas de ZoneMinder.
- **Max Bandwidth:** Permite asignar el ancho de banda con el que se conectaran los usuarios remotos.

De acuerdo a las pruebas realizadas en distintos lugares con diferentes anchos de banda se ha comprobado que se necesita un mínimo de 1 Mbps para obtener una visualización óptima de video del sistema de vigilancia al estar varios usuarios

conectados simultáneamente, ya que en las pruebas realizadas con un ancho de banda de 128, 256 y 512 Kbps no fue posible obtener una correcta visualización.

- **Restricted Monitors:** Niega la visualización de los monitores seleccionados.

3.5.2 Mantenimiento del sistema

El mantenimiento se abordara en dos aspectos principales: El mantenimiento a Software y mantenimiento al Hardware.

Software: Este se hará de forma remota por medio SSH Secure Shell Client ya que se ha definido en las configuraciones realizadas en el SLES 11.0. Y Ubuntu 10.04. Donde el administrador podrá realizar actualizaciones, instalación de dependencia, extracción de eventos, cambios de usuarios o eliminación, de una forma segura ya que en SSH toda la información que viaja sobre él es de manera encriptada.

Hardware: En este caso se harán visitas mensuales para dar mantenimientos a los equipos que conformas el sistema de vigilancia y seguridad, en caso de fallos eléctricos se dará una opción adicional al sistema que consiste en un sistema de alimentación basado en inversores y bancos de baterías de almacenamiento.

3.6 Funcionamiento del sistema de vigilancia.

El funcionamiento del sistema de vigilancia y seguridad depende del buen desempeño de cada uno de los dispositivos, software y protocolos que lo integran. Para representar el proceso que se lleva a cabo una vez que el usuario acceda al sistema, ya sea de forma remota o local está representado en el siguiente diagrama.

En este diagrama se explica de la forma más sencilla el conjunto de aplicaciones y la

interacción usuario-servidor, además de la respuesta del sistema a las solicitudes de datos hechas por los usuarios. (Véase figura 71).

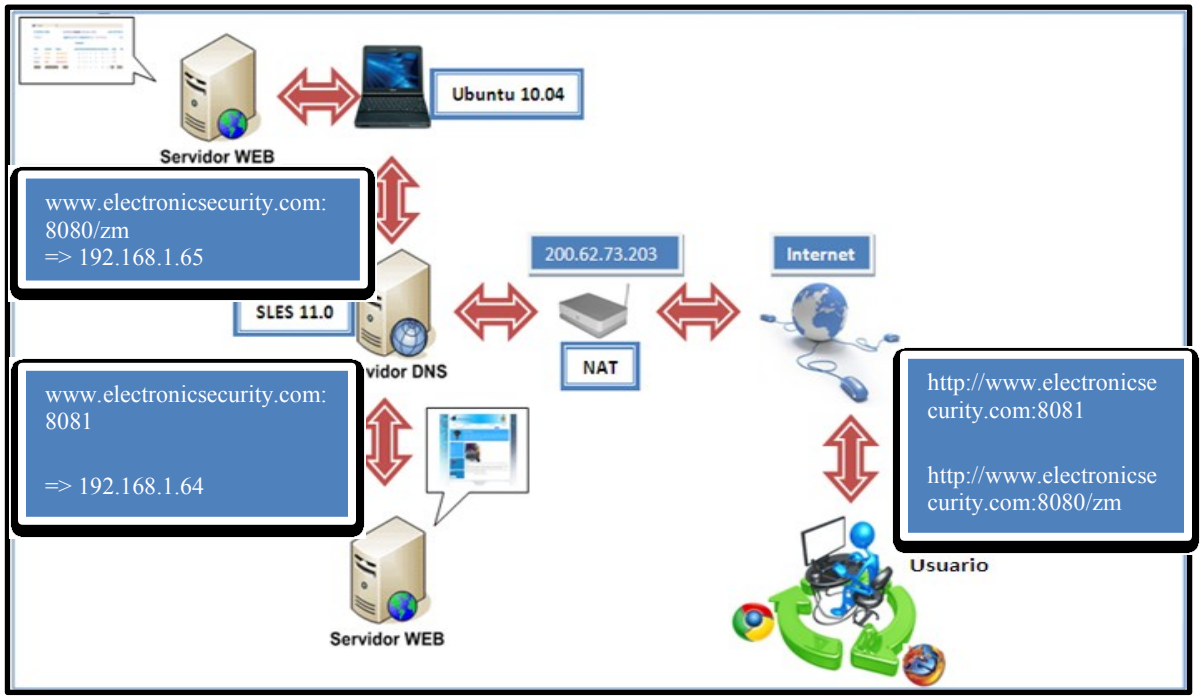


Figura 71. Funcionamiento del sistema de vigilancia.

Los componentes principales del sistema de vigilancia son: Servidor DNS, Web, SSH y el software de vigilancia ZoneMinder, ya que este último nos permitirá la visualización, captura y tratamiento de imágenes y videos provenientes de las cámaras.

Los usuarios generalmente no se comunican directamente con el servidor DNS: la resolución de nombres se hace de forma transparente por las aplicaciones del cliente (por ejemplo, navegadores, clientes de correo y otras aplicaciones que usan Internet). Al realizar una petición que requiere una búsqueda de DNS, la petición se envía al servidor DNS local del sistema operativo. El sistema operativo, antes de establecer alguna comunicación, comprueba si la respuesta se encuentra en la memoria caché. En el caso de que no se encuentre, la petición se enviará a uno o más servidores DNS.

La mayoría de usuarios domésticos utilizan como servidor DNS el proporcionado por el proveedor de servicios de Internet. La dirección de estos servidores puede ser configurada de forma manual o automática mediante DHCP. En otros casos, los administradores de red tienen configurados sus propios servidores DNS.

En cualquier caso, los servidores DNS que reciben la petición, buscan en primer lugar si disponen de la respuesta en la memoria caché. Si es así, sirven la respuesta; en caso contrario, iniciarían la búsqueda de manera recursiva. Una vez encontrada la respuesta, el servidor DNS guardará el resultado en su memoria caché para futuros usos y devuelve el resultado.

Una vez que la solicitud llegue al Router este la re direccionará al servidor DNS local, donde tenemos declarada esta dirección URL en el archivo de registro de configuración de la zona ubicado en var/lib/named/master/electronic.dat. Para que este enrutamiento sea posible se deben declarar en el Router los protocolos que permiten esta trasmisión de datos (TCP/UDP), mediante un NAT.

El TCP es la capa intermedia entre el protocolo de internet IP y la aplicación. Habitualmente las aplicaciones necesitan que las comunicaciones sean fiable, TCP añade la funciones necesarias para prestar un servicio que permita que la comunicaciones entre dos sistemas se efectué libre de errores, sin perdida y con seguridad. El protocolo UDP nos permitirá la transmisión de video y voz a través de la red.

El servidor Web nos permite el alojamiento de la página Web, esta se programó en lenguajes como: HTML, CSS, XML y PHP. Debido a que se configuraron dos servidores Web (SLES para sitio Web y Ubuntu para ZoneMinder) el usuario tenía que digitalizar dos direcciones URL www.electronicsecurity.com:8081/ para cargar el sitio Web y www.electronicsecurity.com:8080/zm para la interfaz de ZoneMinder, se dio solución a este inconveniente mediante el gestor de contenidos

Joomla que permite incorporar un sitio web exterior a cualquier página web creada en él.

La página Web permite al usuario visualizar el video proveniente de las cámaras de forma simultánea así como los eventos que se generen o estén archivados, estos eventos se encuentran almacenados en /usr/share/zoneminder/video, pero el ZoneMinder nos permite archivar nuestros datos de manera remota al configurar un servidor FTP, el cual es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP.

Además en el caso que el usuario este fuera de su domicilio recibirá notificaciones de alertas y alarmas generadas en el sistema a su correo electrónico a través de la configuración en el ZoneMinder del servidor SMTP (Protocolo simple de transferencia de correo), provisto por su proveedor de servicios de internet.

De lo contrario se ha incorporado al sistema un sonido de alerta, el cual dará aviso al usuario en caso de violaciones a las zonas protegidas por las cámaras. Este sonido podrá ser escuchado solo de forma local y si el usuario esta de forma remota dentro de la visualización del monitor el software le accionara alertas en color (Anaranjado) y alarmas (Rojo), así podrá darse cuenta que hubo una violación al sistema.

El mantenimiento al sistema será de forma remota vía SSH (véase figura 72), exclusivo para el administrador del sistema en caso de modificaciones, actualizaciones, extracción de datos, este tendrá que tener en su ordenador instalado el programa Secure Shell Client para Windows u Openssh Server para Linux.

En el Router se debe definir este protocolo para que el administrador pueda accesar al sistema de forma remota, esto se hace mediante el traductor dirección de red donde especificamos el protocolo y el puerto de transmisión.

SSH evita muchos de los ataques más habituales, en los que los datos se ven comprometidos e incluso la seguridad de la red. Uno de los riesgos que evita, es IP spoofing, donde un host remoto envía paquetes que pretenden venir de otro ordenador, el cual es de confianza. Esta suplantación de identidad es bastante peligrosa y SSH nos da una buena protección contra este método.

Aun hoy en día, se suele utilizar el protocolo de conexión entre ordenadores (o servidores), llamado telnet, el cual ha sido extremadamente útil y utilizado en los últimos años. El problema es que el nombre de usuario y la contraseña son enviados en texto claro por la red. Esto significa que si alguien en el medio de la red (entre tu ordenador y el ordenador destino), captura los datos con un sniffer (herramienta de captura de datos), puede conseguir el usuario y la contraseña para poderlos utilizar en el futuro.

SSH encripta estos datos según viajan de una máquina a la otra, por lo que si son capturados, no tendrán ningún sentido para el que ha conseguido esta información.

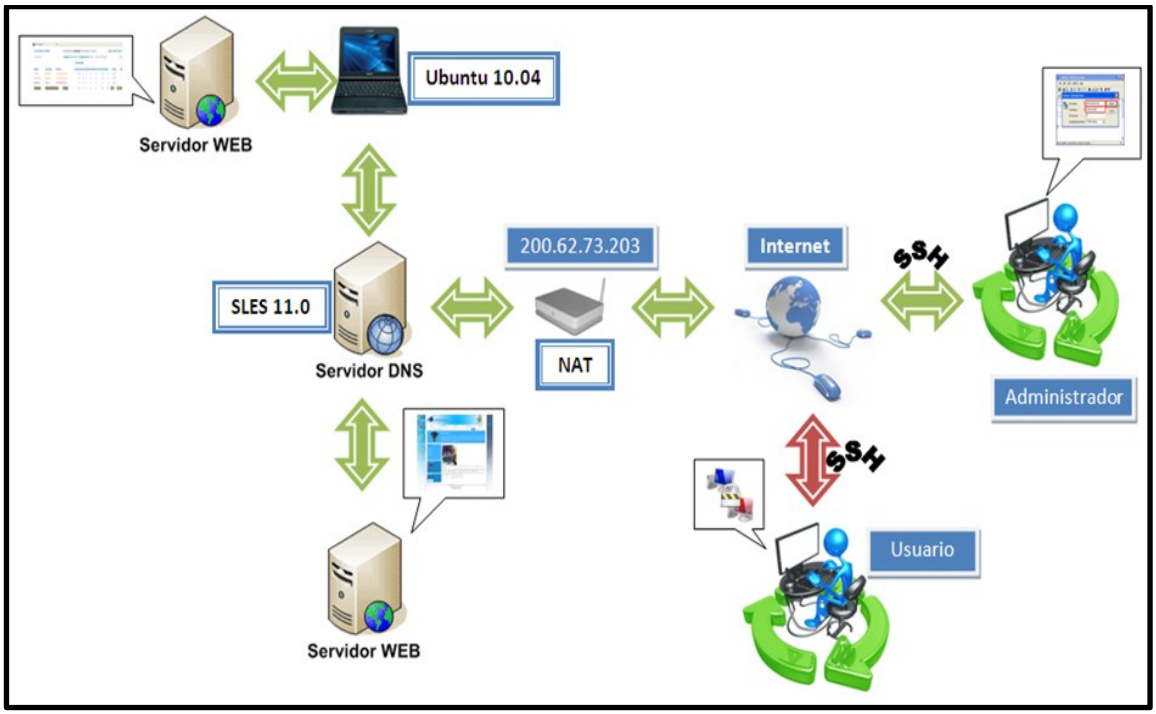


Figura 72. Diagrama de funcionamiento de SSH

3.7 Instalación de cámaras de seguridad.

Debido a que el costo de las cámaras IP es un poco alto, se empleó la utilización de 4 cámaras Web y una cámara IP. La desventaja de las cámaras web es su rango de captura y la falta de visión nocturna. Se utilizaron 2 cámaras Web Ezonics, y 2 cámara Klip Xtreme. La cámara IP es una Panasonic BL-C1A, seleccionada debido a que es uno de los modelos más sencillos y por consiguiente su costo es accesible.
Para agregarla al ZoneMinder debemos de rellenar los siguientes campos en la opción add monitor:

Remote Host Name: <user>:<pass>@<ip>
Remote Host Port: <port number>
Remote Host Path: /SnapshotJPEG?Resolution=320x240&Quality=Clarity
24 bit color Gutsy Gibbon - 7.10
Capture width: 320
Capture height: 240

Para todas las conexiones se utilizó cable UTP categoría 5e, en el caso de las cámaras Web se hicieron extensiones USB con cable UTP, ubicando en los extremos conectores USB hembra y macho, esto debido a que las distancias de las cámaras con respecto a las servidores son mayores a 5 m, el cual es el mínimo que se permite para conectar cables USB, además de su alto costo en comparación con el UTP.

A continuación se explica cómo crear las extensiones USB.

Material necesario

- Cable UTP categoría 5e.
- 1 conector USB hembra y 1 macho por cada cable que se desea alargar.
- Cautín y soldadura.

- Cinta negra

Procedimiento:

El cable/conector USB se compone de 4 pines, 2 para la corriente y 2 para los datos. El Pin 1 y 4 se usan para la corriente y el 2 y 3 para los datos como se muestra en la siguiente tabla:

Pin	Nombre	Color cable	Descripción
1	VCC	Rojo	+5v
2	D−	Blanco	Data −
3	D+	Verde	Data +
4	GND	Negro	Tierra

Tabla 3. Definición de pines de conectores USB

El cable UTP viene estructurado con 4 pares trenzados, diferenciándose por colores, se procedió a soldar cada par de hilos a cada pin de los conectores USB hembra y macho, según como se muestra e la siguiente tabla.

PIN USB	COLOR
1	Blanco-naranja-Naranja
2	Blanco-verde-verde
3	Blanco-azul-Azul
4	Blanco-café-Café

Tabla 4. Conexiones de conectores USB a cable UTP

Primeramente se corta un pedazo de funda termo táctil y se coloca dentro de cada extremo del cable. Luego se separan los cables del UTP y se pelan las puntas.

Luego se sueldan los cables en cada conector USB como se explicó anteriormente:

Figura 73. Conexiones UTP a USB

Luego se coloca la funda termo táctil en la parte del cable que está descubierto el cobre y se calienta para cubrirlo.

Para la instalación de la cámara IP se utilizó el software incluido Panasonic, para la asignación de una dirección IP, usuario y contraseña. Este proceso se hizo instalando el software en Windows 7, ya que no es compatible con ninguna distribución de Linux. El cableado se hizo con cable UTP, categoría 5e y conectores RJ-45 bajo la norma 568B.

3.8 Sistemas de alimentación contra falla de energía convencional (opcional).

En la actualidad, la energía eléctrica encara una creciente demanda. Esto ha ocasionado un aumento importante en las caídas de suministro y en los daños ocasionados por problemas eléctricos. Los problemas más frecuentes relacionados con el suministro de energía son peaks o picos de energía, ruido eléctrico, altibajos de voltaje y apagones.

Estos problemas están ocasionados por sobredemanda de energía, mantenimiento deficiente o inexistente a las plantas, fallas en las líneas de transmisión, falta de normatividad, desastres naturales, accidentes y errores humanos. Los factores mencionados anteriormente justifican la inversión de un sistema de respaldo de energía, tanto en proyectos nuevos como en proyectos ejecutados.

Debido a estos problemas se recomienda en este sistema el uso de inversores, que garantizaran el funcionamiento del sistema de vigilancia en ocasiones de cortes de energía eléctrica convencional, ya que estos además de deshabilitar completamente el sistema, pueden ocasionar daños en el hardware debido a las alteraciones y cambios de corriente en la energía eléctrica. Esta propuesta es opcional, dependerá de la necesidad del cliente y la zona donde este habite ya que en la actualidad los cortes energéticos han ido disminuyendo.

En la mayoría de los casos en donde la red eléctrica falla, se encuentran generadores de energía a combustible, como se sabe estos equipos generan energía solo mientras están funcionando, consumiendo combustible en forma constante, se este o no utilizando la energía eléctrica generada. Además, ya que no poseen ninguna forma de almacenamiento, la energía generada que no se consume se pierde, resultando un sistema muy costoso. En esta situación el uso de un inversor/cargador nos presenta ventajas muy convenientes para nuestro bolsillo, más allá de lo incalculable de disfrutar del silencio y de la protección del medio ambiente puro.

Ventajas de la utilización del inversor/cargador:

1. Energía 24 horas del día sin ruido (Dependiendo de la cantidad de bancos de baterías).
2. Ahorro de combustible.
3. Ahorro de tiempo y mantenimiento del generador.
4. Utilización de hasta el 100% de la energía generada.
5. Estabilización de la energía eléctrica convencional, evitando así el daño al hardware del sistema.

Se recomienda un sistema de respaldo independiente que solo alimentará al sistema de vigilancia y seguridad con un inversor/cargador con las siguientes especificaciones:

X-VERTER 812 800VA/600W

Propiedades:

- Panel de Control.
- Botón de encendido.
- Terminales de salida (4) NEMA 5-15R.
- Ventilador de enfriamiento.
- Protección contra sobrecarga.
- Conector de Baterías (l2V OC).
- Cable de alimentación AC espiga NEMA 5-15P.

Características:

- Sistema avanzado de UPS de Línea Interactiva.
- Onda 100% Senoidal.
- Tiempo de transferencia menor a 5 ms.
- Gran rango de regulación de voltaje, similar a un UPS en línea.
- Cargador inteligente de dos etapas.
- Elimina el 90% de los problemas eléctricos.
- Ideal para la protección de equipo médico, laboratorio, servidores de misón crítica o telecomunicaciones. Donde se requiera tiempo de respaldo prolongado.
- Alerta de reemplazo de batería en tiempo real.

Con la aplicación de un inversor/cargador de calidad, adicionando un banco de baterías, se podrá recargar estas baterías simultáneamente con la energía eléctrica convencional en este caso Unión Fenosa y una vez que esta falle, el banco de baterías proporcionara energía por varias horas al sistema de vigilancia. La duración de encendido del sistema cuando ocurran apagones lo determinaran la potencia del banco de baterías y esto se calcula mediante la siguiente fórmula:

La Potencia (P) * Tiempo (t)= Consumo

Consumo/V Sistema= La corriente (I)

La corriente determina el número de baterías a utilizar en relación al tiempo que se desee que el sistema permanezca encendido cuando no haya energía convencional.

La siguiente tabla muestra los componentes que lleva el sistema de seguridad dando un consumo total Watts/Unidad de 500 W. Con estos valores podemos determinar el banco de baterias a utilizar con las fórmulas que presentamos con anterioridad.

Producto	Cantidad	Watts/Unidad
PC Clon	1 u	430 W
Notebook Toshiba	1 u	40 W
Cámara IP Panasonic	1 u	3 W
Cámara Web Ezonic	2 u	2 W
Cámara Web Rlip Xtreme	1 u	2 W
Switch Nexxt	1 u	7 W
Router Thomson	1 u	18 W
Total	8 u	500 W

Tabla 5. Potencia consumida del sistema de vigilancia.

Se realizaron los cálculos para una duración de 3 horas debido a que la energía de la red convencional sufre cortes con una duración promedio de 2 h y media.

P= 500 W P*T= 500 W*3h=1500 Consumo

T= 3 h

I= Consumo/Vsistema= 1500/12V= 125 A

Esto quiere decir que para que nuestro sistema dure 3h de encendido después que no haya energía convencional se necesita un banco de batería de 125 A**.** El tipo de banco de batería a utilizar es marca SYNTHESIS power 105 A la cual es una de las baterias más accesibles en la actualidad. En este caso se haría la inversión en 2 baterias SYNTHESIS power 105 A, para cubrir la demanda de amperaje de los equipos conectados al inversor, con un tiempo de duración de más de 3h de funcionamiento.

.

Capítulo IV

4.1 CONCLUSIONES

- El sistema de vigilancia es un medio para mejorar la seguridad, pero su adecuado uso es responsabilidad del administrador y de cada usuario.

- El sistema de vigilancia no garantiza la no ocurrencia de hechos delictivos u otro tipo porque esto dependerá de factores físicos, como humanos y de cobertura de las diferentes zonas.

- La ubicación de las cámaras de pende de su distancia focal, la altura del objeto y de lo lejos que este la cámaras del objeto. La distancia focal (f) viene dada por el fabricante, la cual varía entre 4mm, 8mm, 12 mm, 16 mm, 25 mm. Los ángulos de enfoque de cada cámara vienen predeterminados de acuerdo a "f".

- Este proyecto es un Sistema de Vigilancia y Seguridad basado bajo plataforma Linux, el cual tiene como ventaja acceso a múltiples usuarios que a diferencia de los sistemas convencionales IP (Brindados por las empresas privadas), son configurados bajo sistemas operativos Windows, complementados por software genéricos de alto costo.

- El software de Monitoreo y tratamiento de imágenes y videos ZoneMinder, es una herramienta de vanguardia en el área de vigilancia de forma gratuita al público en general y es en si la base de nuestro sistema vigilancia, debido a su fácil configuración y compatibilidad con sistemas operativos Linux, ya que nos permite conocer y archivar los eventos capturados por cada cámara, exportación de videos, opciones de formatos de compresión, alertas y alarmas con mensajes vía correo electrónico y tono alerta de manera local.

- El uso de software libre nos garantiza un menor costo en comparación con los sistemas de vigilancia convencionales en Windows, convirtiéndolo en un

sistema apto para las pequeñas y medianas empresas ya que en la actualidad en el mercado Nicaragüense no se ofrecen este tipo de sistema.

- La Web creada es una interfaz de fácil navegación, amigable para los usuarios ya que el gestor de contenido Joomla nos permite incorporar nuevas aplicaciones y editar aquellas que ya han sido creadas, a través de él, logramos incorporar la interfaz web del software de vigilancia (ZoneMinder) en el sitio web.

- La altura en donde se ubicaron las cámaras de seguridad dependerá de la función que estas desempeñan, ya sea para visualización y ver detalles o de vista panorámica.

- El SSH nos facilita una comunicación fiable entre dos sistemas usando una arquitectura cliente-servidor, que permite al administrador conectarse al sistema remotamente, de esta manera el soporte técnico se hace de forma no presencial.

- La vida útil del sistema de vigilancia dependerá del uso y manteniendo de sus diferentes componentes, la actualización de este permitirá alargar su vida útil, por lo tanto se recomienda hacerlo de forma mensual.

4.2 RECOMENDACIONES

- Debido a la gran cantidad de distribuciones de sistemas operativos Linux, se debe de tomar en cuanta, utilizar aquellas versiones que se especializan en aspectos muy concretos, tomando en cuenta tres características fundamentales:

  - **Seguridad**
  - **Fácil de actualizar**
  - **Estabilidad**

- Al igual que los sistemas operativos Linux, existen también una gran cantidad de cámaras de videos. Para poder definir el sistema de vigilancia que queremos implementar, debemos de estudiar a profundidad las ventajas, desventajas y costos de cada aparato al igual que definir las áreas y ángulos que queremos que sean gravados.

- Para la instalación de los sistemas operativos, dependencias y repositorios se deben de seguir los asistentes de instalación típicos de cada programa, para evitar problemas en caso de que se intente hacer de forma avanzada.

- Debido que el tratamiento de imágenes y videos requiere el aprovechamiento al máximo de los recursos de nuestro servidor. Debemos utilizar equipos con buenas características de hardware e implementar un software que aproveche al máximo los recursos de nuestro ordenador, haciendo instalaciones simples y configurando los servicios con programas adicionales al sistema.

- Las orientaciones al usuario deben de ser simples, pero de gran impacto en la manipulación del sistema. Se debe concientizar al usuario hasta donde puede

manipular el equipo y que medidas debe de tomar si desea hacer un cambio en el hardware o software del sistema en ejecución.

- Se deben de configurar solo los servicios que son necesarios para la ejecución del sistema, esto nos garantizará el ahorro de recursos y tiempo. Además de la simplicidad de nuestros sistema. No obviando la posibilidad de mejoras y el uso de nuevas tecnologías de vigilancia y seguridad.

- ZoneMinder es capaz de enviar mensajes texto a un móvil, al generarse una alarma en el sistema esto solo es posible configurando un servidor SME Server 7.2. El cual no se hizo debido al corto tiempo de desarrollo del proyecto, por eso recomendamos su realización para que el sistema sea más eficiente.

- Para la transmisión de sonidos de forma remota se debe configurar un servidor streaming, el cual es útil como forma de alerta para el usuario en el caso de que este se encuentre fuera de su residencia.

- Se debe tomar en cuenta la importancia de la implementación de un sistema de respaldo en caso de fallas con la energía convencional, ya que este permitirá que el funcionamiento del sistema de no sea interrumpido y evitara daños a los equipos en caso de variaciones de voltaje.

- Para la visualización del video en tiempo real para cada una de las cámaras lo recomendable es tener un ancho de banda de 1Mbps, ya que en conexiones inferiores presentan retardos en la visualización de movimientos.

4.3 BIBLIOGRAFÍA

Aiyer, Ghosh. (2002). Clustering and Dependencies in Free/Open Source Software. Canadá: ISEF.

Ballester, G. (2003, 1 de Septiembre). Configuración de un servidor DNS en debían. Granada, España. (pp 1-13).

Barrero, F. David., y Martínez, Aldo R. (2007). Manejo de la consola bajo linux. Tesis de Maestría en Computación. UNAN-León, León Nic.

Coar, Ken. (1999). Adding PHP to Apache on Linux. Extraído el 14 de Agosto del 2011 desde http://www.linuxplanet.com/linuxplanet/tutorials/1374/1/

Comunidad Ubuntu Nicaragua. (2010). Ubuntu 10.04 LTS- Long-term support. Extraído el 30 de Agosto del 2011 desde http://www.ubuntu.com/download/ubuntu/download

Dodwell, C. (2001). Methodology and Preliminary Analysis. Extraído el 10 de septiembre del 2011 desde http://www.idei.asso.fr/Commun/Conferences/Internet/OSS2002/Papiers/Ghosh.PDF.

Escamilla, A. (2005). Evolución y eficacia de las medidas tecnológicas de intrusión para entidades financieras. II jornada de seguridad en entidades financieras (online). Seguritecnia disponible en http://www.borrmart.es/articulo_seguritecnia.php?id=1833

Enríquez, Mauricio. (2002, 26 de septiembre). Instalación ZoneMinder en español. Extraído el 12 de septiembre del 2011 desde http://www.zoneminder.com/documentation.

Flores, A. Noel. (2006). Configuración de servidores bajo plataforma Linux. Monografía de Ingeniería no publicada Universidad Popular Nicaragüense. Managua, Nicaragua.

Gómez, R. (2004). Administración básica de sistemas Linux. Monografía de Ingeniería no publicada Universidad Nacional de Colombia. Bogotá, CO.

González, Jesús M. (2008). Software libre y monopolios. Extraído el 20 de septiembre del 2011 desde http://sinetgy.org/~jgb/articulos/soft-libre-monopolios/.

González, E. (2009). Cámaras IP, la revolución digital de la video vigilancia. Extraído el 30 de Octubre del 2011 desde http://www.idg.es/dealerworld/Camaras-IP,--la-revolucion-digital-de-la-videovigilancia.Crecen-las-aplicaciones-mas-alla-de-la-seguridad/seccion-productos/articulo-195544

Gordillo, V. (2007). Sistemas de seguridad en video cámaras. Extraído 5 de Noviembre del 2011 desde http://www.actiweb.es/videonet/preguntas_frecuentes.html

Kelly, Christopher. (2007). Free Software/Free Science. Extraído el 1 de octubre del 2011 desde http://firstmonday.org/issues/issue6_12/kelty/.

Langfeldt, Nicolai., y Norrish, Jamie. (2001). DNS HOWTO, V 9.0. Extraído el 5 de octubre del 2011 desde http://www.linux.org/docs/ldp/howto/DNS-HOWTO.html

Linux Study. (2007). Questionnaire on Linux kernel developers. Extraído el 10 de Octubre del 2011 desde http://www.psychologie.uni-kiel.de/linux-study/

Melin, Ross. (2011, 26 de Agosto). ZoneMinder v 1.24.0. Extraído el 20 de 0ctubre del 2011 desde http://www.zoneminder.com/news.

Miro, Corporation. (2005, 17 de Agosto). Joomla 1.5.24 Full Package. Extraído el 5 de octubre del 2011 desde http://www.joomla.org/download.html.

Novell, Inc. (1982). Manual de Instalación de SLES 11 SP1. Extraído el 6 de Agosto del 2011 desde http://www.suse.com/documentation/sles11/

Pfeifer, Gerald. (2009). Suse Linux Enterprise Server. Extraído el 4 de Noviembre del 2011 desde http://en.wikipedia.org/wiki/SUSE_Linux_Enterprise_Server

Pressman, Roger. (1997). Ingeniería del Software: Un enfoque práctico. (Ed. 5) McGrawHill (pp. 5-60).

Revillini, J. (2010). Ubuntu 10.04 (Lucid Lynx) Desktop. Extraído el 2 de Octubre del 2011 desde http://www.zoneminder.com/wiki/index.php/Ubuntu_10.04_(Lucid_Lynx)_Desktop

Valdivia, P. (2006). Sistemas de seguridad y vigilancia mediante cámaras. Extraído el 28 de Octubre del 2011 desde http://www.camarasip.cl/sistema_de_seguridad_mediante_camaras.html

Valeriano, J. (2006). Que es y cómo funciona una cámara IP. Extraído el 6 de noviembre del 2011 desde http://valetron.eresmas.net/CamarasIP.htm

Wawro, A. (2011). Convierte una cámara web en una cámara de seguridad. Extraído el 23 Noviembre del 2011 desde http://www.pcworld.com.mx/Articulos/19643.htm

4.4 ANEXOS

4.4.1 Cotizaciones

Para determinar la comparación de costos de este sistema, se realizaron una serie de cotizaciones en empresas que distribuyen sistemas de seguridad con cámaras IP, ya sea con monitoreo a través de un DVR o por medio de una PC. También incluimos un sistema con cámaras analógicas y el costo aproximado de nuestro proyecto.

1- Sistema de vigilancia con cámaras IP con monitoreo a través de un PC con software Panasonic para visualización de varias cámaras IP a la vez.

Tecnología Computarizada S.A

Calle Principal Altamira D'este No.589 Ferreteria Sinsa 25vrs arriba
Telefono:PBX (505) 267-4012 - Fax:(505)270-6224 - Email : ventas@comtech.com.ni
RUC No. J0310000000603 - www.comtech.com.ni

Cliente: ROLAN OBANDO
Atención:
Teléfono:
Email:

No. Prof. 22871
Fecha 21/11/2011
Válida hasta 21/12/2011
Condiciones CONTADO

#	Código	Descripción	Cant	Precio	Total
1	00301-013	PROCESADOR INTEL CELERON E3400 / 2.6GHZ (800 MHZ) - LGA775 - BX80571E3400	1	U$ 51.28	U$ 51.28
2	00101-059	TARJETA MADRE ASROCK G41M-VS3 S775 / DDR3 / FSB1333	1	U$ 52.00	U$ 52.00
3	00201-175	MEMORIA KINGSTON 2GB - DDR3 - 1066 - KVR1066D3S8N7/2G - CAJA Y GRANEL	1	U$ 12.83	U$ 12.83
4	00701-029	DVDRW LITE ON / SATA / 22X / NEGRO / HAS122-04B	1	U$ 19.99	U$ 19.99
5	00401-020	DISCO DURO 500GB / SATA /WD / WDHD5000AAKX	1	U$ 98.00	U$ 98.00
6	01101-018	CASE MICRO ATX MYO- ATX5855	1	U$ 24.99	U$ 24.99
7	02201-040	MONITOR BENQ 18.5" - G925HDA - LCD - NEGRO - 9H.L2WLB.Q8L	1	U$ 103.00	U$ 103.00
8	01901-069	TECLADO MYO STANDAR ENGLISH USB2/MYO-KB25	1	U$ 3.56	U$ 3.56
9	02101-068	MOUSE MYO OPTICAL USB CABLE BLAK/MYO-2535	1	U$ 2.69	U$ 2.69
10	01501-002	ALMOHADILLA CON GRAFICO - AC260GEN50	1	U$ 1.00	U$ 1.00
11	05701-074	SWITCH ENCORE 8P/ ENH908-NWY / 10-100 (30 DIAS GARANTIA)	1	U$ 14.10	U$ 14.10
12	03101-099	CABLE UTP - CAT-5E - METRO	40	U$ 0.33	U$ 13.20
13	07701-016	CONECTOR RJ45 CAT-5 10/100	8	U$ 0.18	U$ 1.44
14	10301-001	CAMARA IP PANASONIC/BLC101A	4	U$ 180.10	U$ 720.40
15	05701-160	CANALETA CON ADHESIVO - 1.60" X 0.90" - COLOR BLANCO	20	U$ 5.09	U$ 101.80
16	02401-002	ESTABILIZADOR CDP 1000VA / BAVR1006	1	U$ 10.88	U$ 10.88
17	05701-161	CONSOLA PANASONIC - WJ-NV200KP - NVR 16-CAN - H.264 MPEG-4 M-JPEG/ 2 HDD SATA/ FACE MATCHING/ HDMI/	1	U$ 1,895.99	U$ 1,895.99

Comentarios:

Recoring Software Panasonic (MPG4/JPEG) = U$ 442.37 + IVA.

Subtotal	U$ 3,127.15
Impuesto	U$ 469.07
Total	U$ 3,596.22

Nota: T/C 23.0000
Es valida solamente con el sello de la empresa

Carlos Narvaez

COMTECH REDES Y COMUNICACION

Nota: Somos Grandes Contribuyentes.
Estamos Exentos del 1% de la Retencion en la Fuente

2- Sistema de vigilancia con cámaras IP con monitoreo a través de una PC con visualización de una cámara a la vez.

COMPU-PARTES S.A
Todo en computadoras y accesorios.

TRIPP-LITE EPSON EXCEED YOUR VISION

CLIENTE	ELECTRONIC SECURITY	FECHA	noviembre 21, 2011
		VENDEDOR	JOYCE BOLAÑOS
ATENCION		TELEFONO	22774037 CEL. 88965414
DIRECCION	MANAGUA	EMAIL	j.bolanos@msn.com
TELEFONO		Nº RUC.	*0501079472

Estimado (s) Señor (es):
Es una enorme satisfacción y un privilegio que nuestra empresa pueda cotizar a usted (es) nuestros productos, esperamos que nuestros precios puedan llenar plenamente sus espectativas.
A continuación relacionamos los productos y precios con sus respectivas características

Cantidad	Descripción	Precio Unitario	Total
1	COMPUTADORA INTEL CELERON DUAL 2.6 GHZ INTEL CELERON 2.6 GHZ TARJETA MADRE CHIP G41M-VS3 SOCKET 775 6 PUERTOS USB, 1 PCI EXPRESS RED 10/100, MEMORIA DDR3 4 GB PC 1333 MHZ DISCO DURO 500 GB SATA 7200 RPM LECTOR DE MEMORIAS, UNIDAD DVD-RW SATA TECLADO, MOUSE , MOUSE PAD MONITOR PANTALLA PLANA LCD 15.6" UPS 750 VA/ SUPRESOR DE VOLTAJE INTEGRADO	$398.00	$796.00
4	CAMARAS PANASONIC BL-C1A	$150.68	$602.72
4	CAMARAS DE SEGURIDAD ETHERNET		
4	CANALETAS 2 - 1/3"	$5.00	$20.00
40	METROS DE CABLE UTP CAT. 5E	$20.00	$20.00
8	CONECTORES RJ - 45	$2.00	$2.00
1	SWITCH DE 8 PUERTOS 10/100	$15.00	$15.00
		TOTAL	$1,455.72
		15% I.G.V.	$218.36
		TOTAL	$1,674.08

GARANTIA REAL: 1 AÑO
TAZA DE CAMBIO 22.85
CONTADO O CHEQUE - COMPUPARTES Y/O FELIX CRUZ B.

Atentamente: JOYCE BOLAÑOS
ALTAMIRA FERRETERIA SINSA 1C. AL SUR, 1/2C. AL ESTE

Altamira D' Este 582 de Ferretería Sinsa 1 c. al sur 1/2 arriba.
Telefax : 2782245 - 2525992 - 2525972 - 2525963

Compu - Partes, S.A. COMPUTER TECHNOLOGY VENTAS

3- Sistema de vigilancia con cámaras Analógicas con monitoreo a través de un DVR con monitoreo únicamente para 4 cámaras analógicas.

SEVASA
Tecnología a tu alcance

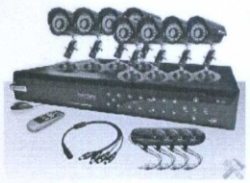
SUCURSAL ALTAMIRA
calle principal altamira de la ferreteria
Roberto Morales 100mts al Sur
PBX : 2252-4204 EXT 210
TEL : 2278-7282

Cotización

Nombre : **Sr. Rolan Obando**
Atención :
Email:
Telefono: Fax :

Fecha : 21-nov-11
Vendedor: Santos Zelaya
Celular: 86010048
correo:szelaya@sevasaonline.com

Cant.	Descripcion	P. Unit	P.Total
1	Camaras de Seguridad Kguard 4 Canales 4 Camaras 8 Canales H.264 DVR Velocidad de grabacion 240fps(NTSC), 200fps(PAL) Resolucion Maxima de 1440x900 Disco Duro hasta 2TB Sata Puede vigilar desde: Iphone, blacberry, Android, Windows mobile, Symbian Phone. Camaras contra agua Iluminacion: Olux (IR ON) Disco Duro de 500GB Incluido	$439,00	$439,00
1	**Monitor de 23" LED Marca Aoc**	$172,80	$172,80



Sub Total	$611,80
IVA 15%	$91,77
Total U$	$703,57
Total C$	C$ 16.252,47

Forma de Pago

- (•) Contado
- ( ) NO ACEPTAMOS CK Personales

Tipo de Cambio: C$ 23,10
SI APLICA RETENCION A NOMBRE DE **SEVASA**
RETENCION ES DE 1%
de RUC: 0306059521

Santos Zelaya
Ejecutivo de Ventas

Tiempo de Garantia: 6 Meses
Tiempo de Entrega: INMEDIATA OFERTA VALIDA POR 8 DIAS
NOTA: PRECIOS SUJETOS A CAMBIO

4- Sistema de vigilancia con cámaras IP con monitoreo a través de un DVR con monitoreo únicamente para 8 cámaras analógicas.

SEVASA
Tecnologia a tu alcance

DE LOS SEMAFORO DEL COLONIAL 1/2 ARRIBA
Telefono : 2248-2810 EXT 303

Cotización

No 063

Nombre : GERSON PEREZ
Atención :
Email: perez_gerson89@yahoo.es
Telefono: 22 70 79 50 Fax : 88 53 32 15

Fecha : 30-nov-11
Vendedor: Maria Jose arana
Celular: 84-05-17-34
Correo: ventasbello@sevasaonline.com

Cant.	PRODUCTO	P. Unit	P.Total
1	CAMARA DE SEGURIDAD 8CH 8CAMARAS KG FACIL INSTALACION Y MANEJO 8 CAMARAS DE VISION INFRAROJA SOMBRERO QUE EVITA EL REFLEJO DE LOS RAYOS SOLARES SOPORTE ARTICULADO METALICO QUE PERMITE ENFOCAR LA ZONA DESEADA INCLUYE DETECCION DE MOVIMIENTO ES PERFECTO PARA TENER MAYOR SEGURIDAD EN SU CASA O EMPRESA INCLUYE UN DISCO DURO DE 500 GB SAT 		$729.00
		Sub Total	$729.00
		IVA 15%	$109.35
		Total General	$838.35

Forma de Pago

- [x] CONTADO
- [ ] CHEQUES BAC O BANCENTRO NOMBRE: SEVASA
- [ ] OTRO TIPO DE BANCO :

TIPO DE CAMBIO:23.15
Vencimiento de Oferta : 3 dias habiles
SOMOS RETENEDORES 1%

Maria Jose Arana M
Ejecutivo de Ventas

Tiempo de Garantia: *3 MESES*

Tiempo de Entrega: INMEDIATA

4.4.2 Presupuesto de costo del Sistema de Vigilancia.

Sistema de vigilancia con cámaras Web e IP con monitoreo a través de software ZoneMinder.

Cantidad	Descripción	Precio Unitario	Total
1	PC CLON Intel Celeron 2.5 GHZ, HHD 500 GB, RAM 2 GB DDR2, Teclado, Mouse, Parlantes, Monitor LCD 16 in.	U$ 350	U$ 350
2	cámaras Web Ezonic	U$ 10.00	U$ 20.00
2	cámaras Web Klip Xtreme	U$ 22.00	U$ 44.00
1	Dirección IP publica (256 Kbps)	U$ 64.00	U$ 64.00
1	Switch Nexxt de 8 puertos	U$ 16.00	U$16.00
1	Cámara IP Panasonic BL-C1	U$ 175.00	U$ 175.00
40	Cable UTP-CAT-5E-METRO	U$ 0.33	U$ 13.20
6	Conectores RJ45	U$ 0.17	U$ 1.04
6	Conectores USB Tipo SHASIS	U$ 0.56	U$ 3.39
TOTAL			U$ 686.63

Tabla 6. Costo del sistema de vigilancia aplicado (Incluye IVA).

4.4.3 Cotización de sistema de respaldo (opcional)

Inversor/Cargador CDP y Batería para alimentación del sistema en caso de fallo de energía eléctrica convencional.

TECNOSOL ENERGIA EN SUS MANOS	PROFORMA	CÓDIGO	PVT-F02-01
		VERSIÓN	01
	REFERENCIA DE LA NORMA ISO 9001:2008: 5.2, 7.1, 7.2, 7.2.1, 7.2.2, 7.2.3, 8.4, 8.5	Fecha:09/06/2011	Jun -9

PROFORMA2111116

Cliente : GERSON PEREZ
Atención :
Dirección : MANAGUA
E-mail :
Tel: 2270-7950

Fecha : 21 de noviembre del 2011
Vendedor: Francisco Hernández
E-mail :
fhernandez@tecnosolsa.com
Teléf. : 225151-52
Cel. : 8465-0145

Cantidad	Descripción	Precio Unitario	Total
1	INVERSOR DE PODER DE 600W	315.00	315.00
2	BATERIAS DE 105AH SYNTHESIS	105.00	210.00
2	CABLES DE CONEXIÓN BC1	11.00	22.00
2	CABLES DE CONEXIÓN BC5	25.00	50.00
ENTREGA:SUJETA A CAMBIOS TIPO DE CAMBIO:22.94 BATERIAS EXCENTAS DE IVA		*Sub-total* ***SUB-TOTAL*** *IVA* ***TOTAL US$***	597.00 597.00 54.75 651.75

NOTA:
* Esta proforma es válida por 15 días a partir de su fecha de recepción. Después de este tiempo deberá consultar por posibles cambios en los precios y equipos en existencia.
* Los precios de esta cotización están en dólares americanos. Si el pago se realiza en córdobas favor hacer conversión en base al tipo de cambio oficial de BANCENTRO.
* Favor Elaborar Cheque **Certificado** a Nombre de TECNOSOL y/o Vladimir Delagneau Barquero.
* El tiempo de entrega: INMEDIATO
* Forma de Pago: CONTADO
* Estamos **Exentos de retención de IR.**

Rotonda Bello Horizonte 420 metros al este. Managua, Nicaragua. PBX: 2251-5152 – Cel: 8883-4464
Vdelagneau@tecnosolsa.com.ni- tecnosol@ibw.com.ni – www.tecnosolsa.com.ni

4.4.4 Comparación de 4 software de vigilancia y monitoreo, incluyendo el ZoneMinder utilizado en el proyecto implementado.

	AXIS Camera Station	CamUniversal	WebCam Monitor	ZoneMinder	Witness-Pro
Transparencia respecto al fabricante de cámaras.	Moderada	Si	Si	Si	Si
Soporta cámaras IP.	Si	Si	Si	Si	No
Soporta webcams usb.	No	Si	Si	Si	No
Soporta cámaras analógicas.	No	No	No	Si	Si
Administración de las grabaciones.	Si	Si	Si	Si	Si
Detección de movimiento.	Si	Si	Si	Si	Si
Gestión de la detección de movimiento.	Si	Si	Si	Si	Si
Gestión de varias fuentes de vídeo simultáneas.	Si	Si	Si	Si	Si
Agrupación de fuentes de vídeo por grupos lógicos.	Si	No	No	Si	No
Gestión de usuarios.	Si	Si	Si	Si	Si
Acceso remoto.	Web Browser o Cliente Windows (Funcionalidad limitada)	Web Browser o Cliente Windows (Funcionalidad limitada)	Web Browser	Web Browser	Web Browser o Cliente Windows (Funcionalidad limitada)
Control de cámaras PTZ.	Si	No	Si	Si	Si
Envío de emails.	Si	Si	Si	Si	No
Envío de ficheros vía FTP.	No	Si	Si	Si	No
Envío de SMS.	No	No	Si	Si	No
Creación de eventos en función de un calendario.	Si	Si	Si	Si	Si

	AXIS Camera Station	CamUniversal	WebCam Monitor	ZoneMinder	Witness-Pro
Multilenguaje.	Si	Si	Si	Si	Si
Creación de archivos de vídeo	JPEG o MPEG-4	AVI	WMV	MPEG, WMV, AVI, 3GP, MOV	JPEG y MPEG-4
Creación de logs.	Si	Si	Si	Si	Si
Compresión de archivos.	No	No	No	*.Zip y *,Tar	No
Soporte de protocolos domóticos.	No	No	No	X10	No
Control del ancho de banda.	No	No	No	Si	No
Acceso desde dispositivos de interfaz reducida.	No	No	No	Si	No
Soporte para audio.	Semidúplex en tiempo real.	Si	Si	Si(Limitado)	Si
Posibilidades de ampliación de características.	No para el software, pero se proporcionan comandos de diálogo con las cámaras Axis	No (sujeto al fabricante)	No (sujeto al fabricante)	Código abierto	No (sujeto al fabricante)
Precio aproximado	714,00 $	49,95 $	49,95 $	Software Libre	709,00 € (Con tarjeta de 4 puertos)

4.4.5 Especificaciones de las cámaras de vigilancia utilizadas.

Cámara IP Panasonic BL-C1A

La Cámara IP para interior Panasonic BL-C1 vigila tu casa o tu negocio desde cualquier lugar, con un sencillo explorador y una conexión Internet, con las nuevas cámaras IP de Panasonic, la domótica más sencilla para tu nuevo hogar digital. Gracias a su nueva línea de elegante diseño y a su pequeño tamaño, las nuevas cámaras IP son la mejor solución para controlar el hogar y todo lo que ocurre dentro de él. Con estos sencillos sistemas, el usuario no tendrá que preocuparse más por la seguridad de su hogar ya que a través de estas unidades podrá ver las imágenes desde su móvil, su PC o incluso su televisor (necesario equipamiento opcional) controlando en todo momento las áreas monitorizadas. Lo único que necesitará para ello será una conexión a Internet (ADSL, Cable módem).

Características.

Tanto esta cámara BL-C1 con cable, como la BL-C20, inalámbrica, son fácilmente instalables y muy discretas. Además, las nuevas cámaras se caracterizan por su facilidad de uso gracias al asistente de configuración automática (UPnP) y a un sistema que permite la definición y los ajustes automáticos para la conexión a red.

Estos dos nuevos modelos poseen un zoom digital de 10 aumentos, perfecto para ampliar la zona que se está observando y obtener una imagen nítida y de gran calidad. Con estas dos unidades no tendrás que preocuparte más por tu hogar, la BL-C1 monitorizan varias áreas a la vez gracias a su función multi-cámara, que permite visualizar hasta 12 cámaras simultáneas. Las cámaras son capaces de ajustar automáticamente, en el modo de visualización nocturna, el brillo de la imagen para poder monitorizar imágenes en espacios oscuros y a color.

A su vez, la BL-C1 pueden detectar movimiento basándose en una sensibilidad predefinida para luego transferir las imágenes obtenidas (es capaz de almacenar hasta 250 imágenes en la memoria interna de la cámara) a una dirección FTP o bien por email. De esta forma, el usuario puede controlar su casa a cualquier hora y desde una ubicación distante utilizando simplemente una PC o un teléfono móvil. Hasta 20 Usuarios simultáneos Resolución de vídeo: 640x480, 320x240, 160x120, compresión de imágenes: JPEG, M-JPEG, Zoom digital x10.

- Tasa de trama Max 15 fotogramas por segundo (320x240).
- Medidas: 85 mm x 85 mm x 25 mm (sin base de montaje)
- Base de pie o para techo.
- Distancia focal de 8 mm
- Sensor 1/4" CMOS 320.000 pixeles
- Luminosidad de 10 lux a 10000 lux (en modo Nocturno desde 4 lux).
- Angulo de visualización 53 grados horizontales, 41 grados verticales.
- Velocidad máxima 15 i/s, iris fijo, resolución seleccionable (máxima 640x480)
- Buffer Interno para aproximadamente 250 imágenes, hasta 20 accesos simultáneos.
- Protocolos soportados TCP/IP, UDP/IP, HTTP, FTP, SMTP, POP3, DNS, DDNS, DHCP, ARP, ICMP, NTP.
- Temperatura: 5ºC-40ºC. Consumo: 1,7 W
- Alimentación: 120-240 V AC, 50/60 Hz – 9VDC.

Cámara Web Ezonic s.a III

Características:

Sensor:	100,000 pixel CMOS
Resolución:	352 x 288, 320 x 240, 176 x 144 160 x 120
Salida de video:	24 - bit Color (RGB)
Rango de captura	30 cuadros por segundo
Lente:	Foco manual de 10cm al infinito
Interface:	con cable incluido USB de 50.8cm
Alimentación:	5.0V DC sin adaptador, únicamente por USB
Dimensiones:	9.5cm x 4.6cm x 12.0cm
Peso:	390 grs
Sistema Operativo soportado:	Windows 98/ME, Windows 2000,Windows XP
Software incluido.	EZCam III hardware drivers Ezonics,EZSuite Interface BestOn,EZPhoto Tools BestOn,EZPhoto Browser BestOn,EZShowtime MMS BestOn,EZVideo Mail BestOn,Greeting Cam Deluxe
Requisitos del sistema:	Computadora 300Mhz 32MB RAM (64MB Recomendados). Puerto USB Windows 98, ME, Windows 2000 y XP Tarjeta de sonido Modem.

Cámara Web Klip Xtreme 300

Características:

- **Descripción del producto:** Klip Xtreme Xcam 300
- **Tipo de dispositivo:** Cámara Web fija
- **Color:** Roja
- **Tipo de Sensor:** Óptico 3 k píxeles
- **Interfaces:** Hi-Speed USB
- **Visión:** Auto balance de blanco, rotación omnidireccional
- **Soporte de Audio:** No
- Omnidireccional de rotación
- AWB (Balance automático de blancura)
- Enfoque manual.
- Velocidad de fotograma hasta 30 fps
- Distancia focal 30mm
- Formato de imágenes RGB24

Caracteristicas de visualizacion con respecto al tipo de lente

Imagen original					
Distancia focal equivalente de imagen de cámara compacta	22 mm	32 mm	43 mm	65 mm	135 mm
Distancia focal	4 mm	6 mm	8 mm	12 mm	25 mm
Tapa	2,0	2,0	2,0	2,0	2,5
Angulo de visión horizontal	90°	60°	45°	31°	15°
Angulo de visión vertical	67°	45°	34°	23°	11°
Distancia 1 m	**m**	**m**	**m**	**m**	**m**
• Ancho de imagen	2,0	1,1	0,8	0,5	0,3
• Alto de imagen	1,3	0,8	0,6	0,4	0,2
Distancia 5 m	**m**	**m**	**m**	**m**	**m**
• Ancho de imagen	10,0	5,7	4,1	2,7	1,3
• Alto de imagen	6,6	4,1	3,0	2,0	1,0
Distancia 10 m	**m**	**m**	**m**	**m**	**m**
• Ancho de imagen	20,0	11,5	8,2	5,5	2,6
• Alto de imagen	13,3	8,2	6,1	4,0	1,9
Distancia 20 m	**m**	**m**	**m**	**m**	**m**
• Ancho de imagen	40,0	23,0	16,4	11,0	5,2
• Alto de imagen	26,6	16,4	12,2	8,0	3,8
Distancia 50 m	**m**	**m**	**m**	**m**	**m**
• Ancho de imagen	100,0	57,5	41,0	27,5	13,0
• Alto de imagen	66,0	41,0	30,5	20,0	9,5

4.4.6 Tipos de cámaras IP

Cámaras IP tipo Domo:

Cámara IP domo fijas

Cámaras Domo:

Una cámara domo fija, también conocida como mini domo, consta básicamente de una cámara fija preinstalada en una pequeña carcasa domo. La cámara puede enfocar el punto seleccionado en cualquier dirección. La ventaja principal radica en su discreto y disimulado diseño, así como en la dificultad de ver hacia qué dirección apunta la cámara. Asimismo, es resistente a las manipulaciones.

Uno de los inconvenientes que presentan los domos fijos es que normalmente no disponen de objetivos intercambiables y si pueden intercambiarse, la selección de objetivos está limitada por el espacio dentro de la carcasa domo. Para compensarlo, a menudo se proporciona un objetivo varifocal que permita realizar ajustes en el campo de visión de la cámara. Este tipo de cámaras se instala, generalmente, en la pared o en el techo.

Camaras IP domo PTZ

Cámaras domos PTZ

Las cámaras PTZ o domos PTZ pueden moverse horizontalmente, verticalmente y acercarse o alejarse de un área o un objeto de forma manual o automática. Todos los comandos PTZ se envían a través del mismo cable de red que la transmisión de video. A diferencia de lo que ocurre con la cámara analógica PTZ, no es necesario instalar cables RS-485.

Las cámaras de red domo PTZ pueden cubrir una amplia área al permitir una mayor flexibilidad en las funciones de movimiento horizontal, vertical y zoom. Asimismo, permiten un movimiento horizontal continuo de 360º y un movimiento vertical de normalmente 180º. Debido a su diseño, montaje y dificultad de identificación del ángulo de visión de la cámara (el cristal de las cubiertas de la cúpula puede ser transparente o ahumado), los domos PTZ resultan idóneas para su uso en instalaciones discretas.

Los domos PTZ también proporcionan solidez mecánica para operación continua en el modo ronda de vigilancia, en el que la cámara se mueve automáticamente de una posición predefinida a la siguiente de forma predeterminada o aleatoriamente. Normalmente, pueden configurarse y activarse hasta 20 rondas de vigilancia durante distintas horas del día. En el modo ronda de vigilancia, un domo PTZ puede cubrir

un área en el que se necesitarían 10 cámaras de red fijas. El principal inconveniente de este tipo de cámara es que sólo se puede supervisar una ubicación en un momento concreto, dejando así las otras nueve posiciones sin supervisar.

El zoom óptico de un domo PTZ se mueve, generalmente, entre valores de 10x y 35x. Este tipo de cámaras se utilizan con frecuencia en situaciones en las que se emplea un operador. En caso de que se utilice en interiores, se instala en el techo o en un poste o en una esquina cuando se trata de instalaciones exteriores.

Camaras IP tipo Bullet:

Cámaras IP Bullet PTZ

El término cámara PTZ tiene dos usos dentro de la industria de los productos de seguridad de video y vigilancia. En primer lugar, PTZ es un acrónimo de pan-tilt-zoom y puede referirse sólo a las características de las cámaras de vigilancia específicas. En segundo lugar, cámaras PTZ también puede ser utilizado para describir toda una categoría de cámaras en una combinación de sonido, movimiento y cambios en la firma de calor puede permitir para activar la cámara, el enfoque y tema presuntos cambios en el campo del video.

Las cámaras PTZ pueden moverse horizontalmente, verticalmente y acercarse o alejarse de un área o un objeto de forma manual o automática. Todos los comandos PTZ se envían a través del mismo cable de red que la transmisión de vídeo. Algunas de las funciones que se pueden incorporar a una cámara PTZ incluyen:

- ✓ Estabilización electrónica de imagen (EIS): Esta ayuda a reducir el efecto de la vibración en un vídeo.

- ✓ Máscara de privacidad Permite bloquear o enmascarar determinadas áreas de la escena frente a visualización o grabación.

- ✓ Posiciones predefinidas: Muchas cámaras PTZ y domo PTZ permiten programar posiciones predefinidas, normalmente entre 20 y 100.

- ✓ Autoseguimiento: El autoseguimiento es una función de vídeo inteligente que detecta automáticamente el movimiento de una persona o vehículo y lo sigue dentro de la zona de cobertura de la cámara.

Camaras IP tipo bullet fija

Cámaras fijas tipo Bullet

Es cámara de red fija, que puede entregarse con un objetivo fijo o varifocal, es una cámara que dispone de un campo de vista fijo (normal/telefoto/gran angular) una vez montada. Es un dispositivo tradicional en el que la cámara y la dirección a la que apunta son claramente visibles. Este tipo de cámara es la mejor opción en aplicaciones en las que resulta útil que la cámara esté bien visible. Normalmente, las cámaras fijas permiten que se cambien sus objetivos. Pueden instalarse en carcasas diseñadas para su uso en instalaciones interiores o exteriores.

Camaras IP mecanicas:

Cámaras mecánicas fijas

Cámaras PTZ no mecánicas

Las cámaras de red PTZ no mecánicas ofrecen capacidades de movimiento horizontal, vertical y zoom sin partes móviles, de forma que no existe desgaste. Con un objetivo gran angular, ofrecen un campo de visión más completo que las cámaras de red PTZ mecánicas.

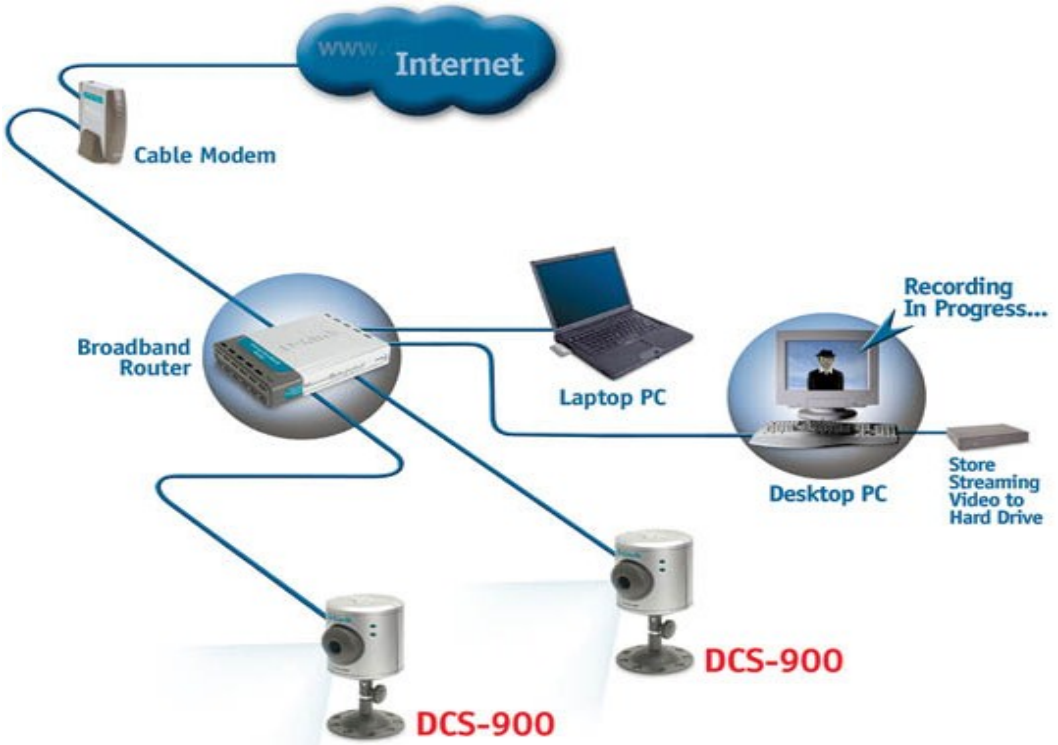
Una cámara PTZ no mecánica utiliza un sensor de imagen megapíxel y permite que el operador aleje o acerque, de forma instantánea, cualquier parte de la escena sin que se produzca ninguna pérdida en la resolución de la imagen. Esto se consigue presentando una imagen de visión general en resolución VGA (640x480 píxeles) aunque la cámara capture una imagen de resolución mucho más elevada. Cuando se da la orden de acercar o alejar cualquier parte de la imagen de visión completa, el dispositivo utiliza la resolución megapíxel original para proporcionar una relación completa 1:1 en resolución VGA. El primer plano resultante ofrece buenos detalles y una nitidez mantenida. Si se utiliza un zoom digital normal, la imagen acercada pierde, con frecuencia, en detalles y nitidez Una cámara PTZ no mecánica resulta ideal para instalaciones discretas montadas en la pared.

Cámaras mecánicas PTZ

Cámaras PTZ mecánicas

Las cámaras de red PTZ mecánicas se utilizan principalmente en interiores y en aplicaciones donde se emplea un operador. El zoom óptico en cámaras PTZ varía normalmente entre 10x y 26x. Una cámara PTZ puede instalarse en el techo o en la pared.

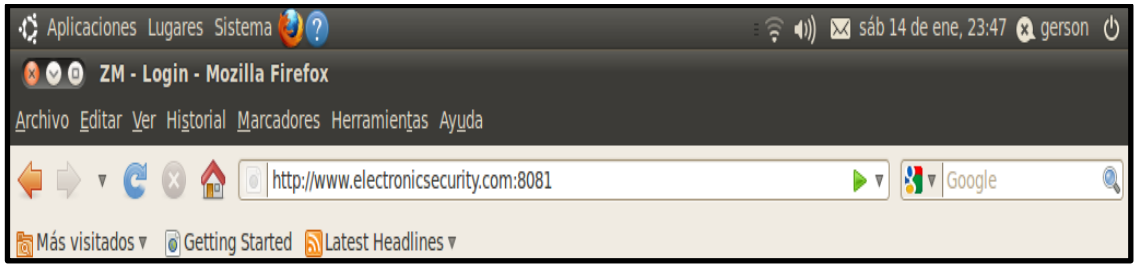
4.4.7 Diagrama de conexión de cámaras IP



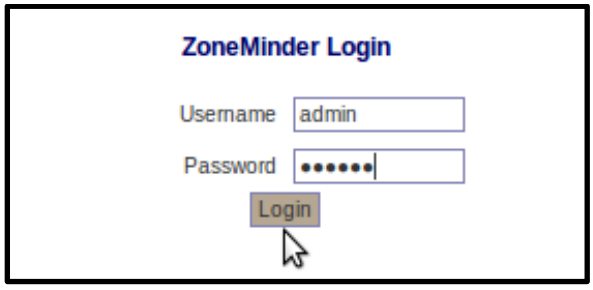
Manual de usuario

1. Seleccionar el navegador con el cual estableceremos la sesión de ZoneMinder (Firefox, Chrome, Explorer).

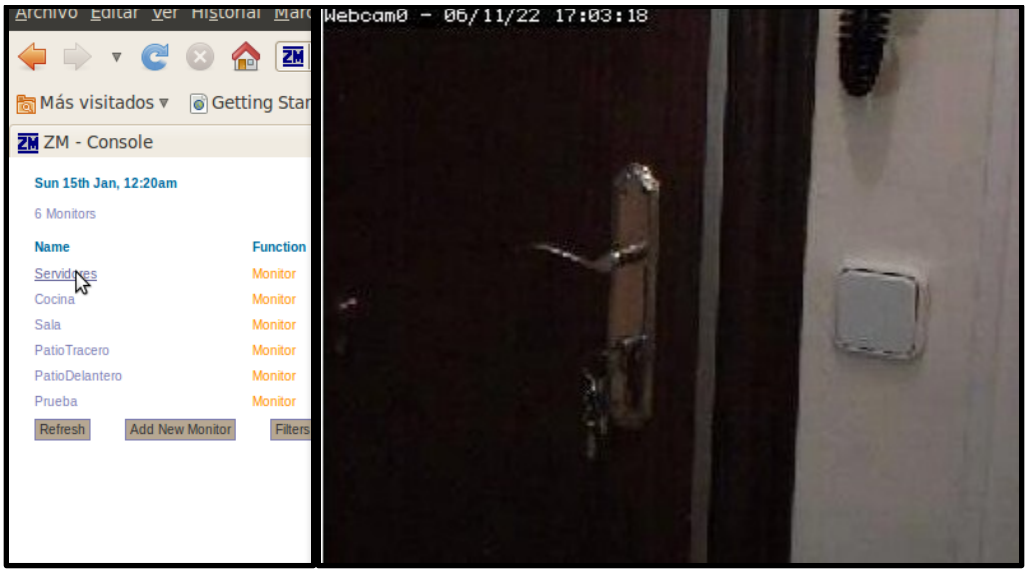
2. Digitar la dirección URL (www.electronicsecurity.com:8081) en la barra de navegación.



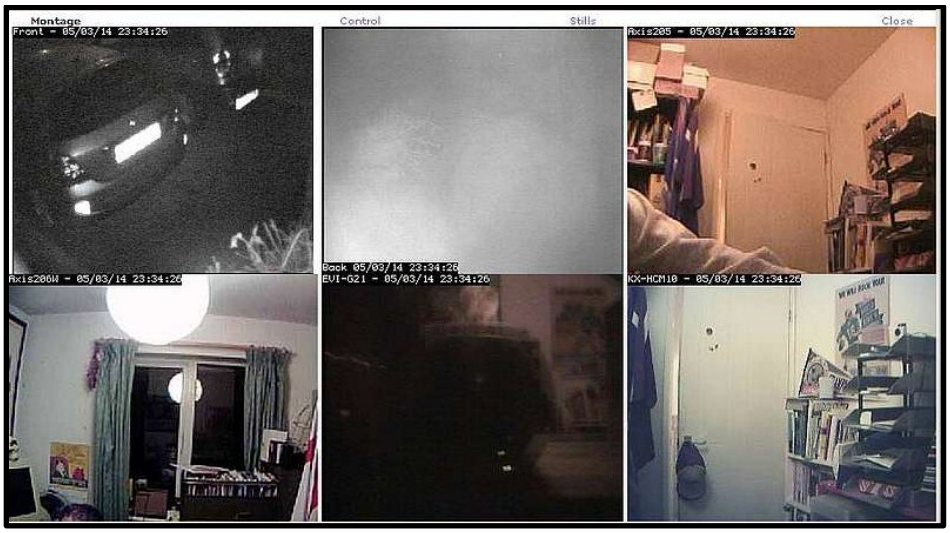
3. Escribir el Usuario y contraseña en el panel del ZoneMinder.



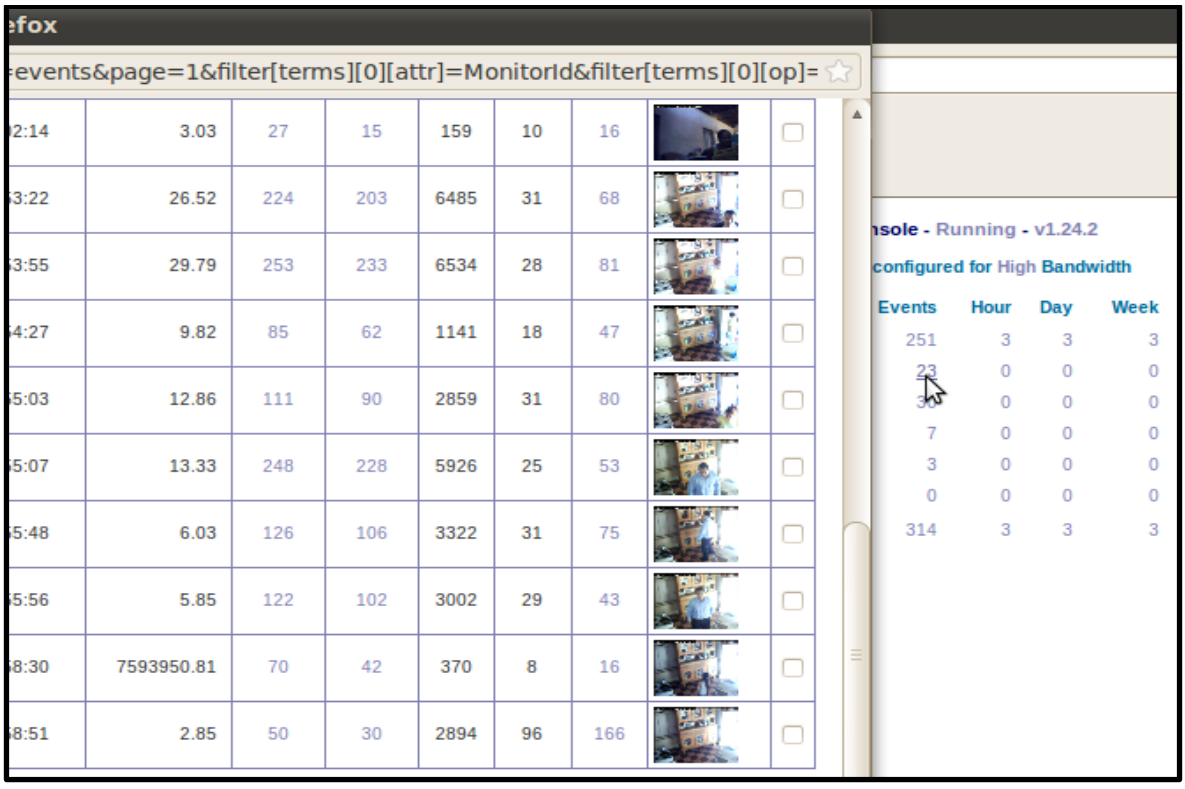
4. Para la visualización de cada cámara instalada se debe dar click en el nombre de cada monitor.



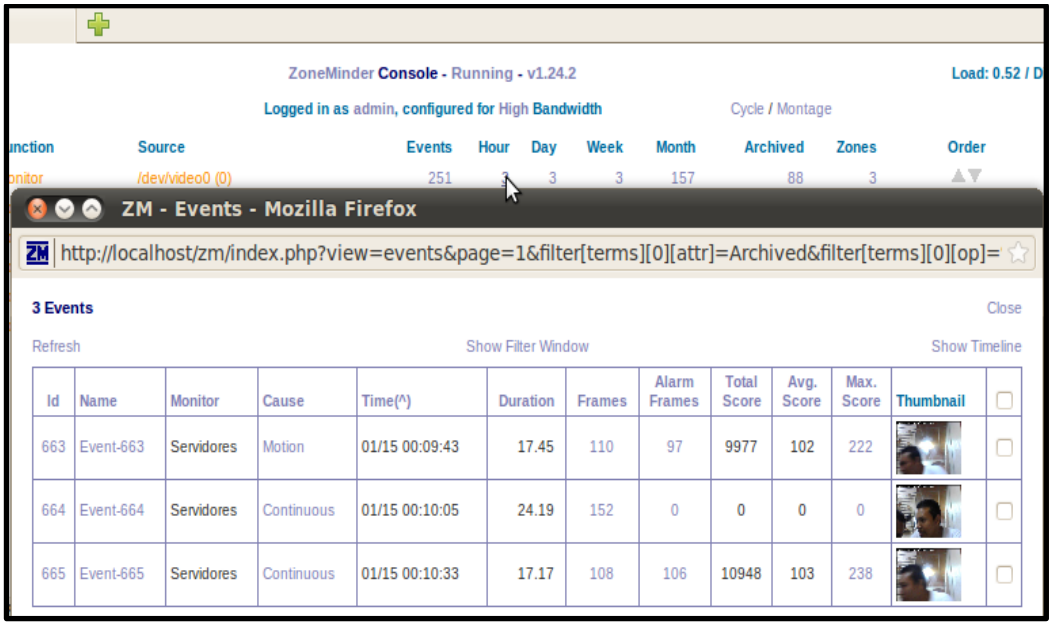
5. Si se desea observar todas las cámaras a la vez, se da clic en la opción "Montage" (Parte superior derecha del panel)



6. Para observar los eventos captados por las cámaras se debe dar clic en la columna "Events", el cual contendrá el número de eventos por monitor en orden descendente.



7. De la misma manera para observar los eventos, de acuerdo a los siguientes parámetros: Horas, Día, Semana, Mes. Se debe dar clic en las columnas correspondiente a cada parámetro.



8. El proceso de tratamientos de las imágenes se caracteriza de acuerdo al color en que se muestran "Function y Source" y puede ser según lo siguiente:

None: El monitor está desactivado, no se visualizará imagen.

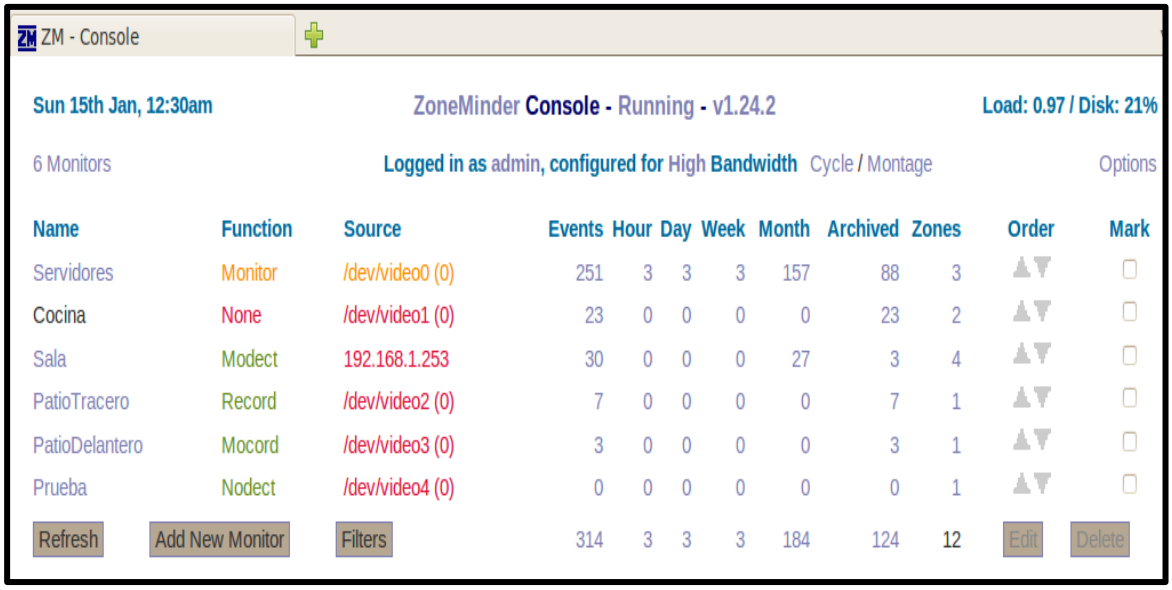
Monitor: El monitor ha sido activado, solo se permite visualización de imágenes.

Modect: Este es el modo de función de detección, que ante cualquier movimiento en una zona activa, se realiza el tratamiento del video, almacenando un evento y generando un tono de alarma.

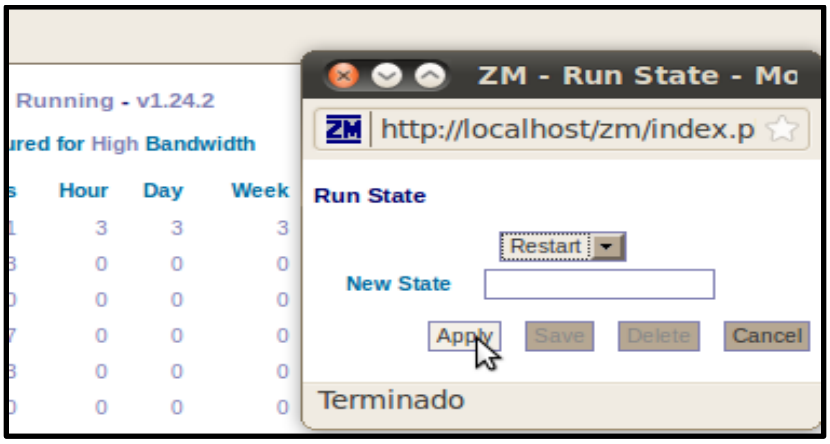
Record: En este estado se gravará continuamente eventos con una longitud de tiempo determinada sin que haya o no movimiento.

Mocord: Es un estado entre Modect y Record, y el resultado son eventos de longitud fija con las zonas de detección de movimiento remarcadas dentro de la misma zona.

Nodect: Este es un modo especial diseñado para ser usado con eventos externos.



9. En el caso de tener problemas con el ancho de banda, es recomendable reiniciar el ZoneMinder, por medio de la opción "Running".



10. Para salir del sistema se debe cerrar únicamente el navegador web.