UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y COMUNICACIONES

Tema:

"SISTEMA IP PARA PROVEER SEGURIDAD REMOTA A LA EMPRESA SISTELDATA S.A."

Trabajo de Graduación. Modalidad: TEMI. Trabajo Estructurado de Manera Independiente, presentado previo la obtención del título de Ingeniero en Electrónica y Comunicaciones.

AUTOR: Jorge Luis Freire Núñez

TUTOR: Ing. Mario Geovanni García Carrillo M.Sc.

Ambato –Ecuador

Septiembre 2012

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema: "SISTEMA IP PARA PROVEER SEGURIDAD REMOTA A LA EMPRESA SISTELDATA S.A.", del señor Freire Núñez Jorge Luis, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad técnica de Ambato.

.

Ambato septiembre 10, 2012

EL TUTOR

Ing. Mario Geovanni García Carrillo M.Sc.

AUTORÍA

El presente trabajo de investigación titulado: SISTEMA IP PARA PROVEER SEGURIDAD REMOTA A LA EMPRESA SISTELDATA S.A.

Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato septiembre 10, 2012

Jorge Luis Freire Núñez

CC: 1803814050

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Marco Antonio Jurado Lozada M.Sc e Ing. Juan Pablo Pallo Noroña M.Sc, revisó y aprobó el Informe Final del trabajo de graduación titulado: "SISTEMA IP PARA PROVEER SEGURIDAD REMOTA A LA EMPRESA SISTELDATA S.A.", presentado por el señor Jorge Luis Freire Núñez de acuerdo al Art. 18 del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad técnica de Ambato.

.

Ing. Oswaldo Eduardo Paredes Ochoa M.Sc.
PRESIDENTE DEL TRIBUNAL

Ing. Marco Antonio Jurado Lozada M.Sc.
DOCENTE CALIFICADOR

Ing. Juan Pablo Pallo Noroña M.Sc.
DOCENTE CALIFICADOR

DEDICATORIA:

El presente trabajo está dedicado con mucho cariño y entusiasmo, primeramente a nuestro ser supremo Dios, quien ha puesto a las personas indicadas en mi vida y me ha dotado de dones y virtudes. A mis padres Jorge y Teresa, pilares fundamentales en mi vida, a mis hermanas, hermano y sobrinos por contagiarme alegría; por ser quienes día a día a base de esfuerzo, cariño y comprensión me ayudaron a culminar con este anhelado logro.

Jorge Luis Freire Núñez

AGRADECIMIENTO:

Mi más sincero agradecimiento a la Universidad Técnica de Ambato por los conocimientos adquiridos.

Un especial agradecimiento a mi querida hermana Elena por todo su esfuerzo y dedicación para que esta meta personal se haya culminado con éxito.

Al Ing. Mario García por su paciencia y acertada dirección para culminar con éxito el presente proyecto.

A todos ellos mil gracias.

Jorge Luis Freire Núñez

ÍNDICE GENERAL

CAPÍTULO II

MARCO TEÓRICO

CAPÍTULO III

METODOLOGÍA

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

CAPÍTULO VI

PROPUESTA

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El presente trabajo denominado “SISTEMA IP PARA PROVEER SEGURIDAD REMOTA A LA EMPRESA SISTELDATA S.A.”, se refiere al diseño de un sistema de seguridad basado en cámaras con tecnología IP, este diseño está estructurado en seis capítulos en los cuales se detalla a continuación cada uno de ellos:

En el primer capítulo se determina el problema, el cual radica en la inexistencia de un sistema de seguridad en la empresa SISTELDATA S.A, lo que impidela seguridad de la misma. Además se determinan los objetivos que se desea alcanzar, proponiendo como punto principal el diseño de un sistema IP para brindar seguridad remota a la empresa.

En el capítulo dos se describen las bases teóricas para entender lo que posteriormente se plantea como solución al problema, se presenta el sistema IP haciendo una introducción y desarrollando la teoría para entender mejor el funcionamiento y conocer las ventajas y desventajas que ofrece el sistema de seguridad IP.

En el capítulo tres se describe la forma y métodos de cómo se procedió para resolver el problema.

En el capítulo cuatro se describe la situación actual de la empresa, se hace un análisis de los resultados de la encuesta aplicada entre los empleados de la empresa.

Las conclusiones que se determinan se refieren principalmente a las necesidades que la empresa tiene en cuanto a seguridad, pero teniendo también en cuenta las especificaciones del cliente. Además se realizan recomendaciones con el fin de dar la solución a futuras aplicaciones.

En el capítulo seis de la propuesta se habla de los pasos a seguir para realizar el diseño del proyecto, averiguando lo que quiere el cliente y posteriormente llevado a cabo la elección, ubicación y funcionamiento de los equipos a instalar, como la configuración de los mismos, realizando también el presupuesto del sistema de seguridad para el edificio.

En la parte de anexos se adjunta la ficha técnica de los equipos a utilizar, así como también los planos de la implementación de cámaras y sensores, las cámaras con su ángulo de cobertura para cada área de la edificación, los planos fueron diseñados con el programa denominado AutoCAD, el cual es uno de los mejores programas utilizados en el diseño de planos.

INTRODUCCIÓN

La industria de Circuito Cerrado de Televisión (CCTV), continúa creciendo. En los últimos años el factor más importante es el creciente interés y demanda de los sistemas de vigilancia basados en cámaras IP.

El desarrollo tecnológico va muy por delante de la adaptación comercial del sector de la seguridad. El mercado ha reaccionado rápidamente y con entusiasmo en la implementación de los sistemas de seguridad remota basados en vigilancia mediante cámaras IP.

Los sistemas de seguridad remota con tecnología IP es un hecho ya que esta revolucionando las comunicaciones, ya no se trata de una tecnología que esta a prueba sino que su utilización es un recurso indispensable en lugares donde hay tránsito de personas.

La empresa ahorra una gran cantidad de dinero al poder usar en su infraestructura sistemas de seguridad remota IP, la cual acelera su evolución tecnológica. Así muchas empresas descubrieron los beneficios de esta tecnología como reducción significativa en el presupuesto de viajes, ahorro de tiempo para toma de decisiones y mayor capacidad de reacción de la empresa.

Un problema que tenían era la instalación de un estudio de uso exclusivo, que era la única solución disponible en ese entonces no estaba al alcance del presupuesto de todos, eso debido principalmente a que los proveedores de esta tecnología se las ingeniaban para que su marca no sea compatible con otra, por tal razón se procedió a estandarizar la tecnología de video vigilancia IP para evitar este monopolio.

Las razones principales por las cuales la popularización del sistema de video vigilancia IP son: la reducción de precios y la estandarización de protocolos de comunicación, que han permitido acceder a esta tecnología. Así, podemos ver que

una gran ventaja de estos nuevos servicios es el aumento del nivel de seguridad para los diferentes tipos de organismos a nivel mundial.

CAPÍTULO I
EL PROBLEMA DE INVESTIGACIÓN

1.1 Planteamiento del problema

1.1.1. Contextualización

En el ámbito mundial de las comunicaciones el avance tecnológico se ha desarrollado a grandes pasos a través de los años, cada vez hay mejores servicios y aplicaciones que requieren una mayor capacidad, calidad y seguridad de transmisión, para ello las compañías que ofrecen los servicios de sistemas de seguridad, han incrementado su capacidad de transmisión de información tanto en su ancho de banda como en su velocidad, y han implementado calidad de servicio en sus transmisiones, estas compañías han ido migrando de tecnología en tecnología con el transcurso de los años.

La variedad de sistemas de seguridad,los cuales son ofertados por las diferentes empresas dedicadas al servicio de seguridad, están permitiendo que en el Ecuador se vayan implementando sistemas de seguridad de última tecnología, dependiendo de los requerimientos del cliente que se siente amenazado por la inseguridad que existe en cada provincia, esto permite el desarrollo de nuevas tecnologías en seguridad en varias provincias.

En la Provincia de Tungurahua se tiene varias empresas que ofertan los servicios de seguridad, con una diferencia que algunos cantones tienen un avance superior en los servicios que se ofrecen las mismas, mientras que en otros se oferta balos servicios en materia de seguridad, esto es un impedimento para las empresas que desean minimizar al máximo el riesgo de robos. En el cantón Ambato existen muchas empresas que brindan servicios de seguridad mediante el monitoreo de

alarmas, pero cada vez el desarrollo de los demás cantones y sus empresas advertirán la necesidad de proteger la inversión realizada en las empresas de la Provincia de Tungurahua, esto va a causar la expansión de estos servicios hacia todos los cantones.

La empresa SISTELDATA brinda los servicios de sistemas, telecomunicaciones y redes de datos a todo tipo de organizaciones, la cual también está expuesta a robos por parte de la delincuencia; pero no existe un sistema de seguridad de última tecnología que permita proteger la inversión de la empresa que brinda los servicios antes mencionados.

1.1.2. Análisis critico

La empresa al ser relativamente nueva no dispone de una tecnología que pueda proteger los bienes de la misma, esto está siendo un impedimento para el desarrollo de la empresa, lo que puede provocar pérdidas económicas debido al crecimiento de la delincuencia que cada vez se ingenia mejores formas para efectuar los robos.

Al no existir una infraestructura adecuada para proteger los bienes de la empresa, la cual se encuentra vulnerable al ataque de la delincuencia debido al costo de los equipos con los cuales la empresa realiza sus trabajos, actualmente la tecnología existente en el país no es suficiente para implementar un sistema de seguridad de última generación,

1.1.3. Prognosis

Si no se resuelve en un futuro esta situación, la empresa detendría su avance, habría pérdidas económicas considerables debido a costo de los equipos con los que cuenta, ya que los sistemas de seguridad existentes no satisfacen las necesidades que requiere la empresa.

1.2. Formulación del problema

¿De qué forma ayudaría el diseño de un sistema de seguridad IP para la empresa SISTELDATA?

1.2.1. Preguntas directrices

1.2.1.1 ¿Qué es un sistema IP?

1.2.1.2 ¿Qué es un sistema de seguridad?

1.2.1.3 ¿Qué tipo de protocolo de comunicación es el más adecuado?

1.2.2 Delimitación del problema

El diseño de un sistema de seguridad IP se lo realiza para la empresa SISTELDATA S.A. y se desarrolló en el periodo de 12 meses a partir de su aprobación por el Honorable Consejo Directivo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.3 Justificación

Es fundamental tener un sistema de seguridad de última generación el cual ofrezca las prestaciones adecuadas que garanticen la seguridad en la empresa con el fin de resguardar los bienes con los que cuenta la empresa.

La empresa SISTELDATA se beneficiara con la implementación de un sistema de seguridad que le permita la protección de sus bienes, con lo que podrá a la vez añadir a su línea de servicios este nuevo servicio con el cual captará una mayor cantidad de clientes que buscan estos servicios.

Los usuarios miran a la seguridad como un gasto más no como una inversión que pueda ayudarles a ahorrar y cuidar sus recursos económicos con lo que se ha perdido un gran mercado, esto ha motivado a la empresa SISTELDATA para iniciar una investigación acerca de los sistemas de seguridad IP d última generación con los cuales puede disminuir los costos en la contratación de estos servicios.

Este proyecto investigativo es factible en todo ámbito ya que existe una gran cantidad y fuentes de información tales como internet, libros, artículos técnicos,

además se cuenta con la colaboración de la empresa SISTELDATA que proporcionará la ayuda necesaria para la investigación que se pretende realizar.

1.4 Objetivos de la investigación

1.4.1. Objetivo general

Diseñar un sistema IP para proveer seguridad remota a la empresa SISTELDATA S.A.

1.4.2 Objetivos específicos

1.4.2.1 Analizar las políticas de seguridad utilizadas en la empresa.

1.4.2.2 Determinar los alcances técnicos y seguridad de los sistemas IP

1.4.2.3 Plantear una propuesta que permita proveer seguridad remota a la empresa SISTELDATA S.A. a través del uso de tecnología IP.

CAPÍTULO II
MARCO TEÓRICO

2.1 Antecedentes Investigativos

Previa la investigación realizada en los archivos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato existe un proyecto de pasantía sobre "DISEÑO DE UN SISTEMA DE SEGURIDAD MEDIANTE CAMARAS IP PARA LA EMPRESA PROALPI DE LA CIUDAD DE PILLARO" elaborado por Cecilia Izurieta Pazmiño, así como también un trabajo de graduación mediante seminario denominado "DISEÑO DE UN SISTEMA DE VIDEO VIGILANCIA IP PARA EL CONTROL Y MONITOREO REMOTO DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL DE LA UNIVERSIDAD TECNICA DE AMBATO", elaborado por Washington Giovanny Amancha,los mismos que servirán como soporte para desarrollar el proyecto de investigación.

2.2 Fundamentación

2.2.1. Fundamentación Legal

El presente proyecto esta basado en las leyes de comunicaciones así como los reglamentos de la Constitución de la República del Ecuador, las cuales son controladas por el CONATEL, el mismo que regula la implementación de tecnologías en comunicaciones de la empresa SISTELDATA S.A. que tiene su propio reglamento interno de la empresa, el proyecto también cumple con los requisitos en el aspecto legal del Reglamento de graduación de la Universidad Técnica de Ambato.

2.2.2. Categorías fundamentales

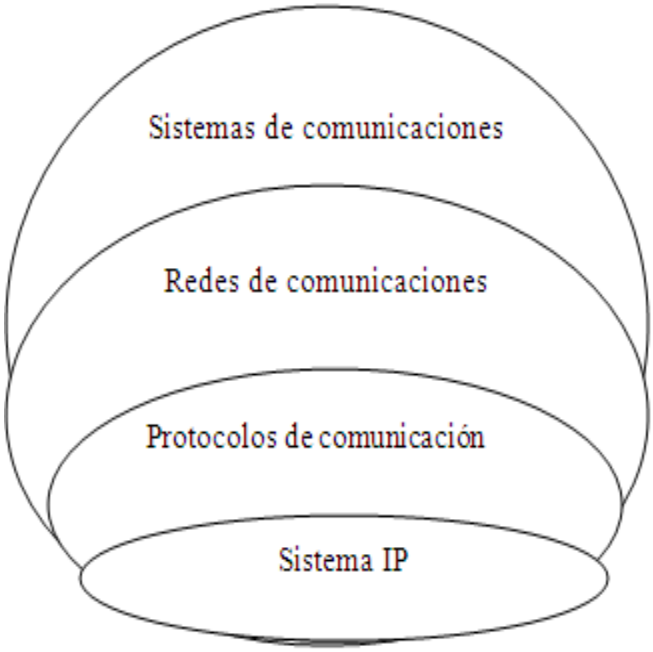


Figura 2.1 Variable Independiente

Fuente: Investigador

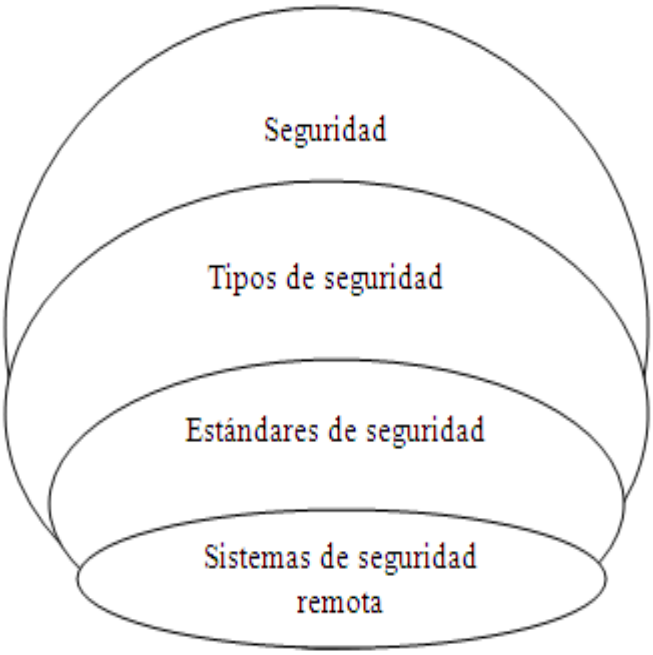


Figura 2.2 Variable Dependiente

Fuente: Investigador

2.2.2.1. SISTEMAS DE COMUNICACIONES[1]

Sistema de comunicación es el conjunto de elementos que intervienen en el proceso de intercambio de información.

2.2.2.2 Modelo De Un Sistema De Comunicaciones

La Comunicación es la transferencia de información desde un lugar (remitente, origen, fuente, transmisor) a otro lugar (destino, receptor). Por otra parte información, es un patrón físico al cual se le ha asignado un significado comúnmente acordado. El patrón debe ser único (separado y distinto), capaz de ser enviado por el transmisor, y capaz de ser detectado y entendido por el receptor.

Si la información es intercambiada entre comunicadores humanos, por lo general se transmite en forma de sonido, luz o patrones de textura en forma tal que pueda ser detectada por los sentidos primarios del oído, vista y tacto. El receptor asumirá que no se está comunicando información si no se reciben patrones reconocibles.

En la figura 2.3, se muestra un diagrama a bloques del modelo básico de un sistema de comunicaciones, en éste se muestran los principales componentes que permiten la comunicación.

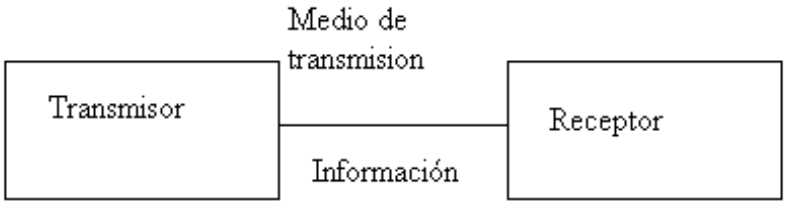


Figura 2.3 Elementos del sistema de comunicaciones

Fuente: Investigador

En toda comunicación existen tres elementos básicos (imprescindibles uno del otro) como son:

[1] http://pdf.rincondelvago.com/sistemas-de-comunicaciones.html

a) El transmisor
b) El canal de transmisión
c) El receptor.

Cada uno tiene una función característica como se indica a continuación:

a) El Transmisores el elemento encargado depasar el mensaje que se desea transmitir, al canal de transmisión en forma de señal. Para lograr una transmisión eficiente y efectiva, se deben desarrollar varias operaciones de procesamiento de la señal. La más común e importante es la modulación, un proceso que se distingue por el acoplamiento de la señal transmitida a las propiedades del canal de transmisión, por medio de una onda portadora.

b) El Canal de Transmisión o medio es el enlace eléctrico entre el transmisor y el receptor, siendo el puente de unión entre la fuente y el destino. Este medio puede ser un par de alambres, un cable coaxial, el aire, etc.

Pero sin importar el tipo, todos los medios de transmisión se caracterizan por la atenuación, la disminución progresiva de la potencia de la señal conforme aumenta la distancia.

c) El Receptor es el elemento encargado de extraer el mensaje emitido por el transmisor, que ha sido enviada en forma de señalpor el canal de transmisión, la señal es entregada al transductor de salida. Como las señales son frecuentemente muy débiles, como resultado de la atenuación, el receptor debe tener varias etapas de amplificación. En todo caso, la operación clave que ejecuta el receptor es la demodulación, el caso inverso del proceso de modulación del transmisor, con lo cual vuelve la señal a su forma original.

2.2.2.3 Comunicación de redes

La comunicación de redes es la interconexión de redes pequeñas llamadas LAN (Redes de Área Local), las cuales se comunican a través de medios físicos como cables de red, fibra óptica; y medios no físicos como ondas de radiofrecuencia, las cuales se propagan por medio del aire.

Red de redes[2]

Internet se ha convertido en el factor más potente que guía el proceso de convergencia. Esto es debido principalmente al hecho de que la suite del protocolo estándar utilizado en casi cualquier servicio. La suite del protocolo Internet está compuesto principalmente por el protocolo Internet (IP), y el protocolo de control del transporte (TCP); consecuentemente el término TCP/IP refiere a la familia del protocolo al completo. Las redes basadas en IP tienen una gran importancia en la sociedad de la información actual.

A primera vista esta tecnología puede parecer un poco confusa y abrumadora pero empezaremos por presentar los componentes de red subyacentes sobre los que está construida esta tecnología.

Una red se compone de dos partes principales, los nodos y los enlaces. Un nodo es cualquier tipo de dispositivo de red como un ordenador personal. Los nodos pueden comunicar entre ellos a través de enlaces, como son los cables. Hay básicamente dos técnicas de redes diferentes para establecer comunicación entre dos nodos de una red: las técnicas de redes de conmutación de circuitos y las de redes de conmutación de paquetes. La primera es la más antigua y es la que se usa en la red telefónica y la segunda es la que se usa en las redes basadas en IP.

Una red de conmutación de circuitos crea un circuito cerrado entre dos nodos de la red para establecer una conexión. La conexión establecida está dedicada a la comunicación entre los dos nodos. Uno de los problemas inmediatos de los circuitos dedicados es la pérdida de capacidad, dado que casi ninguna transmisión usa el 100% del circuito todo el tiempo. Además, si un circuito falla en el medio de una transmisión, la conexión entera se pierde y debe establecerse una nueva.

Por otra parte las redes basadas en IP utilizan la tecnología de conmutación de paquetes, que usa la capacidad disponible de una forma mucho más eficiente y que minimiza el riesgo de posibles problemas como la desconexión. Los mensajes enviados a través de una red de conmutación de paquetes se dividen primero en paquetes que contienen la dirección de destino. Entonces, cada paquete se envía a

[2] http://www.casadomo.com/casadomo/biblioteca/axis_las_redes_ip.pdf

través de la red y cada nodo intermedio o router de la red determina a donde va el paquete. Un paquete no necesita ser enrutado sobre los mismos nodos que los otros paquetes relacionados. De esta forma, los paquetes enviados entre dos dispositivos de red pueden ser transmitidos por diferentes rutas en el caso de que se caiga un nodo o no funcione adecuadamente como se muestra en la figura 2.4.

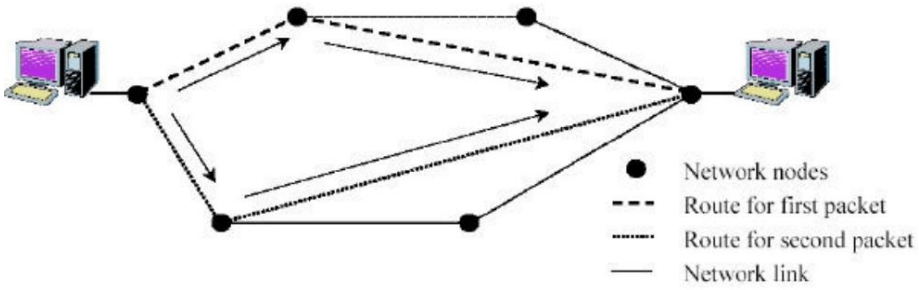


Figura 2. 4Una red de conmutación de paquetes enruta cada paquete de forma independiente

Fuente: http://www.casadomo.com/casadomo/biblioteca/axis_las_redes_ip.pdf

Soluciones de redes basadas en IP

Las soluciones de redes basadas en IP son sustitutos flexibles y económicos para soluciones que utilizan tecnologías de red antiguas. Las diversas propiedades entre estas tecnologías consisten en como se representa, gestiona y transmite la información. La información se estructura simplemente en colecciones de datos y entonces tiene sentido para la interpretación que le damos. Hay dos tipos principales de datos, analógicos y digitales y ambos poseen diferentes características y comportamientos. Los datos analógicos se expresan como ondas continuas variables y por tanto representanvalores continuos. Los ejemplos incluyen la voz y el vídeo.

Por otra parte los datos digitales se representan como secuencias de bits, o de unos y ceros. Esta digitalización permite que cualquier tipo de información sea representada y medida como datos digitales. De esta forma, el texto, sonidos e imágenes pueden representarse como una secuencia de bits. Los datos digitales pueden también comprimirse para permitir mayores ratios de transmisión y puede ser encriptada para su transmisión segura. Los datos digitales pueden ser

transmitidos a través de tres tipos generales de medios: metal, como es el cobre, fibra óptica u ondas de radio.

Las técnicas representadas en la figura 2.5 ofrecen el primer bloque de construcción para las comunicaciones digitales, el nivel de cable y antena. Este nivel permite enviar y recibir datos digitales sobre una amplia variedad de medios. En todo caso, se precisan más bloques de construcción para las comunicaciones digitales seguras.

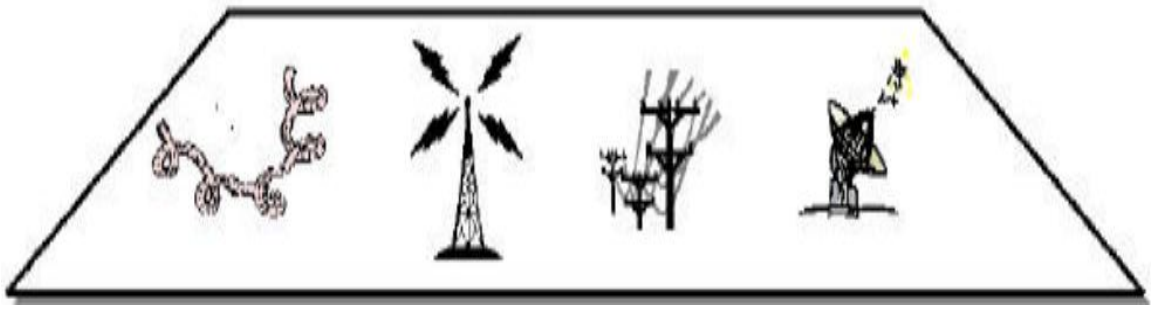


Figura 2.5Nivel de cable y antena; el primer bloque de construcción

Fuente:http://www.casadomo.com/casadomo/biblioteca/axis_las_redes_ip.pdf

2.2.2.4 REDES DE COMUNICACIONES[3]

Las redes o infraestructuras de telecomunicaciones proporcionan la capacidad y los elementos necesarios para mantener a distancia un intercambio de información y/o una comunicación, ya sea ésta en forma de voz, datos, vídeo o una mezcla de los anteriores.

Los elementos utilizados para la comunicación,deben disponer de acceso a la red de comunicaciones, el transporte de la información, los medios y procedimientos (conmutación, señalización, y protocolos para poner en contacto al transmisor y receptor que desean intercambiar información.

a) Conmutación

Conmutación es la conexión que realizan los diferentes nodos que existen en distintos lugares y distancias para lograr un camino apropiado para conectar dos usuarios de una red de telecomunicaciones. La conmutación permite la

[3] http://www.casadomo.com/casadomo/biblioteca/axis_las_redes_ip.pdf

descongestión entre los usuarios de la red disminuyendo el tráfico y aumentando el ancho de banda.

En las redes de comunicaciones, la conmutación se considera como la acción de establecer una vía, un camino, de extremo a extremo entre dos puntos, un emisor (Tx) y un receptor (Rx) a través de nodos o equipos de transmisión. La conmutación permite la entrega de la señal desde el origen hasta el destino requerido.

Mediante la conmutación de redes (una técnica de conexión utilizada con frecuencia hoy en día) puede dividirse un ordenador y una red de vigilancia IP físicos en dos redes lógicas autónomas. Las redes siguen conectadas físicamente, pero el conmutador de red las divide lógicamente en dos redes virtuales independientes.

b) Señalización

La señalización en telecomunicaciones se define como la comunicación que se da entre los equipos de telecomunicaciones, entre centros de procesamiento de información, entre la central y el abonado o entre bloques de software, para el establecimiento y liberación de los canales de comunicación, o para intercambiar información de gestión, tarificación, mantenimiento, etc.

c) Protocolos

Los protocolos son los conjuntos de reglas y convenciones que permiten la comunicación entre un mismo nivel o capa de dos máquinas diferentes. Los modelos de referencia OSI y TCP/IP contemplan el uso de protocolos distintos para cada una de las capas en que están definidos. La lista de protocolos utilizados por cada sistema se denomina pila de protocolos.

d) Redes de datos

Se denomina red de datos aquellas infraestructuras o redes de comunicación que se han diseñado específicamente para latransmisión de información mediante el intercambio de datos.

Las redes de datos se diseñan y construyen en arquitecturas que pretenden servir a sus objetivos de uso. Las redes de datos, generalmente, están basadas en la conmutación de paquetes y se clasifican de acuerdo a su tamaño, la distancia que cubre y su arquitectura física.

e) Red de Área Local (LAN)

Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).

Las redes de área local suelen ser una red limitada la conexión de equipos dentro de un único edificio, oficina o campus, la mayoría son de propiedad privada.

f) Red de Área Metropolitana (MAN)

Las redes de área metropolitanas están diseñadas para la conexión de equipos a lo largo de una ciudad entera. Una red MAN puede ser una única red que interconecte varias redes de área local LAN's resultando en una red mayor. Por ello, una MAN puede ser propiedad exclusivamente de una misma compañía privada, o puede ser una red de servicio público que conecte redes públicas y privadas.

g) Red de Área Extensa (WAN)

Las Redes de área extensa son aquellas que proporcionen un medio de transmisión a lo largo de grandes extensiones geográficas (regional, nacional e incluso internacional). Una red WAN generalmente utiliza redes de servicio público y redes privadas y que pueden extenderse alrededor del globo.

Interconexión de una LAN en una arquitectura basada en IP

La interconexión de LAN podemos observarla con mayor claridad en la figura2.6

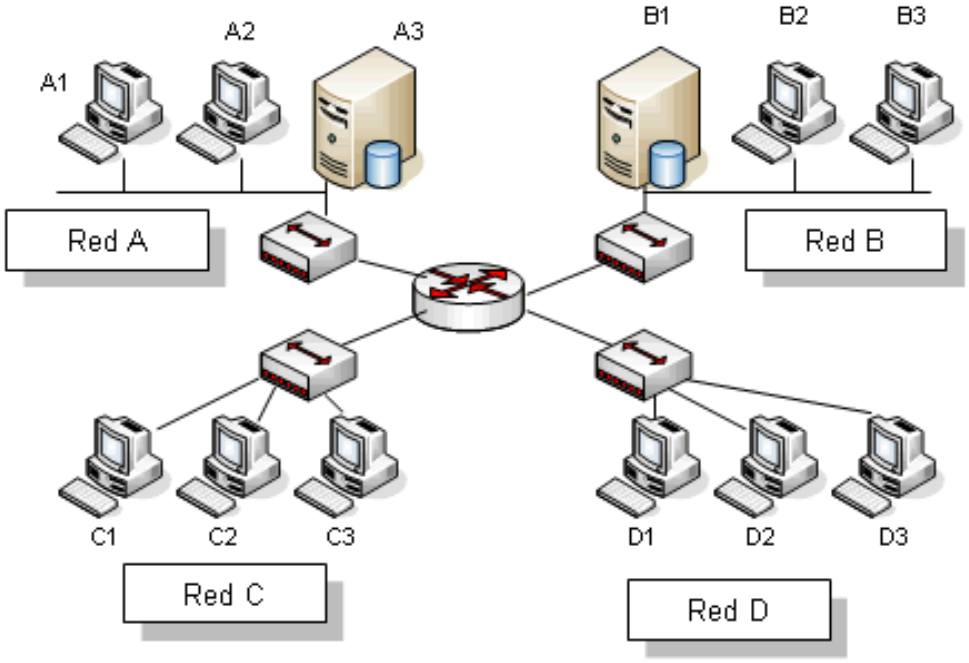


Figura 2.6: Interconexión de redes LAN

Fuente:http://www.google.com.ec/imgres?q=capas+del+sistema+osi&hl

Hasta ahora se ha descrito como los dispositivos de red comunican sobre diferentes tipos de LANs. En cualquier caso, las diferentes LANs están diseñadas para cubrir objetivos y necesidades diferentes. A veces es preciso interconectar varias LANs para extender la comunicación fuera de los límites de la red. Las colecciones de redes interconectadas, y geográficamente dispersas, se denominan *Redes de Área Extensa* (*Wide Area Network, WAN*). Probablemente la WAN más conocida sea Internet, que cubre la mayoría del planeta.

Es necesaria una arquitectura de comunicación compartida para todos los usuarios, ya sean personas privadas, empresas, oficinas de la administración pública u otras organizaciones, para ser capaces de intercambiar información digital con cualquier otro a través de una WAN.

Esta arquitectura debería ser un estándar abierto y soportar diferentes protocolos de nivel de transmisión, particularmente aquellos que pueden ser utilizados sobre una amplia variedad de medios de transmisión. Afortunadamente la suite del protocolo Internet ofrece una solución bien diseñada para ajustarse a estos requerimientos.

2.2.2.5 PROTOCOLOS DE COMUNICACIÓN[4]

Los protocolos de comunicación son reglas que permiten el flujo de información entre equipos que manejan lenguajes distintos, por ejemplo, dos computadoras conectadas en la misma red pero con protocolos diferentes no podrían comunicarse jamás, para ello, es necesario que ambas "hablen" el mismo idioma. El protocolo TCP/IP fue creado para las comunicaciones en Internet. Para que cualquier computador se conecte a Internet es necesario que tenga instalado este protocolo de comunicación.

Propiedades típicas de los protocolos de comunicación

Los protocolos de comunicación pueden variar mucho en propósito y sofisticación, la mayoría indica una o más de las siguientes propiedades:

- Detección de la conexión física subyacente (con cable o inalámbrica), o la existencia de otro punto final o nodo.
- Handshaking.
- Negociación de varias características de la conexión.
- Cómo iniciar y finalizar un mensaje.
- Procedimientos en el formateo de un mensaje.
- Qué hacer con mensajes corruptos o formateados incorrectamente (corrección de errores).
- Cómo detectar una pérdida inesperada de la conexión, y qué hacer entonces.
- Terminación de la sesión y/o conexión.

Niveles de abstracción de datos

Es la representación de las características esenciales del paquete de datos, esta abstracción de datoses una técnica o metodología que permite diseñar estructuras de datos.

Consiste básicamente en representar bajo ciertos lineamientos de formato las características esenciales de una estructura de datos.

[4] http://www.monografias.com/trabajos33/telecomunicaciones/telecomunicaciones.shtml

Este proceso de diseño se olvida de los detalles específicosde implementación de los datos.

En el campo de las redes informáticas, los protocolos se pueden dividir en varias categorías, una de las clasificaciones más estudiadas es la OSI.

Según la clasificación OSI, la comunicación de varios dispositivos ETD se puede estudiar dividiéndola en 7 niveles, que son expuestos desde su nivel más alto hasta el más bajo como se muestra en la tabla 2.1:

Nivel	**Nombre**	**Categoría**
Capa 7	Nivel de aplicación	Aplicación
Capa 6	Nivel de presentación	
Capa 5	Nivel de sesión	
Capa 4	Nivel de transporte	
Capa 3	Nivel de red	Transporte de datos
Capa 2	Nivel de enlace de datos	
Capa 1	Nivel físico	

Tabla 2.1 Capas del sistema OSI

Fuente: Investigador

A su vez, esos 7 niveles se pueden subdividir en dos categorías, las capas superiores y las capas inferiores. Las 4 capas superiores trabajan con problemas particulares a las aplicaciones, y las 3 capas inferiores se encargan de los problemas pertinentes al transporte de los datos.

Otra clasificación, más práctica y la apropiada para TCP/IP, se indica en la tabla2.2 que muestra cinco distintos niveles de capas:

Nivel
Capa de aplicación
Capa de transporte
Capa de red
Capa de enlace de datos
Capa física

Tabla2.2 Capas del sistema TCP/IP

Fuente: Investigador

Los protocolos de cada capa tienen una interfaz bien definida. Una capa generalmente se comunica con la capa inmediata inferior, la inmediata superior, y la capa del mismo nivel en otros computadores de la red. Esta división de los protocolos ofrece abstracción en la comunicación.

Una aplicación (capa nivel 7) por ejemplo, solo necesita conocer cómo comunicarse con la capa 6 que le sigue, y con otra aplicación en otro computador (capa 7). No necesita conocer nada entre las capas de la 1 a la 5. Así, un navegador web (HTTP, capa 7) puede utilizar una conexión Ethernet o PPP (capa 2) para acceder a la Internet, sin que sea necesario cualquier tratamiento para los protocolos de este nivel más bajo. De la misma forma, un router sólo necesita de las informaciones del nivel de red para enrutar paquetes, sin que importe si los datos en tránsito pertenecen a una imagen para un navegador web, un archivo transferido vía FTP o un mensaje de correo electrónico.

La suite del protocolo Internet

La suite del protocolo Internet es una familia de protocolos en niveles, en la que cada nivel se construye a partir del nivel inferior, añadiéndole nuevas funcionalidades. El nivel más bajo está ocupado exclusivamente en el envío y la

recepción de datos utilizando el nivel de transmisión. Los superiores son protocolos diseñados para tareas específicas como son el envío y la recepción de películas animadas, sonido e información de control. Los protocolos intermedios gestionan aspectos como la división de los mensajes en paquetes y el envío fiables entre dispositivos de red.

El protocolo Internet

El protocolo Internet (IP) es la base de la suite del protocolo Internet y es el protocolo de red más popular del mundo. El protocolo de Internet permite que se transmitan los datos a través y entre redes de árealocal, de ahí su nombre, inter-net protocol (protocolo entre redes). Los datos viajan sobre una red basada en IP en forma de *paquetes IP* (unidad de datos). Cada paquete IP incorpora unacabecera y los datos del propio mensaje, y en la cabecera se especifican el origen, el destino y otra información acerca de los datos.

IP Es un protocolo sin conexión de manera que cada paquete se trata como una entidad separada, como un servicio postal. Todos los mecanismos para asegurar que los datos enviados llegan de formas correctas e intactas los proporcionan los protocolos de más alto nivel dentro de la suite.

Cada dispositivo de red tiene al menos una dirección IP que lo identifica de forma única delresto de dispositivos de la red. De esta manera, los nodos intermedios pueden guiar correctamente un paquete enviado desde el origen a su destino.

El protocolo de Transporte

El Protocolo de Control del Transporte (*Transport Control Protocol, TCP*) es el protocolo más común para asegurar que un paquete IP llega de forma correcta e intacta. TCP ofrece la transmisión fiable de datos para los niveles superiores de aplicaciones y servicios en un entorno IP. TCP proporciona fiabilidad en la forma de un envío de paquetes de extremo a extremo orientado a conexión a través de una red interconectada.

2.2.2.6 SISTEMA IP[5]

El desafíos más importante de lo que se supone constituirá la nueva generación de redes IP en esta investigación, será la implementación de servicios de seguridad mediante cámaras IP, multiconferencia, multimedia y los diferentes protocolos a emplear. Además de la introducción de nuevos servicios, Con esta idea, aparte de tener que tratar los problemas típicos asociados a los servicios en tiempo real (como la QoS), debemos tener en cuenta la necesidad de buscar mecanismos de señalización y control que permitan un despliegue eficaz de los servicios suplementarios.

Los dos enfoques más prometedores son el conjunto de protocolos que la ITU-T ha desarrollado bajo la denominación de H.323, y la propuesta del lado del IETF: el SIP. Aunque la arquitectura que proponen es muy similar, se pueden encontrar profundas diferencias en su planteamiento. H.323 es la solución más madura, y ha seguido un desarrollo orientado principalmente a la Telefonía IP (TIP), centrándose, por tanto, en la interoperabilidad con la PSTN y el soporte de los servicios suplementarios. SIP se ha desarrollado sin embargo con un objetivo mucho más amplio, centrándose en la provisión del desarrollo de nuevas funcionalidades y servicios que no se vean coartadas en el futuro, es un protocolo pensado para aplicaciones que vayan más allá de la TIP (videoconferencia, streaming de vídeo, mensajería instantánea).

Integración IP

El estudio de la integración de IP sobre redes ópticas. Estudiando la encapsulación de los distintos niveles IP sobre los distintos niveles WDM. Analizando la gestión, la funcionalidad y arquitectura de las redes ópticas.

En un principio lo que se quiere exponer el estado actual y el desarrollo futuro de equipos y redes IP, de cómo WDM propone las medidas para implementar estas funciones y mejora la funcionabilidad de las redes.

Con este trabajo se pretende introducir aspectos importantes a tener en cuenta cuando se considera la posibilidad de IP sobre WDM. Provee un buen fondo para cualquiera que trabaje en lo concerniente a la reducción de la cabecera necesaria

[5] http://www.slideshare.net/ronaldreales/direccionamiento-ip-basico-i

para el transporte de paquetes IP en canales ópticos. Uno de los aspectos a tratar es la de tener una perspectiva de la capa IP. Mirar lo que está disponible en términos de funcionalidad, software y hardware en la capa IP.

El protocolo de Internet versión 6 (IP V6)[6]

El protocolo de Internet versión 6 (IPv6), es probablemente la mejor elección en las futuras redes IP sobre WDM. Esta investigación, muestra también el desarrollo al que tienden los routers y valorar los router Gigabit, así como estos forman la base para las redes de transporte IP sobre WDM. Algunos cambios en configuraciones de hardware están también identificados, esto es necesario a la hora de hacer routers capaces de manejar paquetes de velocidades de Gigabits, como usar switch en vez de buses. Esto muestra que para clasificar los paquetes IP dentro del flujo y conmutándolos en las capas inferiores en vez de enrutarlos, mirando las tablas de enrutamiento en cada nodo puede reducir significativamente la latencia de la red.

Técnica MPLS

Una técnica de la que hablaremos en particular es MPLS (MultiProtocolLabelSwitching) la cual fue propuesta por la IETF (Internet EngineeringTaskForce) y ya está implementada en muchos routers. MPLS tiene la ventaja de aliviar el peso de las largas tablas de enrutamiento en los routers y al mismo tiempo soporta la realización de funcionalidades de la red, como VPN (Virtual Private Network) y CoS (Class of Service). Las técnicas que se necesitan para la integración de la capa IP sobre la capa WDM, dando una visión general de los diferentes métodos de encapsulamiento de los paquetes IP preparándolos para ser transportados en una longitud de onda.

[6] http://www.plusformacion.com/Recursos/r/Sistemas-telecomunicaciones-Concepto-IP-nuevas-redes-Integradas

Transporte de paquetes IP[7]

En la adaptación de los paquetes IP sobre WDM se evalúa los diferentes mecanismos de encapsulación de la cantidad de cabecera necesaria para transportar los paquetes IP.

El trabajo muestra algunas de las posibilidades que WDM puede dar en términos de funcionalidad. Tres diferentes posibilidades se puede dar para soportar CoS usando longitudes de onda:

- Mejora en la capacidad de los nodos y por tanto CoS para sobre aprovisionamiento.
- Paso por los routers a través de enrutamiento de longitud de onda así como el decremento del retraso en las redes.
- Uso de longitudes de onda como etiquetas para la clasificación de CoS.

  También veremos las diferentes opciones de conexión cruzada y enrutado de los flujos IP la ayuda de las longitudes de onda y por consiguiente obteniendo una menor latencia en la red. En este, se identifican las tendencias predominantes en IP sobre WDM. Estas tendencias discutidas son:
- Routers más rápidos à 2,5 Gb/s de hoy a los 10 Gb/s.
- Aumento del número de longitudes de onda a 32 sistemas de longitudes de onda a 200 sistemas de canal.
- Moviendo el enrutamiento a las capas inferiores y aminorando la latencia de las redes.
- Nuevos protocolos dedicados a adaptar IP sobre WDM.
- Menor conversión de protocolos entre las distintas partes de la red.

Resumen de la suite del Protocolo Internet

La suite del protocolo Internet proporciona una adaptación a los protocolos de nivel de transmisión y ofrece una arquitectura estandarizada para las comunicaciones a través de una colección de LANs interconectadas. Esto representa un avance tremendo, principalmente por ser capaces de conectar y

[7] *http://www.monografias.com/trabajos29/direccionamiento-ip/direccionamiento-ip.shtml*

comunicar a través de diferentes conexiones físicas de una forma estandarizada. Con IP como base, la suite del Protocolo Internet ofrece el tercer bloque de construcción para unas comunicaciones digitales idóneas, el Nivel IP como se muestra en la figura 2.7.

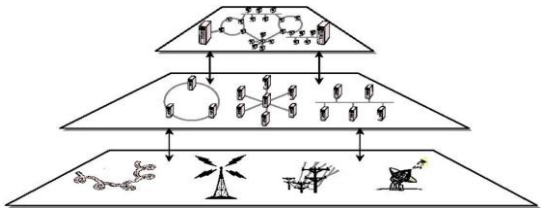


Figura 2.7 Suite del protocolo de Internet

Fuente:http://www.casadomo.com/casadomo/biblioteca/axis_las_redes_ip.pdf

La suite del protocolo Internet ha crecido rápidamente y se ha convertido en un bloque de construcción fundamental para el intercambio de información. A medida que la tecnología de comunicación se convierte en algo cada vez más importante, hay una presión creciente para usar esta tecnología para reducir costes sin sacrificar ninguna capacidad o beneficio. Las redes basadas en IP solucionan muchos de los problemas a los que se enfrenta en un entorno complejo, a la vez que proporciona una solución elegante que cubre las necesidades actuales y las venideras. Últimamente, todas las formas de comunicación que incluyan datos, voz imágenes en movimiento y entretenimiento convergirán en una red de transporte común.

Los beneficios primarios de una estrategia de redes basadas en IP son los ahorros de costes y las mejoras operacionales derivadas del uso de una red convergente frente a las de muchas redes pequeñas dedicadas a propósitos específicos como voz, datos o imágenes en movimiento. El segundo grupo de ventajas más importantes de las redes convergentes reside en su capacidad para crear nuevas aplicaciones. Las nuevas aplicaciones no sólo generan reducciones de costes, sino que pueden convertirse en fuentes de ingresos que ofrezcan un valor esencial a empresas y usuarios.

La convergencia está aquí y sus beneficios son reales. Ahora es el tiempo de elegir a los socios estratégicos, aquellos que entienden el amplio espectro de necesidades

y que se comprometen a solucionar, y a dar los primeros pasos hacia un futuro basado en IP.

Convergencia[8]

Las modernas tecnologías digitales permiten la convergencia entre diferentes servicios, y combinaciones de estos servicios, que pueden proporcionarse a través de infraestructuras acomodadas sólo a un tipo de servicio. Hay tres factores principales que crean las condiciones para la convergencia: la tecnología digital, la tecnología de transmisión y los protocolos de comunicación estandarizados. La tecnología digital permite que toda información ya sea texto, sonido o imágenes, por ejemplo, se representen como bits y se transmitan como secuencias de ceros y unos. La tecnología de transmisión permite una mejor utilización de la capacidad disponible en diferentes infraestructuras. Consecuentemente los servicios querequieren una alta capacidad pueden ser ofrecidos a partir de infraestructuras que previamente estaban disponibles para proporcionar unos servicios más simples.

Se ha observado como la tecnología basada en IP proporciona una arquitectura excelente para el imparable proceso actual de convergencia. En el corazón de la suite del Protocolo Internet está el Protocolo Internet que representa el bloque que conecta uniformemente diferentes redes físicas con una amplia variedad de aplicaciones. Además las soluciones disponibles actualmente y basadas en IP pueden integrarse totalmente con otros sistemas disponibles.

EL ANCHO DE BANDA[9]

El ancho de banda es la cantidad de tráfico de información que circula por una red de datos, el ancho de banda utilizado por los productos de vigilancia IP depende de la configuración de éstos. Por ejemplo, el uso de ancho de banda de una cámara depende de factores tales como:

- El tamaño de la imagen
- La compresión

[8] http://www.wordreference.com/definicion/convergencia
[9] http://www.alegsa.com.ar/Dic/ancho%20de%20banda.php

- La frecuencia de imagen por segundo
- La complejidad de la imagen

Hay muchas formas de aprovechar al máximo el sistema de vigilancia IP y administrar el consumo de ancho de banda, entre ellas se incluyen las siguientes técnicas:

Redes de altas velocidades de transmisión de datos: El precio de los conmutadores y enrutadores baja constantemente, por lo que las redes con capacidad para gigabytes son cada día más asequibles. Al reducir el efecto de la limitación del ancho de banda, las redes más rápidas aumentan el valor potencial de la vigilancia remota sobre red.

Frecuencia de imagen condicionada a sucesos: En la mayoría de las aplicaciones no es necesario disponer de 30 cuadros por segundo (cps) en todo momento en todas las cámaras. Las posibilidades de configuración y los sistemas inteligentes incorporados a las cámaras de red o el servidor de vídeo permiten establecer frecuencias de cuadro menores (por ejemplo, 1-3 cps), reduciendo drásticamente el consumo de ancho de banda. En caso de alarma, si está activada la detección de movimiento, la frecuencia de cuadro de la grabación puede aumentarse automáticamente hasta un nivel superior.

En la mayoría de los casos, la cámara sólo enviará vídeo a través de la red si merece la pena grabar las imágenes, es decir, se transmitirá a la red esta información si el sensor detector de movimiento de la cámara se activa.

2.2.2.7 SEGURIDAD[10]

La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la

[10] http://definicion.de/seguridad/

organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.

- **La información contenida:** Se ha convertido en uno de los elementos más importantes dentro de una organización. La seguridad informática debe ser administrada según los criterios establecidos por los administradores y supervisores, evitando que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario la organización corre el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando lecturas erradas o incompletas de la misma. Otra función de la seguridad informática en esta área es la de asegurar el acceso a la información en el momento oportuno, incluyendo respaldos de la misma en caso de que esta sufra daños o pérdida producto de accidentes, atentados o desastres.

- **La infraestructura computacional:** Una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y prever en caso de falla planes de robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

- **Los usuarios:** Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios

de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los funcionarios y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

2.2.2.8 TIPOS DE SEGURIDAD[11]

Toda persona que utilice los servicios que ofrece la red, deberá conocer yaceptar el reglamento vigente sobre su uso, el desconocimiento del mismo, noexonera de responsabilidad al usuario, ante cualquier eventualidad que involucre laseguridad de la información o de la red institucional.

En términos generales el manual de normas y políticas de seguridad informática, engloba los procedimientos más adecuados, tomando como lineamientos principales cuatro criterios, que se detallan a continuación:

Seguridad Organizacional

Es el marco formal de seguridad que debe sustentar la institución, incluyendo servicios o contrataciones externas a la infraestructura de seguridad, Integrando el recurso humano con la tecnología, denotando responsabilidades y actividades complementarias como respuesta ante situaciones anómalas a la seguridad.

Seguridad Lógica

La seguridad lógica establece e integra los mecanismos y procedimientos, que permitan monitorear el acceso a la red de algún intruso que intente ingresar a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a las aplicaciones y documentación sobre sistemas, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software malicioso.

[11] http://definicion.de/seguridad/

Seguridad Física

Es la seguridad enfocada a proteger los distintos equipos y dispositivos que conforman la red de comunicación.

Identifica los límites mínimos que se deben cumplir en cuanto a perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en la importancia de los activos

Seguridad Legal

Integra los requerimientos de seguridad que deben cumplir todos los empleados, socios y usuarios de la red institucional bajo la reglamentación de la normativa interna de políticas y manuales de procedimientos de la institución en cuanto al recurso humano, sanciones aplicables ante faltas cometidas, así como cuestiones relacionadas con la legislación del país y contrataciones externas.

Almacenamiento basado en el servidor

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

Por ejemplo, un disco duro con el software de gestión de vídeo AXIS Camera Station está preparado para almacenar grabaciones procedentes de seis hasta ocho cámaras. De 12 hasta 15 cámaras, se deben utilizar al menos dos discos duros para dividir la carga. Para 50 cámaras o más, se recomienda utilizar un segundo servidor.

Almacenamiento conectado a la red (NAS) y Red de almacenamiento por área(SAN)[12]

Cuando la cantidad de datos almacenados y los requisitos de gestión superan las limitaciones de un almacenamiento directamente conectado, como se tiene en la figura 2.8, un almacenamiento conectado a la red (NAS) o una red de almacenamiento por área (SAN) permite aumentar el espacio de almacenamiento, la flexibilidad y recuperabilidad.

Figura 2.8: Almacenamiento conectado a red.

Fuente: http://www.plusformacion.com/Recursos/r/Sistemas-telecomunicaciones-Concepto-IP-nuevas-redes-Integradas

El NAS proporciona un solo dispositivo de almacenamiento que está conectado directamente a una LAN y ofrece almacenamiento compartido a todos los clientes de la red. Un dispositivo NAS es fácil de instalar y administrar y ofrece una solución de almacenamiento rentable. Aún así, ofrece un caudal limitado para los datos entrantes porque sólo tiene una conexión de red, lo que puede provocar problemas en sistemas de alto rendimiento. Las SAN son redes especiales de alta velocidad para almacenamiento, conectadas típicamente por fibra a uno o más servidores. Los usuarios no pueden acceder a los dispositivos de almacenamiento de la SAN a través de los servidores y el almacenamiento es ampliable a cientos de terabytes. El almacenamiento centralizado reduce la administración y ofrece un conjunto de almacenamiento flexible de alto rendimiento para uso de entornos de multiservidores como se aprecia en la figura 2.9. La tecnología de canal de fibra se suele usar para ofrecer transferencias de datos a cuatro gigabytes por segundo y permitir que se almacenen grandes cantidades de datos con un alto nivel de redundancia.

[12] http://www.axis.com/es/products/video/about_networkvideo/bandwidth.htm

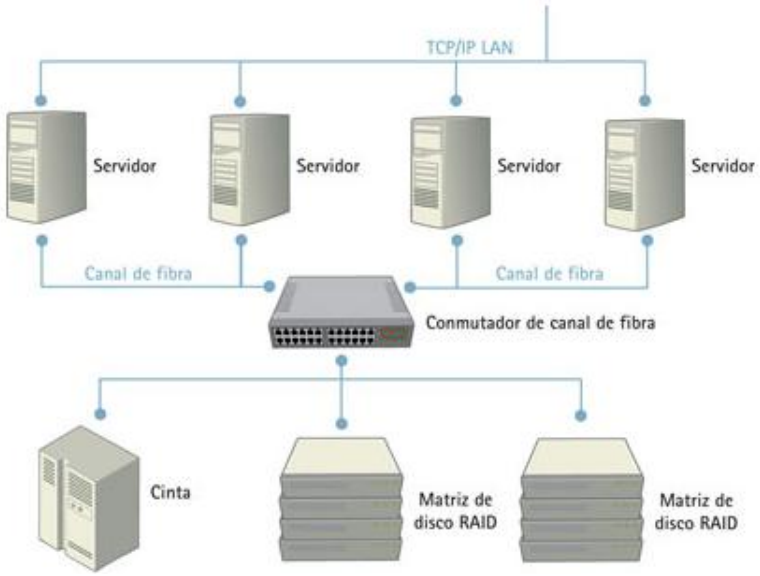


Figura 2.9: Arquitectura de SAN

Fuente:
http://www.axis.com/es/products/video/about_networkvideo/bandwidth.htm

Almacenamiento redundante

Los sistemas SAN generan redundancia en el dispositivo de almacenamiento. La redundancia en un sistema de almacenamiento permite guardar vídeo o cualquier otra información de forma simultánea en más de una ubicación. Esto proporciona una copia de seguridad para recuperar vídeo si una parte del sistema de almacenamiento no se puede leer. Existen varias opciones de ofrecer esta capa de almacenamiento añadida en un sistema de vigilancia IP con una matriz redundante de discos independientes (RAID), replicación de datos, agrupamiento de servidores y múltiples destinatarios de vídeo.

Matriz redundante de discos independientes (RAID), es un método de distribución de varios discos duros estándar, de modo que ante el sistema operativo funcionan como un gran disco duro. La configuración de RAID extiende datos por múltiples unidades de disco duro con suficiente redundancia a fin de que puedan recuperarse en caso de avería de la unidad. Existen diferentes niveles de RAID, desde prácticamente ninguna redundancia hasta una solución completa de duplicación de discos en la que no hay interrupción alguna ni se pierden datos en el evento de avería de unidad de disco.

Replicación de datos. Se trata de una función común en muchos sistemas operativos de red. Los servidores de archivos en una red se configuran para replicar los datos de uno a otro, de forma que proporciona una copia de seguridad si se produce una avería de un servidorcomo se muestra en la figura 2.10.

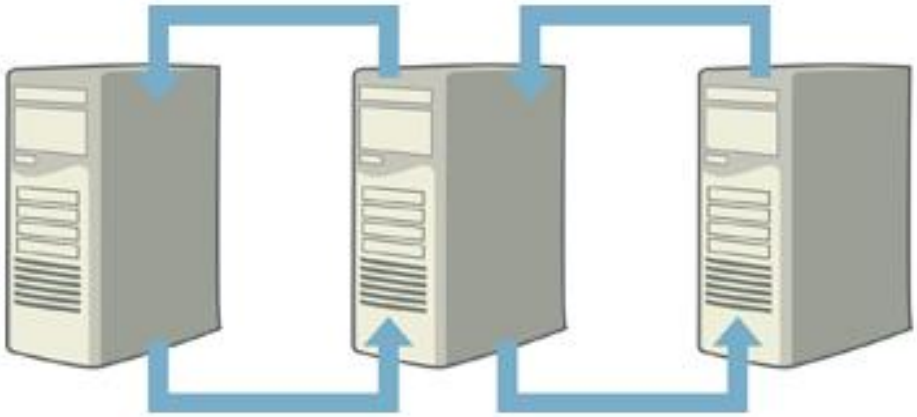


Figura 2.10 Replicación de datos.

Fuente:http://www.axis.com/es/products/video/about_networkvideo/bandwidth.htm

Agrupamiento de servidores

Un método común de agrupamiento de servidores es tener dos servidores trabajando con el mismo dispositivo de almacenamiento, como por ejemplo un sistema RAID. Cuando un servidor sufre una avería, el otro, que está configurado exactamente igual, se hace cargo. Estos servidores hasta pueden compartir la misma dirección IP, lo que hace la llamada "conmutación por error" totalmente transparente para los usuarios.

Múltiples destinatarios de vídeo

Un método habitual para garantizar una recuperación de desastres y un almacenamiento fuera de la instalación habitual en el vídeo en red es el envío simultáneo del vídeo a dos servidores distintos que se encuentran en emplazamientos diferentes. Estos servidores pueden estar equipados con RAID, funcionar en agrupamientos o replicar sus datos con servidores que incluso se encuentren mucho más lejos. Este es un enfoque especialmente útil cuando los

sistemas de vigilancia se encuentran en áreas de riesgo o de difícil acceso, como por ejemplo instalaciones de tránsito masivo o instalaciones industriales.

Configuraciones de sistema[13]

Sistema pequeño (1 a 30 cámaras)

Un sistema pequeño suele estar formado por un servidor que ejecuta una aplicación de vigilancia que graba el vídeo a un disco duro local. Un mismo servidor visualiza y gestiona el vídeo. Aunque la mayor parte de la visualización y gestión se realizará en el servidor, un cliente (local o remoto) puede conectarse con el mismo objetivo como tenemos en la figura 2.11.

Figura 2.11 Sistema pequeño

Fuente:http://www.axis.com/es/products/video/about_networkvideo/bandwidth.htm

Sistema mediano (25 a 100 cámaras)

Una instalación típica de tamaño mediano tiene un servidor con almacenamiento adicional conectado a él. El almacenamiento suele estar configurado con RAID con el fin de aumentar el rendimiento y la fiabilidad. El vídeo normalmente se visualiza y gestiona desde un cliente, más que desde el mismo servidor de grabación como tenemos en la figura 2.12.

[13] http://www.axis.com/es/products/video/about_networkvideo/bandwidth.htm

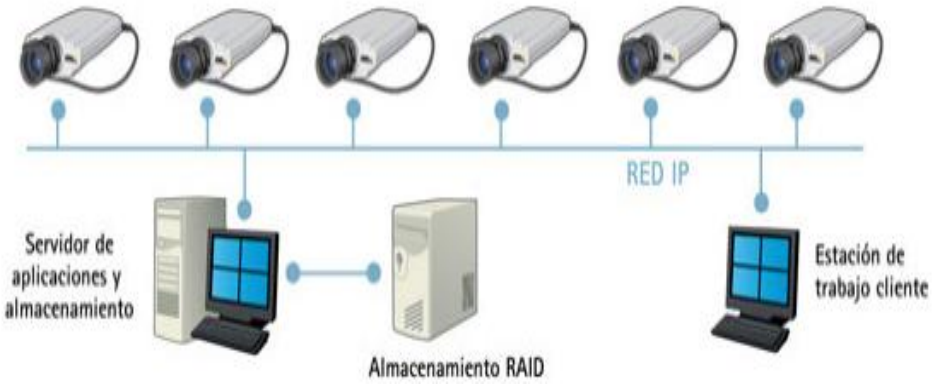


Figura 2.12 Sistema mediano

Fuente:http://www.axis.com/es/products/video/about_networkvideo/bandwidth.htm

Sistema grande centralizado (de 50 hasta +1.000 cámaras)

Una instalación de gran tamaño requiere un alto rendimiento y fiabilidad para gestionar lagran cantidad de datos y el ancho de banda. Esto requiere múltiples servidores con tareas asignadas. Un servidor maestro controla el sistema y decide qué tipo de vídeo se almacena y en qué servidor de almacenamiento. Al haber servidores de almacenamiento con tareas asignadas, se puede equilibrar la carga. En una configuración de estas características, también es posible escalar el sistema añadiendo más servidores de almacenamiento cuando se necesite y efectuar mantenimiento sin cerrar todo el sistemacomo tenemos en la figura 2.13.

Figura 2.13 Sistema amplio centralizado

Fuente:http://www.axis.com/es/products/video/about_networkvideo/bandwidth.htm

Sistema grande distribuido (de 25 hasta +1.000 cámaras)

Cuando varias ubicaciones requieren vigilancia con una gestión centralizada, se pueden utilizar sistemas de grabación distribuidos. Cada ubicación graba y almacena el vídeo procedente de las cámaras locales. El controlador maestro puede visualizar y gestionar las grabaciones en cada ubicacióncomo tenemos en la figura 2.14.

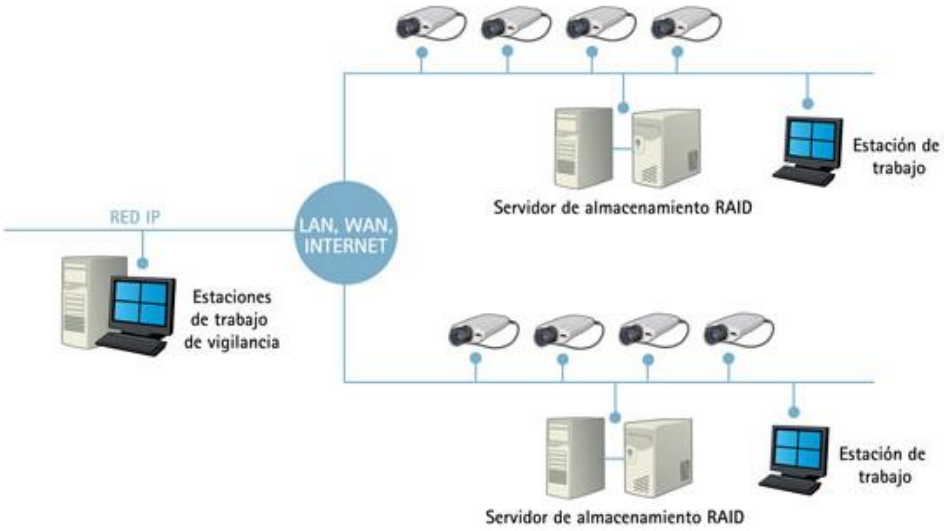


Figura 2.14 Sistema grande distribuido

Fuente:http://www.axis.com/es/products/video/about_networkvideo/bandwidth.htm

2.2.2.9 ESTÁNDARES DE SEGURIDAD[14]

La información y los procesos, sistemas y redes de apoyo son activos comerciales importantes. Definir, lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener una ventaja competitiva, el flujo de caja, rentabilidad, observancia legal e imagen comercial.

Las organizaciones y sus sistemas y redes de información enfrentan amenazas de seguridad de un amplio rango de fuentes; incluyendo fraude por computadora, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como código malicioso, pirateo computarizado o negación de ataques de servicio se hacen cada vez más comunes, más ambiciosas y cada vez más sofisticadas.

[14] http://www.sistemasdeseguridad.com.ec/pdf/AV-AVC796ZD.pdf

La seguridad de la información es importante tanto para negocios del sector público como privado, y para proteger las infraestructuras críticas. En ambos sectores, la seguridad de la información funcionará como un facilitador; por ejemplo para lograr e-gobierno o e-negocio, para evitar o reducir los riesgos relevantes. La interconexión de redes públicas y privadas y el intercambio de fuentes de información incrementan la dificultad de lograr un control del acceso. La tendencia a la computación distribuida también ha debilitado la efectividad de un control central y especializado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que se puede lograr a través de medios técnicos es limitada, y debiera ser apoyada por la gestión y los procedimientos adecuados. Identificar qué controles establecer requiere de una planeación cuidadosa y prestar atención a los detalles. La gestión de la seguridad de la información requiere, como mínimo, la participación de los accionistas, proveedores, terceros, clientes u otros grupos externos. También se puede requerir asesoría especializada de organizaciones externas.

Estándares conocidos

Aquí tenemos a los estándares más utilizados en la seguridad informática:

IS0/IEC 27000
X.805 de UIT-T
TCSEC (Orange Book)
ITSEC (White Book)
FIPS 140 (Federal Information Precessing Systems 140)
CC (Common Criteria)
COBIT (Control Objectives for Information and Related Technology)
ITIL (Information Technology Infrastructure Library)
OSSTMM (Open Source Security Testing Methodology Manual)

2.2.2.10 SISTEMAS DE SEGURIDAD REMOTA[15]

En redes de computadoras, acceder desde una computadora a un recurso ubicado físicamente en otra computadora, a través de una red local o externa (como internet).

En el acceso remoto se ven implicados protocolos para la comunicación entre máquinas, y aplicaciones en ambas computadoras que permitan recibir/enviar los datos necesarios. Además deben contar con un fuerte sistema de seguridad (tanto la red, como los protocolos y las aplicaciones).

Remotamente se puede acceder prácticamente a cualquier recurso que ofrece una o más computadoras. Se pueden acceder a archivos, dispositivos periféricos (como impresoras), configuraciones, etc. Por ejemplo, se puede acceder a un servidor de forma remota para configurarlo, controlar el estado de sus servicios, transferir archivos, etc.

Existen múltiples programas que permiten controlar una computadora remotamente, entre ellos uno de los más populares es el VNC, que es gratuito y libre. También existen aplicaciones web que permiten el acceso remoto a determinados recursos utilizando sólo un navegador web, ya sea a través de internet o cualquier otra red.

Otra forma fácil (porque es gráfica) de acceso remoto es a través de un escritorio remoto.

Existen programas para el acceso remoto a través de comandos de texto, pero suelen ser más complicados de usar.

Se ha desarrollado en variadas ocasiones proyectos en los que contemplan uno, dos o tres sistemas de seguridad electrónica y en la mayoría de los casos estos actúan de manera independiente; es decir que no poseen una plataforma central que les permita administrar los sistemas de seguridad. Esto ha motivado a los fabricantes a desarrollar y aplicar nuevos criterios de comunicación y plataformas de interacción que permitan al operador tener un control total de los sistemas de seguridad adquiridos, a groso modo un sistema integrado de seguridad electrónica está compuesto de los siguientes puntos:

[15] http://www.plusformacion.com/Recursos/r/Sistemas-telecomunicaciones-Concepto-IP-nuevas-redes-Integradas

1) Sistema de Acceso

2) Sistema de Intrusión

3) Sistema de Prevención de Incendio

4) Circuito Cerrado de Televisión (CCTV)

5) Plataforma de Integración

Antes de introducirnos en lo que son los sistemas de seguridad electrónica, hablaremos brevemente de la evolución de los protocolos de comunicación utilizados en este campo. Inicialmente se utilizaba el protocolo serial RS-232 para comunicaciones directas con la PC, luego se aplicó el RS-485 para comunicaciones de equipos en cascada, este utilizaba al final un convertidor RS-232 para tener comunicación con la computadora.

En la actualidad se mantienen estas comunicaciones pero la que ha permitido ir más allá en el tema de integración o interacción con los sistemas ha sido el protocolo de comunicación TCP/IP, que ha dado una nueva perspectiva a las formas de gestionar la seguridad electrónica, ya que este protocolo de redes ha borrado la barrera que hace un par de años existía en el tema de control de los sistemas por acceso remoto y centralización.

La integración no debe ser considerado como un capricho tecnológico, más bien debe ser evaluado como la forma innovadora que permite realizar, bajo la gestión de un software, el monitoreo en tiempo real de todos los sistemas de seguridad electrónica de la empresa. A continuación se describe algunas de las razones por la cual optar por la integración es una alternativa saludable:

- **CCTV**: Esta forma de trabajo reduce en gran medida el número de falsas alarmas ocasionadas por otros sistemas revisando los elementos que se encuentren bajo la cobertura de las cámaras, logrando la confirmación visual de la alarma anunciada.
- **Reducción de Redundancia:** Elimina la necesidad de manejar cada sistema por separado.
- **Relación costo/beneficio:** una sola plataforma que centralice todos los servicios implica una importante reducción de costos de mantenimiento, operación, etc.

- **Software amigable y autónomo:** La plataforma de integración presenta una interfaz amigable y autónomo; las tareas preventivas son automáticas, "saben" cómo actuar ante cada contingencia, evitan las falsas alarmas, detectan problemas técnicos, etc.
- **Acceso remoto:** empleando la comunicación TCP/IP es posible realizar las gestiones desde cualquier región.
- **Diseño según las necesidades del cliente:** Los sistemas electrónicos de seguridad se están desarrollando con la cualidad de que permita realizar la integración, esto da un mayor catálogo de productos permitiéndonos escoger las soluciones que más se adapten al cliente.

Control Energético

- La finalidad es satisfacer las necesidades del hogar al mínimo coste. En este control se pueden distinguir tres aspectos diferenciados:
- ***Regulación:*** con la que se pueda obtener la evolución del consumo energético dela vivienda o edificio.
- ***Programación:*** para programar distintos parámetros como temperatura según horarios, días de la semana, mes, etc.
- ***Optimización:*** de modo que se minimice el consumo. El aprovechamiento de la energía y reducción de su consumo, es uno de los apartados más importantes en la instalación de un sistema domótico, puesto que revierte a medio y largo plazo en su amortización, además de estar muy ligadas al concepto de confort.

Seguridad y alarmas.

El sistema de seguridad IP tiene un gran abanico de posibilidades. Se puede utilizar sensores de movimiento en las zonas principales de paso, sensores de magnéticos en puertas.

Monitorización, visualización, registro y operación.

Tanto en los edificios residenciales como en los funcionales a menudo es necesario grabar e informar de los estados de los distintos sistemas. Esto se refiere tanto al interior como al exterior del edificio.

Los datos registrados incluyen:

- Mensajes de funcionamiento (estados de operación), errores técnicos y alarmas.
- Datos de vigilancia relativos al exterior del edificio.
- Datos de vigilancia de personas (detección de movimiento).

Transmisión digital

El vídeo IP puede transmitirse casi a cualquier parte. No está limitado por un medio particular y actualmente es de uso común sobre redes LAN conmutadas a 10Mbit, 100Mbit y 1Gbit, sobre redes inalámbricas, RDSI, PSTN, PHS, CDCP y GSM. El medio de transmisión elegido por el desarrollador puede verse influenciado por el tipo de aplicación que está desarrollando.

Dentro de un edificio se recomienda el empleo de redes Ethernet a 100 Mbits. Es rápida y, debido a su popularidad, razonablemente barata.

Las redes Ethernet a 100 Mbit transmiten empleando cables de cobre de par trenzado. Este cable puede estar apantallado para evitar ruidos. La longitud de cable máxima está alrededor de100 metros. Si es necesario conectarse a distancias superiores existen diferentes dispositivos que lo hacen posible: fibra óptica o redes inalámbricas…

La velocidad de transmisión se expresa en bits por segundo. Un byte lo componen 8 bits. Para la transmisión de un byte se emplean, aproximadamente, otros dos bits adicionales para control, lo que supone que para transmitir un byte son necesarios 10 bits.

1byte/seg.~ 10 bits/seg.

1kbit/seg.~ 1000 bits/seg.

1Mbit/seg. ~ 1000 kbits/seg.

Ancho de banda = Tamaño del fichero x ratio de imágenes/seg. x 10

Para conectarse a redes existen diversos métodos de transmisión, que se describen a continuación, así como los dispositivos que lo hacen posible.

En la sociedad actual, la demanda de sistemas de vigilancia visual ha crecido enormemente. Se han usado diferentes soluciones de cámaras para monitorizar

actividades en una amplia variedad de entornos como son comercios, edificios de empresas o prisiones. Hasta hace muy poco, los sistemas de Circuito Cerrado de Televisión (sistemas CCTV) eran la única alternativa para este tipo de monitorización de actividades. Estos sistemas dedicados generalmente precisan un enlace de comunicaciones propio entre la cámara y el monitor. Este enlace separado es caro de comprar, instalar y mantener. Las imágenes de la cámara se transmiten sobre cableado de red dedicado hacia grabadores de lapsos de tiempo o a los monitores dedicados de un Centro de Control. Un moderno sistema de vigilancia visual basado en IP, por otras parte, no está limitado como los sistemas de CCTV tradicionales. Las empresas pueden instalar cámaras de red, cámaras de vigilancia visual basadas en IP que se conectan directamente a la red de la empresa. Cada cámara tiene su propia dirección IP como cualquier otro dispositivo de la red. Las principales diferencias entre estos sistemas y los sistemas de CCTV son que la digitalización del vídeo se lleva a cabo a nivel de cámara y la suite del protocolo Internet se utiliza para transferir las imágenes a través de la red. Esto es beneficioso dado que en casi todas las empresas existen redes actualmente y probablemente no sería necesario un cableado adicional Un sistema de cámaras de red, en comparación con un sistema de CCTV también ahorra dinero al reducir lacantidad de equipamiento necesario para gestionara el sistema de seguridad. Por ejemplo, no precisa monitores dedicados.

Una solución basada en IP también permite que las imágenes se almacenen remotamente y sean monitorizadas a través de cualquier red interconectada, como es Internet. Esto solo abre nuevas oportunidades para las empresas que deseen sub-contratar la monitorización de sus oficinas e instalaciones y facilita a una tercera parte un centro de vigilancia y monitorización. Este centro sólo necesita una contraseña y la dirección IP para acceder a las imágenes en directo, a través de Internet, desde una cámara localizada en cualquier lugar del mundo. Además, la arquitectura basada en IP crea un nuevo mundo de aplicaciones que pueden integrarse completamente. Por ejemplo, las imágenes en movimiento pueden distribuirse aotras soluciones de red, como pueden ser los sistemas de gestión de control de factorías y sistemas de control de accesos.

Conexión de la cámara de red a la red local[16]

A continuación se indica una instalación sencilla, con los siguientes componentes: PC, conmutador, cámara de red y cables Ethernet.

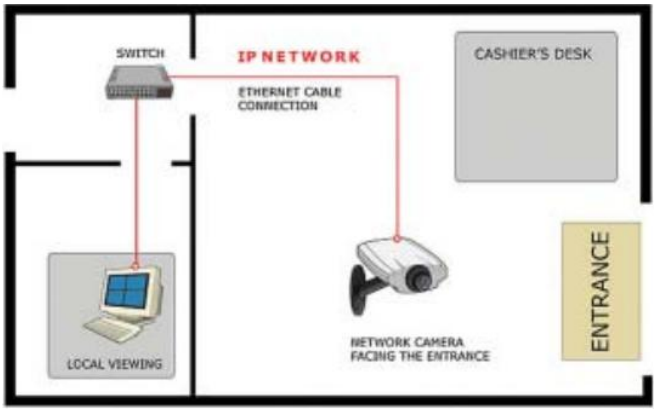


Figura 2.15: Conexión de la cámara a una red

Fuente:http://www.casadomo.com/casadomo/biblioteca/axis_las_redes_ip.pdf

Conexión de una cámara de red a Internet[17]

Ahora que sabemos como acceder a la cámara de red des de una PC local, explicaremos paso a paso como acceder a la cámara desde cualquier sitio remoto a través de Internet.

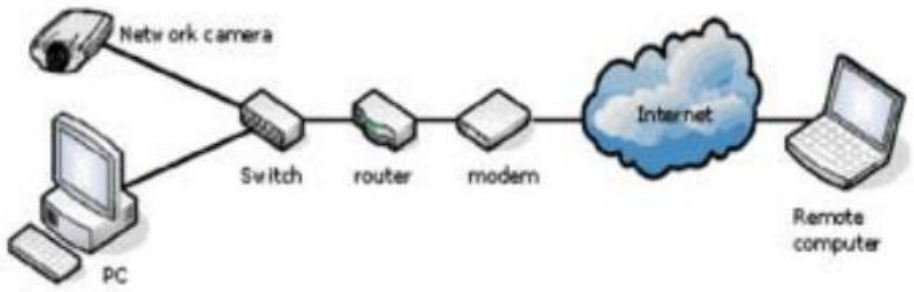


Figura 2.16: Conexión de la cámara a Internet

Fuente:http://www.casadomo.com/casadomo/biblioteca/axis_las_redes_ip.pdf

[16] http://www.casadomo.com/casadomo/biblioteca/axis_las_redes_ip.pdf
[17] http://www.casadomo.com/casadomo/biblioteca/axis_las_redes_ip.pdf

2.3 Hipótesis

El diseño de un sistema IP brindará seguridad remota a la empresa SISTELDATA S.A.

2.4 Determinación de variables

2.4.1. Variable independiente

Sistema IP

2.4.2. Variable dependiente

Sistema de seguridad remota

CAPÍTULO III
METODOLOGÍA

3.1 Enfoque

La presente investigación está enmarcada dentro de un paradigma crítico propositivo, tiene un enfoque cuali-cuantitativo ya que se trabajó con datos estadísticos, así como se tomará en cuenta la información que será proporcionada por la empresa SISTELDATA S.A., analizando todos los factores en sentido holístico, considerando una realidad en constante transformación; pero al mismo tiempo se da énfasis a los resultados.

3.2 Modalidad básica de la investigación

3.2.1 Investigación de Campo

Está basada en una investigación de campo porque se realizó visitas a la empresa en la cual se observó que el sistema de seguridad no existe, siendo este el principal problema en lo que respecta a la seguridad en la empresa.

3.2.2 Investigación Documental – Bibliográfica

Se realizó este tipo de investigación para conocer la manera como está estructurado el sistema de seguridad y las condiciones en las cuales fue elaboradoel sistema de seguridad remota IP, manejar este tipo de información lleva a un claro conocimiento, se observaron los parámetros respectivos para resolver el problema; por lo cual se llegó a un mejor criterio de la seguridad remota con tecnología IP para consecuentemente aprovechar todas sus ventajas y beneficios.

Se investigó toda la información mediante libros, revistas, información obtenida en páginas de Internet.

3.2.3 Proyecto Factible

Es un proyecto factible que permitió solucionar el problema, todos los objetivos planteados son de acuerdo a las condiciones que permitieron tener un monitoreo óptimo en el sistema de seguridad remota con tecnología IP, con los recursos que dispone la empresa y con los años estudiados en la carrera de Ingeniería en Electrónica y Comunicación de la Facultad, se tiene la total conocimiento y capacidad, con la cual se resolvió el problema enunciado en el tiempo estimado.

3.3 Nivel de Investigación.

El nivel exploratorio permitió determinar las características del problema que se encuentra actualmente en la empresa.

El nivel descriptivo facilitó con detalle el conocimiento de cómo es el problema, la magnitud, la frecuencia con que el problema se produce, áreas y personas afectadas; lo cual permitió tener una visión clara y concisa en la propuesta para la solución del problema.

El nivel correlacional facilitó la comparación de las variables como están dentro del contexto analizado por medio de procedimientos que ayudaron directamente a realizar un análisis del problema.

El nivel explicativo en el cual de manera detallada y profunda se procedió a la realización del sistema de seguridad remoto con tecnología IP.

3.4 Población y Muestra

3.4.1 Población

La población involucrada en el proyecto es de 15 personas.

Funciones del Personal	Nº de Personas	(%)
Gerente General	1	6.66
JefeTécnico	1	6.66
Secretaría	1	6.66
Técnicos	7	46.66
Contabilidad y Administración	1	6.66
Bodega	3	20
Mensajería y transporte	1	6.66
TOTAL	**15**	**100**

Tabla 3.1: Personal de la Empresa SISTELDATA S.A.

Fuente: Secretaría – Empresa SISTELDATA S.A.

Elaborado por: Investigador

3.4.2 Muestra

Como la población es reducida se trabajará con toda la población.

3.5 Operacionalización de variables

Variable Independiente: Sistema IP

CATEGORÍA	SUBCATEGORÍA	INDICADOR	ITEM	TÉCNICA
Sistema IP Se conceptúa como: Un sistema que permite realizar una comunicación utilizando una red IP ya sea mediante red de área local o a través de Internet.	Tecnología Control	Tipo Protocolo	¿Qué tipo de tecnología se utilizará en el sistema IP? ¿Cómo será el control del sistema IP?	• Encuesta

Tabla 3.2: Variable Independiente

Fuente: Investigador

Variable Dependiente: Sistema de seguridad remota

CATEGORÍA	SUBCATEGORÍA	INDICADOR	ITEM	TÉCNICA
Sistemas de seguridad remota Se conceptúa como: Es el acceso remoto donde se ven implicados protocolos para la comunicación entre máquinas, que permitan recibir o enviar datos desde los dispositivos de seguridad, que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta	Monitoreo Detección	Visualización Accionamiento del sistema de seguridad	¿Qué periodos en el día son los más inseguros en la empresa? ¿Qué debería detectar el sistema de seguridad? ¿Con qué dispositivos contará el sistema de seguridad?	Encuesta

Tabla 3.3: Variable Dependiente

Fuente: Investigador

3.6. Recolección de la información

La recolección de la información para el diseño de un sistema remoto IP para la empresa SISTELDATA S.A. se realizó mediante los datos proporcionados por la misma, ya que la empresa cuenta con poco personal y la oficina principal se encuentra ubicada en el sector de Pinllo de la ciudad de Ambato provincia de Tungurahua.

3.7 Procesamiento de la Información

Una vez aplicados los procedimientos y analizada la validez de la información se procederá a la ubicación de las áreas críticas, donde se establecerá cuales van hacer las áreas a proteger mediante el sistema de seguridad remoto, si se emplean medios de transmisión inalámbricos o alámbricos para el acceso a la red de cámaras. Se realizará el análisis integral en base a juicios críticos desprendidos del marco teórico, objetivos y variables de la investigación y juicios técnicos obtenidos de los datos tomados en el proceso investigativo.

A continuación se realizará las conclusiones y recomendaciones que organizadas lógicamente permitirán dar solución al problema plateado.

Finalmente como parte fundamental de la investigación crítica y propositiva se estructurará la propuesta pertinente al tema de investigación enfocada al diseño de un sistema IP para brindar seguridad remota a la empresa SISTELDATA S.A.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Análisis de los Resultados

En el presente capítulo se trata con la información obtenida por parte del investigador mediante una encuesta realizada al personal que labora en la empresa SISTELDATA S.A., a continuación se analiza los resultados por cada pregunta y al final de este capítulo se realiza un análisis general de la encuesta.

Interpretación de los datos de la encuesta sobre seguridad realizada al personal de la empresa SISTELDATA S.A.

- **Pregunta № 01:** ¿La empresa cuenta con un sistema de seguridad?

  Resultados tabulados de la encuesta aplicada al personal de la empresa SISTELDATA S.A.

Alternativa	Personas encuestadas	%
si	2	13.33
no	13	86. 67
total	**15**	**100**

Tabla 4.1: Cuenta con sistema de seguridad

Fuente: Investigador

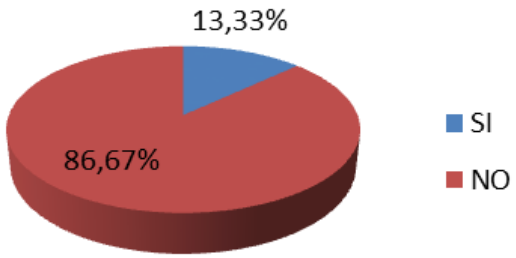


Figura 4.1: Cuenta con sistema de seguridad

Elaborado por: Investigador

Interpretación:

El 13,33% de los encuestados contestaron SÍ a la pregunta planteada y el 86,67% expresó un NO por respuesta.

Análisis:

El 86,67% de los encuestados respondieron que la empresa no cuenta actualmente con un sistema de seguridad, siendo este el problema que presenta la misma.

- **Pregunta № 02:** ¿Debería la empresa contar con un sistema de seguridad?

  Resultados tabulados de la encuesta aplicada al personal de la empresa SISTELDATA S.A.

Alternativa	Personas encuestadas	%
Si	14	93.33
No	1	6.67
total	**15**	**100**

Tabla 4.2: Debería contar con sistema de seguridad

Fuente: Investigador

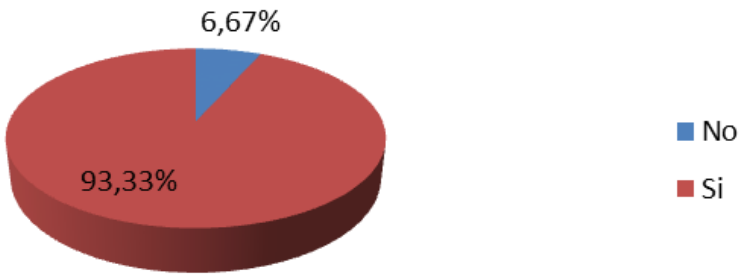


Figura 4.2: Debería contar con sistema de seguridad

Elaborado por: Investigador

Interpretación:

El 93,33% de los encuestados contestaron SÍ a la pregunta planteada y el 6,67% expresó un NO por respuesta.

Análisis: El 93,33% de los encuestados respondió que es necesaria la incorporación de equipos de seguridad en la empresa ya que se encuentran vulnerables ante la delincuencia.

- **Pregunta № 03:** ¿El monitoreo del sistema de seguridad se lo debería realizar desde cualquier lugar?

  Resultados tabulados de la encuesta aplicada al personal de la empresa SISTELDATA S.A.

Alternativa	Personas encuestadas	%
SI	14	93,33
NO	1	6,67
total	**15**	**100**

Tabla 4.3: Monitoreo remoto

Fuente: Investigador

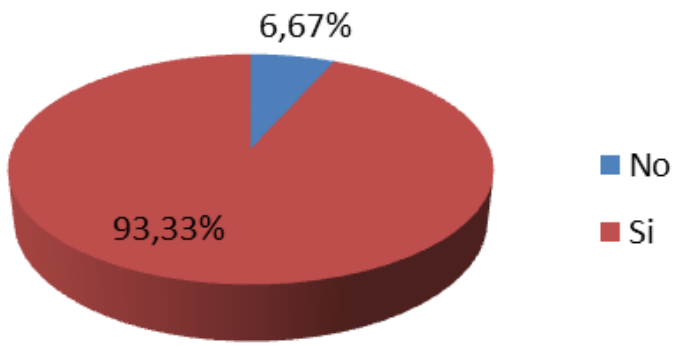


Figura 4.3: Monitoreo remoto

Elaborado por: Investigador

Interpretación:

El 93,33% de los encuestados contestaron SÍ a la pregunta planteada y el 6,67% expresó un NO por respuesta.

Análisis:

El 93,33% de los encuestados respondió que sería muy factible que el monitoreo del sistema de seguridad sea remota y que esta se la realizara desde cualquier lugar y a cualquier hora.

- **Pregunta № 04:** El sistema de seguridad tendría que contar con:

a. Cámaras
b. Sensores
c. Cámaras y sensores

Resultados tabulados de la encuesta aplicada al personal de la empresa SISTELDATA S.A.

Alternativa	Personas encuestadas	%
Cámaras	2	13,33
Sensores	2	13,33
Cámaras y Sensores	11	73,34
total	**15**	**100**

Tabla 4.4: Elementos del sistema de seguridad

Fuente: Investigador

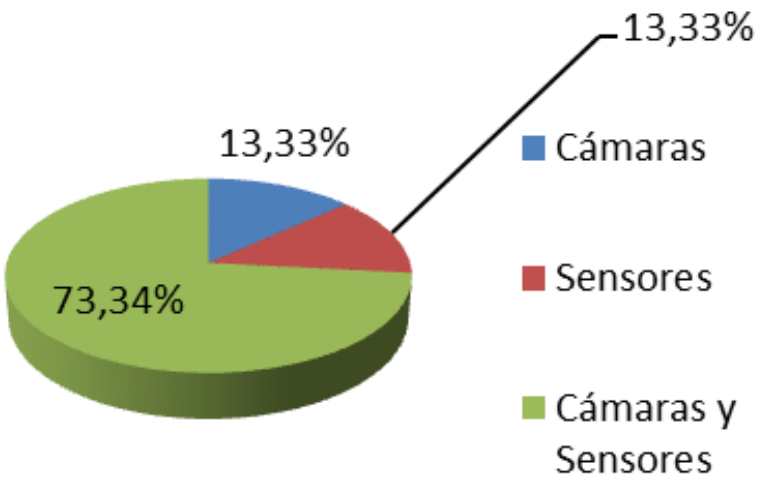


Figura 4.4: Elementos del sistema de seguridad

Elaborado por: Investigador

Interpretación:

El 13,33% de los encuestados contestaron que el sistema de seguridad debería contar solamente con Cámaras, el 13,33% de los encuestados contestaron que el sistema de seguridad debería contar solamente con sensores, mientras que el 73,34% de los encuestados contestaron cámaras y sensores.

Análisis:

El 73,34% de los encuestados respondió que el sistema de seguridad debería contar tanto con sensores como con cámaras para un mejor control sobre el monitoreo en las diferentes áreas de la empresa.

- **Pregunta № 05:** ¿Se debería utilizar un sistema de seguridad IP para brindar seguridad remota a la empresa?

  Resultados tabulados de la encuesta aplicada al personal de la empresa SISTELDATA S.A.

Alternativa	Personas encuestadas	%
SI	15	100
NO	0	0
total	**15**	**100**

Tabla 4.5: Sistema de seguridad IP

Fuente: Investigador

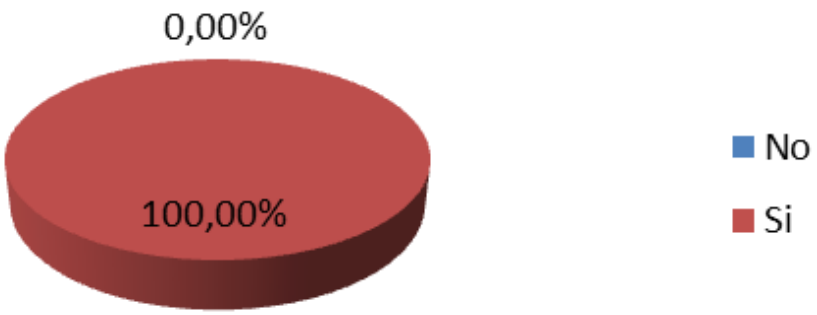


Figura 4.5: Sistema de seguridad IP

Elaborado por: Investigador

Interpretación:

El 100% de los encuestados contestaron SÍ a la pregunta planteada y el 0% expresó un NO por respuesta.

Análisis:

El 100% de los encuestados, es decir todos los empleados respondieron que SI se debería utilizar tecnología IP para la implementación del sistema de seguridad remota que se quiere desarrollar en la empresa.

ANÁLISIS GLOBAL DE LA ENCUESTA

Como se pudo observar en el análisis de resultados de cada pregunta realizada al personal de la empresa SISTELDATA S.A., severificó que la misma carece de un sistema de seguridad, para lo cual se debe implementar un sistema de seguridad con cámaras y sensores, el mismo que permitirá tener tranquilidad al propietario, como a los empleados de la empresa en lo que a seguridad se refiere, ya que podrán respaldarse en las grabaciones de las cámaras para la identificación de personas en caso de robo.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Evidentemente como muestra la encuesta, la empresa carece de un sistema de seguridad que proteja a la misma.
- El sistema de seguridad adecuado para la empresa es un sistema de seguridad remoto IP, el cual permita monitorear desde cualquier punto de conexión a Internet.
- Este sistema contará con cámaras de vigilancia las cuales permitirán tener acceso visual al entorno interno de la empresa, también debe contar con sensores los cuales permitirán saber exactamente que área y entrada fue activada.
- La empresa cuenta con cuatro plantas, en las cuales se ha distribuido los departamentos que conforman la empresa.
- Existen varios lugares dentro de la empresa, donde la cobertura de una cámara no será suficiente para visualizar toda un área

5.2 RECOMENDACIONES

- Implementar un sistema de seguridad remota en la empresa SISTELDATA S.A.
- El ancho de banda para este servicio debe ser superior al necesario para la red de cámaras para tener un adecuado flujo de información.
- Ubicar los dispositivos del sistema de seguridad remota como son las cámaras, en los lugares más vulnerables para que puedan ser monitoreados.
- Realizar un análisis de áreas críticas dentro de la empresa en las que requieran mayor vigilancia.
- No dejar puntos ciegos a las cámaras de seguridad para un eficaz monitoreo, si es necesario colocar más cámaras para cubrir estos puntos ciegos.

CAPÍTULO VI
PROPUESTA

6.1 Datos Informativos

6.1.1 Tema:

"SISTEMA IP PARA PROVEER SEGURIDAD REMOTA A LA EMPRESA SISTELDATA S.A."

6.1.2 Institución Ejecutora:

Universidad Técnica de Ambato - Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

6.1.3 Beneficiarios:

Investigador, Empresa SISTELDATA S.A, estudiantes de la FISEI.

6.1.4 Ubicación:

Provincia: Tungurahua.

Cantón: Ambato.

Parroquia: San Bartolomé

Dirección: El Ollero 06-85 y Aguacollas

6.1.5 Tiempo estimado para la ejecución:

Inicio: Septiembre/2011 – **Fin:** Septiembre/2012.

6.1.6 Equipo Técnico Responsable:

- Ing. Mario García M.Sc.
- Ing. Vinicio Torres
- Jorge Freire.

6.2 Antecedentes de la propuesta

La empresa SISTELDATA S.A. en la actualidad no cuenta con un sistema de seguridad lo cual la deja vulnerable a perdidas por robos o mala utilización de recursos.

El diseño para la instalación del sistema de Video Vigilancia IP tiene como propósito encontrar la mejor ubicación de las cámaras IP dentro de las instalaciones de la empresa SISTELDATA S.A., de tal manera que se alcance una cobertura de las áreas de interés con el menor número posible de cámaras.

Se determinará también el tipo de cámaras IP inalámbricas que se instalarán, pudiendo ser: fijas, móviles, con visión nocturna, con sensores de movimiento, para exterior o interior; tomando en cuenta el formato de compresión de imágenes que usarán.

6.3 Justificación

Es importante que el tema sea investigado, pues los resultados constituirán un referente importante no solo para las autoridades de la facultad y de la universidad , sino para todas las universidades y establecimientos educativos en general que desarrollan sus actividades dentro de la provincia y del país, y constituirán una orientación para que se puedan tomar las medidas preventivas de seguridad adecuadas, por tal motivo es de sumo interés utilizar un sistemas de seguridad remota IP confiable.

El impacto que tendrá la utilización de un sistema de seguridad remota IP en la empresa será muy alto porque permitirá detectar cualquier tipo de situación irregular que represente inseguridad y peligro para todos los miembros que forman parte de la misma.

El principal beneficiario con la realización del presente proyecto de investigación será la empresa SISTELDATA S.A., sus propietarios y por su puesto los empleados, porque se diseñará un sistema de seguridad que es altamente confiable, garantizando así, la seguridad de todos los que forman parte la empresa, así como la de las instalaciones del edificio.

El estudio se enmarca dentro de un proyecto factible porque se va a proponer un diseño de un sistema de seguridad remoto IP que proporcione una solución efectiva para el control y monitoreo de las instalaciones de un edificio, para la

orientación técnica se cuenta con el personal docente de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Además es una investigación similar ya aplicada en muchas empresas con resultados muy favorables.

6.4. Objetivos

General:

- Diseño de un sistema IP para proveer seguridad remota a la empresa SISTELDATA S.A.

Específicos:

- Analizar las políticas de seguridad utilizadas en la empresa.
- Determinar los alcances técnicos y de seguridad de los sistemas IP.
- Plantear una propuesta que permita proveer seguridad remota a la empresa SISTELDATA S.A. a través del uso de tecnología IP.

6.5. Análisis de factibilidad

Factibilidad Técnica

La propuesta se enmarca dentro de un proyecto factible debido a su alta disponibilidad de equipos en el mercado para diseño de seguridad mediante cámaras IP, lo conlleva a tener una propuesta viable para la empresa SISTELDATA S.A.

Factibilidad Operativa

La propuesta desde un punto de vista operativo es factible debido a que la empresa SISTELDATA S.A., cuenta con una infraestructura física como tecnología acorde a los requerimientos que se plantean son necesarios para realizar un sistema de seguridad remota al instalar cámaras IP.

Factibilidad Económica

La propuesta es factible desde el punto de vista económico puesto que la gerencia de la empresa al ser el propietario de la misma, al conocer los beneficios a obtener

con el sistema de seguridad remota, se encuentran con la disponibilidad de brindar los recueros financieros necesario para la futura implementación del proyecto.

6.6 Fundamentación Científico-Técnica

La propuesta está respaldada por la cantidad de libros acercade datos sobre IP, que se encuentran en la biblioteca de la Facultad de Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, así como también las páginas técnicas en el Internet y los conocimientos adquiridos en los años transcurridos en laFacultad de Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato por parte de los docentes en cada una de las materias, esto permite que de una manera confiable se cubra con todas las expectativas planteadas desde un inicio es decir tanto para la edificación así como para sus usuarios, brindando muchas alternativas en cuanto a servicios de seguridad que se pueden ampliar a futuro de acuerdo a las especificaciones de los equipos a utilizarse.

6.6.1 Descripción del Diseño

Los sistemas de seguridad basados en cámaras IP son sistemas de vigilancia remota digital de fácil manejo y que requiere un mínimo costo de mantenimiento.

6.6.2 Obtención de parámetros de diseño

Para el desarrollo del diseño del proyecto se seguirán los siguientes pasos:

- Realizar un reconocimiento de la edificación a la que se implantará el sistema, conocer las especificaciones del cliente, planimetría.
- Clasificar toda la información obtenida en las distintas funciones de seguridad
- Elegir fabricante de los equipos a utilizarse.
- Elección, situación, planimetría y función de los distintos elementos a instalar.

El principal propósito de la instalación del sistema de seguridad remota IP está en lograr la satisfacción del cliente y que esté perfectamente informado de todas las ventajas con las que cuenta dicho sistema para poder hacer uso de las mismas.

6.6.3 Reconocimiento de la edificación.

El reconocimiento de la edificación de la empresa permite una observación superficial acerca de la estructura a la que se va a proveer del sistema de seguridad.

Al realizar el reconocimiento exterior se obtuvo los siguientes datos:

Reconocimiento Exterior	Cuantificación
Número de plantas	4
Estacionamiento	2
Patios	2

Tabla 6.1: Reconocimiento exterior

Fuente: Investigador

Al realizar el reconocimiento interior se obtuvo los siguientes datos:

Planta Baja	Cuantificación
Número de habitaciones	2 oficinas
Número de estancias	1 estancias
Número de pasillos	1 pasillo

Tabla 6.2: Reconocimiento interior planta baja

Fuente: Investigador

Planta # 1	Cuantificación
Número de habitaciones	1bodega
Número de baños	2 baños
Número de pasillos	1 pasillos

Tabla 6.3: Reconocimiento interior planta alta 1

Fuente: Investigador

Planta # 2	Cuantificación
Número de habitaciones	2 oficinas
Número de estancias	1 estancias
Número de pasillos	1 pasillos

Tabla 6.4: Reconocimiento interior planta alta 2

Fuente: Investigador

Planta # 3	Cuantificación
Número de habitaciones	3 oficinas
Número de baños	1 baños
Número de pasillos	1 pasillos

Tabla 6.5: Reconocimiento interior planta alta 3

Fuente: Investigador

Luego de haber obtenido una visión general sobre la estructura procederemos a etiquetar las distintas habitaciones, ya que de acuerdo a su jerarquía y su ubicación física tomaremos en cuenta la seguridad y diseño.

6.6.4 Especificaciones del cliente.

Para un óptimo desarrollo del proyecto es necesario conocer las necesidades y especificaciones del cliente clasificando los servicios con los que contará el inmueble.

Entre los principales tenemos:

1 Análisis de áreas criticas

2 Definir áreas a proteger

3 Análisis de tecnología a utilizar

4 Costos

5 Ubicación del equipo designado como servidor

6 Diseñar el cableado

7 Diseño del sistema de Video Vigilancia IP

6.6.4.1 Análisis de áreas críticas y áreas a proteger

Basándonos en los planos y distribución de áreas que conforman la empresa podemos notar que las áreas críticas y de mayor tránsito de personas son las siguientes:

PLANTA BAJA:

- Pasillo
- Recepción
- Ventas
- Área Externa

PLANTA ALTA 1

- Pasillo
- Bodega

PLANTA ALTA 2

- Pasillo
- Técnicos
- Monitoreo y Equipos
- Cafetería

PLANTA ALTA 3

- Pasillo
- Gerencia
- Secretaría
- Jefe de Operaciones

Se ha considerado al pasillo y a la cafetería como áreas críticas a proteger por ser lugar de tránsito de personas, en los cuales se puede identificar a las mismas.

6.6.4.2Análisis de la tecnología

Considerando los altos costos de transmisión de datos en la telefonía móvil, se ha optado por utilizar Internet para el desarrollo del sistema de seguridad remota, para ello se analizaran los equipos tomando en cuenta las ventajas y desventajas que ofrecen los diferentes modelos y marcas de fabricantes.

Los sistemas de seguridad basados en cámaras IP son sistemas de vigilancia remota digital de fácil manejo y que requiere un mínimo costo de mantenimiento.

6.6.5 Elección de los distintos dispositivos del sistema.

De entre los más de 100 fabricantes que existen en todo el mercado se han elegido varias marcas en función del aparato a usar en este proyecto. Cabe recalcar que en nuestro país no existen muchas empresas que puedan ofrecer productos por lo que se necesitará proveedores extranjeros.

Los criterios de elección se basan en las características técnicas, precio, gama de productos, y uso actual de los elementos.

6.6.5.1 ELEMENTOS:

a) CÁMARAS

Para la elección de cámaras con sensores se ha optado por las siguientes marcas:

- **VIVOTEK**

Modelo: VI-IP7130

Figura 6.1: Cámara VIVOTEK Modelo: VI-IP7130

Esta cámara cuenta con las siguientes especificaciones técnicas:

CAMARA IP COLOR DIA/NOCHE 30FPS C/2 VIAS DE AUDIO CCD (3GPP) PROGRESIVO HR

Resolución: 640x480 / 0.2 Lux. Lente Varifocal A/I 2.9 - 8.2mm.

Compresión Dual-Codec (MJPEG / MPEG4)

Stream de Video: Dual

Conexión: TCP/IP, POE.

Alimentación: 110V.

Incluye: Software de 32ch. Lente, fuente y soporte.

Modelo: VI-IP7161

Figura 6.2: Cámara VIVOTEK Modelo: VI-IP7161

Esta cámara cuenta con las siguientes especificaciones técnicas:

CAMARA FIJA C/ICR DIA/NOCHE 2 M-PIXEL C/2 VIAS DE AUDIO, (3GPP)

Res: 1600x1200 a 15FPS - 1280x720 a 30FPS / 0.8 Lux .(4.5 - 10mm).

Compresión Dual-Codec (MJPEG / MPEG4)

Stream de Video: Múltiple

Conexión: TCP/IP, POE. Ranura para tarjeta SD.

Alimentación: 110V.

Incluye: Software de 32ch. Lente, fuente y soporte.

- **HIKVISION**

  Modelo: DS-2CD8153F-E

Figura 6.3: Cámara HIKVISION Modelo: DS-2CD8153F-E

Este equipo cuenta con las siguientes características:

CAMARA FIJA DIA/NOCHE 2 MEGAPIXEL C/AUDIO, (3GPP)

Res: 1600x1200 a 12,5FPS - 1280x960 a 25FPS / 0,1 Lux . (4mm).

Compresión Dual-Codec (MJPEG / H.264)

Stream de Video: Dual

Conexión: TCP/IP, POE. Ranura para tarjeta SD.

Alimentación: 110V.

Incluye: Software de 64ch. Lente y soporte.

Se ha optado por la cámara IP VIVOTEK VI-IP7153 por las características técnicas de las cuales goza dicha marca, costo de adquisición, garantía y suministro de repuestos, lo que la hace factible para este diseño.

b) GRABADORES PARA CÁMARAS IP

Para la elección de grabadores para cámaras IP (NVR) se ha optado por las siguientes marcas:

- **QNAP VioStar**

Modelo: VS8032U

Figura 6.4 NVR VioStar VS8032U

Especificaciones de hardware

Procesador: Procesador de 2,8 GHz de Intel Core 2 Duo

Memoria: 2 GB DDRII memoria RAM, 128 MB flash (DOM)

Capacidad de disco duro: 8 x bandeja de hot-swap y pueden cerrar con llave

Puerto LAN:2 x puerto RJ-45 Ethernet de Gigabit

Indicadores LED: Estado, LAN, USB, disco duro 1, 2, de la unidad de disco duro 3, de la unidad de disco duro HDD 4, 5, de la unidad de disco duro HDD6, HDD7, HDD8

USB: 4 x puerto USB 2.0Dispositivo de USB UPS de soportes

Panel LCD: Pantalla LCD con iluminación de fondo introduzca el botón, seleccione el botón configuración

Aviso acústico de alarma: Sistema de advertencia

Factor de forma: Montaje en rack de 2U

- **QNAPVioStar**

  Modelo: QN-VS-4016PRO

Figura 6.5: NVR QNAP Modelo: QN-VS-4016PRO

NVR 16CH P/CAMARAS IP VIVOTEK, HIKVISION, AXIS, D-LINK, TREDNET Y

OTRAS, MANEJO DE PTZ, SERIE PRO CON SALIDA VGA PARA MONITOR

Canales de Video: 16ch

Entradas: 2 LAN / serial / sata (2)

Grabación: MJPEG / MPEG4 / H.264

Backup: Vía USB

Conexión: TCP/IP

Discos Duros: Hasta 4HDD (Hasta 2TB c/u)

Incluye: Software de monitoreo remoto hasta 80ch

Alimentación: 110V

- **HIKVISION**

  Modelo: DS-9516NI-S

Figura 6.6: NVR HIKVISION Modelo: DS-9516NI-S

NVR 16CH P/CAMARAS IP HIKVISION

Canales de Video: 16ch

Entradas: 1 LAN / serial / sata (2)

Grabación: MJPEG / MPEG4 / H.264

Backup: Vía USB

Conexión: 10/100/1000Mbps TCP/IP HDD: Hasta 8HDD (Hasta 2TB c/u)

Incluye: Software de monitoreo remoto hasta 64ch

Alimentación: 110V

Se ha optado por el NVR de marca VioStar modelo VS8032U por las siguientes razones: garantía, características técnicas, coste.

c) MONITORES

LG

Modelo: W1943SS-PF

Figura 6.7: Monitor LG Modelo: W1943SS-PF

LCD de 19 Pulgadas a color

Alimentación: 120V

SAMSUNG

Modelo: S19B300N

Figura 6.8: Monitor SAMSUNG Modelo: S19B300N

LCD de 19 Pulgadas a color

Alimentación: 120V

Se optó por el monitor LG **m**odelo: W1943SS-PF por su resolución de pantalla mejor definida.

d) ROLLO DE CABLE DE 305m

Figura 6.9: Cable UTP

Cable NEXXT

Categoría: 5e

Liberty Cables

Categoría: 6

Se optó por utilizar la marca Liberty Cables categoría 6 por su costo en el mercado y prestaciones en seguridad anti-ruido ya que la categoría lo hace un cable mucho más eficaz en la transmisión de datos.

e) Software de aplicación

El software de aplicación está incluido en la adquisición del grabador de video (NVR)

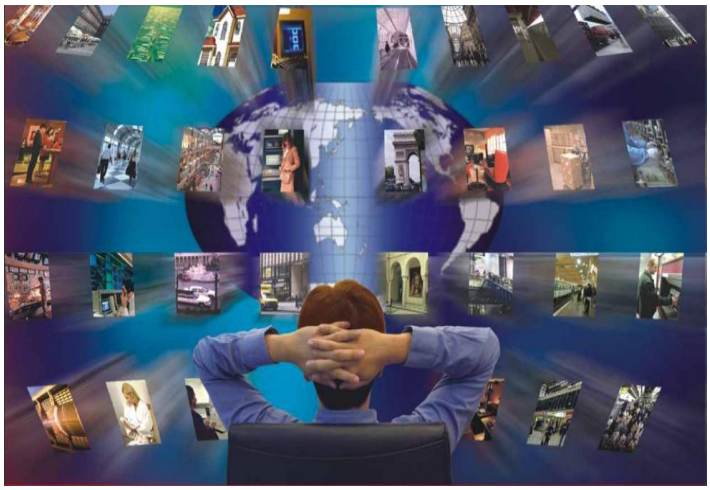


Figura 6.10: Central de monitoreo

Fuente: Guía de equipos TX series

Características:

- Aplicación para Windows de Microsoft.
- Hasta 80 canales de monitorización
- Resolución de grabación hasta D1
- Audio y Vídeo sincronizados
- Log del sistema, de sucesos, y contador de observadores.
- Backup a disco duro, DVD, CD y almacenamiento en red.
- Grabación por detección de movimiento
- Pantalla a tamaño completo
- Control PTZ integrado
- Visualización a través de móviles 3G
- Dispositivo de Entradas / Salidas integrado.

f) **Switch**

Switch Tp Link Tl-sl3428 Gestionado Gigabit-uplink 24 P + 4g

Figura 6.11: Switch Tp Link Tl-sl3428

Fuente: Guía de equipos TX series

Características

- El Vínculo IP-MAC-Port-VID, Seguridad de Puertos, Defensa DoS, Control de tormentas, el Snooping DHCP, la Autentificación 802.1X y el Radio le ofrece sus estrategias de seguridad robusta
- El Snooping L2/L3/L4 QoS y IGMP optimizar la aplicación de voz y video
- Los modos administrador por WEB/CLI, SNMP, RMON aporta una gran variedad de características de administración

g) Conectores RJ-45

Conector Macho RJ-45

Figura 6.12: Conector RJ-45

Fuente: Guía de equipos TX series

h) Canaletas

Canaleta Plástica Decorativa

Figura 6.13: Canaletas

Fuente: Guía de equipos TX series

i) Sirena para alarma VELSVPS5

La sirena electrónica marca Brielco se compone de una unidad de control que ha almacenado en el interior de la secuencia de tonos, y uno o dos altavoces conectados a esta unidad. El uso de sirenas electrónica está muy extendido, siendo especialmente adecuadas para su funcionamiento continuo, también tienen un bajo consumo eléctrico y no requieren mantenimiento, un ejemplo en la fig. 6.11.

La sirena electrónica de última generación utiliza altavoces muy potentes que permiten una mayor audibilidad y, por tanto, una mayor eficacia. Algunos incluso han llegado a 200 vatios de potencia cada uno, y se pueden integrar en el techo del vehículo o en el motor.

Figura 6.14 Sirena

Fuente: Guía de equipos TX series

Características:

- Sirena electrónica de gran potencia.
- Color: negro.
- Alimentación: 12Vdc.
- Dimensiones: 100 x Ø110mm.
- Peso: 430g.

j) Contacto magnético SM-226L-3

Es un componente electromecánico (fig. 6.12) de la marca Honeywell que tiene por objetivo establecer o interrumpir el paso de corriente, ya sea en el circuito de potencia o en el circuito de mando, tan pronto se energice la bobina (en el caso de ser contactores instantáneos).

Tiene la capacidad de cortar la corriente eléctrica de un receptor o instalación, con la posibilidad de ser accionado a distancia, que tiene dos posiciones de funcionamiento: una estable o de reposo, cuando no recibe acción alguna por parte del circuito de mando, y otra inestable, cuando actúa dicha acción. Este tipo de funcionamiento se llama de "todo o nada". En los esquemas eléctricos, su simbología se establece con las letras KM seguidas de un número de orden.

Figura 6.15 Contacto magnético

Fuente: Guía de equipos TX series

Características

- Contacto magnético blindado NA y NC de 70 mm. de rango.
- Reforzado para portones.
- Conducto flexible de acero inoxidable de 61 cm.
- Para ser montado sobre superficie, precableado enfundado.
- Montaje conto tornillo semi-empotrados.
- Abertura: 70mm.Enforcer, Seco-larm USA Inc.

k) **Alarma VELSVPS5**

Figura 6.16 Alarma

Fuente: Guía de equipos TX series

Características del equipo

- Activación
- Desactivación
- Excluir/Bypasear zonas
- Ver condición de falla
- Resetear detectores de humo
- Programar códigos de usuario
- Borrar código de usuario
- Programar código maestro
- Programar código Duress o de coacción (asaltado al ingresar)
- Armar presente (Stay)
- Programar fecha y hora del sistema.
- Prueba de sirena
- Activar avisador de zona (Chime)

- Pánicos por teclado

La tecnología de la cámara de red

Una cámara de red tiene su propia dirección IP y características propias de ordenador para gestionar la comunicación en la red. Todo lo que se precisa para la visualización de las imágenes a través de la red se encuentra dentro de la misma unidad. Una cámara de red puede describirse como una cámara y un ordenador combinados. Se conecta directamente a la red como cualquier otro dispositivo de red e incorpora software propio para servidor Web, servidor FTP, cliente FTP y cliente de correo electrónico. También incluye entradas para alarmas y salida de relé. Las cámaras de red más avanzadas también pueden equiparse con muchas otras funciones de valor añadido como son la detección de movimiento y la salida de vídeo analógico. El componente cámara de la cámara de red captura la imagen, que puede ser descrita como luz de diferentes longitudes de onda, y la transforma en señales eléctricas. Estas señales son entonces convertidas del formato analógico al digital y son transferidas al componente ordenador donde la imagen se comprime y se envía a través de la red.

Cámaras de red

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

Son dispositivos que contienen una cámara, un chip de compresión y un ordenador. Éste ordenador es pequeño y está especializado para aplicaciones en red.

Una cámara de red tiene su propia dirección IP y se conecta a la red como cualquier otro dispositivo; incorpora el software necesario de servidor de web, servidor o cliente FTP, de correo electrónico, etc. y tiene la capacidad de ejecutar pequeños programas personalizados (denominados scripts).

Constitución de las cámaras de red

Las cámaras IP internamente están constituidas por la "cámara" de Vídeo propiamente dicha (Lentes, sensor de imagen, procesador digital de señal), por un "motor" de compresión de imagen (Chip encargado de comprimir al máximo la información contenida en las imágenes) y por un ordenador" en miniatura (CPU, FLASH, DRAM, y módulo ETHERNET/ WIFI) encargado en exclusiva de gestionar procesos propios, tales como la compresión de las imágenes, el envío de imágenes, la gestión de alarmas y avisos, la gestión de las autorizaciones para visualizar imágenes, ... en definitiva, las cámaras IP son un equipo totalmente autónomo, lo que permite conectarlo en el caso mas sencillo directamente a un Router ADSL, y a la red eléctrica y de esta forma estar enviando imágenes del emplazamiento donde este situada. También es posible conectar las cámaras IP como un equipo más dentro de una Red Local, y debido a que generalmente las redes locales tienen conexión a Internet, saliendo de esta forma las imágenes al exterior de la misma manera que lo hace el resto de la información de la Red.

Las cámaras de red están equipadas con entradas y salidas digitales. La entrada digital puede ser usada para activar la transmisión de imágenes a la cámara.

Las salidas digitales se usan, por ejemplo, para abrir remotamente una puerta, o para encender o apagar una luz de una dependencia dentro de un edificio cuando se visualizan remotamente las imágenes.

Las cámaras de red con memoria (buffer) de imágenes pueden guardar y enviar las imágenes que fueron captadas antes de que ocurriera una alarma.

Servidor de video

En multitud de diferentes entornos de trabajo existen sistemas analógicos de seguridad basados en CCTV (Circuito Cerrado de TV). Para poder transmitir las imágenes de estos sistemas a través de una red es necesario instalar un servidor de vídeo IP. Se conecta en paralelo con el equipo ya existente y transmite las imágenes de fuentes de video analógicas a través de una red informática.

Utilizando los puertos serie incluidos en los servidores de vídeo es posible controlar el equipamiento ya existente, como grabadores de control de tiempo y cámaras PTZ (con movimiento vertical, horizontal y zoom), etc. Los servidores de

vídeo IP están equipados con entradas y salidas digitales. Las entradas se pueden usar para activar la transmisión de imágenes desde el servidor.

Los servidores que poseen memoria para imágenes pueden, además guardar y enviar las imágenes grabadas inmediatamente antes y después de la activación de una alarma.

Un servidor de video para red también se puede conectar a una amplia variedad de cámaras especiales, tales como una cámara súper sensible en blanco y negro, una cámara miniatura o una cámara microscópica.

En la figura 2.17 se muestra la conexión básica de un sistema de Video Vigilancia IP.

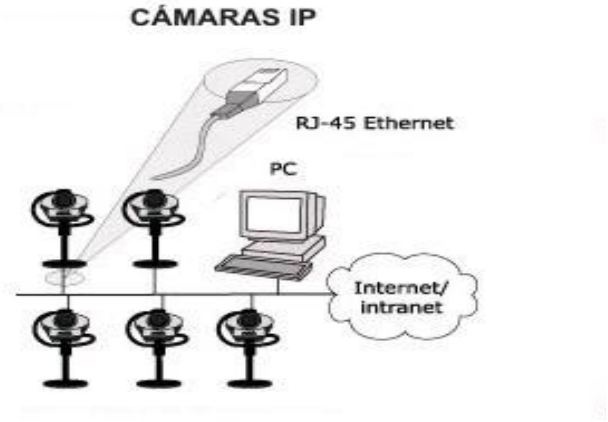


Figura 6.17:Diagrama básico de conexión de una cámara IP

Transmisión digital

El vídeo IP puede transmitirse casi a cualquier parte. No está limitado por un medio particular y actualmente es de uso común sobre redes LAN conmutadas a 10Mbit, 100Mbit y 1Gbit, sobre redes inalámbricas, RDSI, PSTN, PHS, CDCP y GSM. El medio de transmisión elegido por el desarrollador puede verse influenciado por el tipo de aplicación que está desarrollando.

Dentro de un edificio se recomienda el empleo de redes Ethernet a 100 Mbits. Es rápida y, debido a su popularidad, razonablemente barata.

Las redes Ethernet a 100 Mbit transmiten empleando cables de cobre de par trenzado. Este cable puede estar apantallado para evitar ruidos. La longitud de cable máxima está alrededorde 100 metros. Si es necesario conectarse a distancias

superiores existen diferentes dispositivos que lo hacen posible: fibra óptica o redes inalámbricas…

La velocidad de transmisión se expresa en bits por segundo. Un byte lo componen 8 bits. Para la transmisión de un byte se emplean, aproximadamente, otros dos bits adicionales para control, lo que supone que para transmitir un byte son necesarios 10 bits.

1byte/seg.~ 10 bits/seg.

1kbit/seg.~ 1000 bits/seg.

1Mbit/seg. ~ 1000 kbits/seg.

Ancho de banda = Tamaño del fichero x ratio de imágenes/seg. x 10

Para conectarse a redes existen diversos métodos de transmisión, que se describen a continuación, así como los dispositivos que lo hacen posible.

Estándares de compresión

Las imágenes digitales y las de vídeo digital se comprimen siempre con el fin de economizar espacio en los discos duros y para hacer más rápida la transmisión de las mismas. Los ratios (proporción) de compresión habituales están entre 10 y 100. Una imagen con una resolución de 640x480 píxeles ocupa aproximadamente 600 kB (2 bytes por píxel). Comprimiéndola 25 veces el tamaño de la imagen será de aproximadamente 25 kB.

Estándares de compresión de vídeo

Motion JPEG y MPEG-2 son dos formatos altamente recomendados. Son estándares internacionales ampliamente conocidos y muy usados que ofrecen vídeo de alta calidad.

MOTION JPEG

Con Motion JPEG cada imagen de una secuencia se almacena como una imagen completa en formato JPEG. Las imágenes estáticas se muestran a un alto ratio de imágenes por segundo para producir vídeo de alta calidad, aunque el precio de esta calidad implica que produce comparativamente ficheros de mayor tamaño.

MPEG 2

Moving Picture Encoding Group, estándarinternacional ISO/IEC 13818. Un estándar muy popular que ofrece vídeo de alta calidad adecuado para instalaciones en las que se precisa calidad TV. Existen numerosas variaciones de este formato aunque normalmente proporciona una resolución de 720x480 píxeles a 30 imágenes por segundo (NTSC) o 720x576 a 25 imágenes por segundo (PAL). El ratio de bits para transmisión está entre 1-10 Mbit/segundo. Un reproductor de MPEG 2 puede servir tanto para MPEG 2 como para MPEG 1.

Calidad de imagen

Si se compara las imágenes de diferentes cámaras se encontrará que la calidad de las mismas difiere considerablemente entre fabricantes y marcas. Estas variaciones de calidad dependen de varios factores y son especialmente apreciables en condiciones de poca luz.

Factores determinantes

Los principales factores que afectan a la calidad de las imágenes para lascámaras pueden definirse como sigue:

- La lente
- El filtro óptico
- El sensor de imágenes
- El procesador de señales digitales de la cámara
- El estándar de compresión y su implementación

Lista de control de acceso (ACL)[18]

Es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

[18] Referencia: http://es.wikipedia.org/wiki/Lista_de_control_de_acceso

Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición. Sin embargo, también tienen usos adicionales, como por ejemplo, distinguir "tráfico interesante" (tráfico suficientemente importante como para activar o mantener una conexión) en RDSI.

En redes informáticas

En redes informáticas, ACL se refiere a una lista de reglas que detallan puertos de servicio o nombres de dominios (de redes) que están disponibles en un terminal u otro dispositivo de capa de red, cada uno de ellos con una lista de terminales y/o redes que tienen permiso para usar el servicio. Tanto servidores individuales, como enrutadores pueden tener ACL de redes. Las listas de control de acceso pueden configurarse generalmente para controlar tráfico entrante y saliente y en este contexto son similares a un corta fuegos.

Existen dos tipos de listas de control de acceso:

- Listas fija, no cambia
- Listas variable, cambia

Detectores de movimiento

Los detectores de movimiento son útiles actuando sobre ciertas áreas de la edificación, lo cual ayuda a controlar de mejor manera las áreas de posible riesgo.

Alarmas Técnicas

El objetivo es dotar al inmueble de sensores permitiendo la alerta cuando el inmueble este ocupado, o de comunicar estos eventos en caso de ausencia, para que el sistema actúe en consecuencia.

En caso de incidencia se alertará de las siguientes formas:

- Mediante el uso de la iluminación controlada en la instalación.
- Mediante una alarma luminosa o acústica (sirena.

- Las cámaras de seguridad serán ubicadas en sectores con un potencial riesgo de intrusión así como en habitaciones donde se aprecie un mayor valor económico de inversión.

  La unidad de funcionamiento y control central debe instalarse en el cuarto de equipos del edificio, en ella podremos comprobar el estado de todas las instalaciones así como la distribución de equipos en la planta baja y la planta alta

REDES IP

En la actualidad TCP/IP es el protocolo de comunicación más común, utilizado para Internet y para casi todas las redes que se instalan. En una oficina típica la mayoría de los ordenadores están conectados a través de una red Ethernet, por ejemplo en una Red de Área Local (LAN). Cada dispositivo de una LAN debe tener una dirección única, la dirección IP, que permite conectar directamente a Internet. Los ordenadores actuales y los dispositivos de red tienen una alta capacidad para comunicar simultáneamente con varias unidades diferentes.

IP es el protocolo de comunicaciones de mayor difusión en la actualidad. Es el protocolo en el que se basa Internet, el correo electrónico, etc. y casi cada una de las nuevas redes que se instalan. Una de las principales razones de su popularidad es su escalabilidad. En otras palabras, funciona bien tanto en muy pequeñas instalaciones como en las más grandes y está soportado por una creciente variedad de equipamiento de alto rendimiento y bajo coste.

En cualquier oficina moderna la mayoría de los ordenadores de la empresa se hallan conectados a través de una red Ethernet formando una red de área local (LAN), o una LAN inalámbrica. Ethernet proporciona una elevada velocidad de transmisión de datos a un precio razonable. Todos los ordenadores modernos incorporan una tarjeta de conexión a redes Ethernet o se le puede instalar fácilmente. Si usted instala una conexión a Internet (con cable módem, RDSI, ADSL, etc.) lo más probable es que incorpore un conector Ethernet.

Ethernet está disponible sobre redes con cable o inalámbricas y en tres velocidades diferentes: 10 Mbit/seg., 100 Mbit/seg. y 1000 Mbit/seg. Para su uso doméstico y en oficinas se recomienda a 100 Mbit/seg.

Modelo Jerárquico de Redes

El diseño jerárquico consiste en un diseño por capas, de modo que:

- Simplifica la tarea de comunicar dos estaciones
- Cada capa se encarga de tareas específicas
- Utiliza el ancho de banda apropiado entre cada capa
- Facilita la gestión modular y distribuida
- Ahorra coste de personal y aprendizaje
- Está compuesta por tres capas, acceso, distribución y core.

Capa de core:

- Backbone de alta velocidad de conmutación, sin procesamiento de nivel 3
- Alta fiabilidad, redundancia
- Rápida convergencia ante cambios
- Baja latencia
- Sin manipulación de paquetes (filtros)
- Diámetro limitado

Capa de distribución:

- La capa de distribución es una combinación de switches y routers. Hace de frontera para los dominios de broadcast y realiza las funciones de inter-VLAN routing.
- Punto de unión entre la capa de acceso y la de core
- Direccionamiento
- Limitación de los dominios de broadcast y multicast
- Traducciones de medio
- Redistribución entre dominios de routing
- Se realizan las tareas más pesadas de manipulación de paquetes, como routing y seguridad

Capa de acceso:

- Proporciona el acceso a los usuarios
- Caracterizado por LAN conmutada y compartida
- Proporciona acceso a usuarios remotos con FR, RDSI o líneas dedicadas (controla el coste usando DDR)

- La topología habitualmente empleada es la llamada Hub-and-Spoke, que concentra todos los accesos(spoke) en un único punto conectado en la oficina central (hub)
- Se realizan tareas de nivel 2, como VLAN y filtrado por MAC.

Este modelo siempre ha de tener tres capas. Puede ser conmutado (switches en todas las capas) o enrutado (routers en la capa de distribución y/o en la de core)

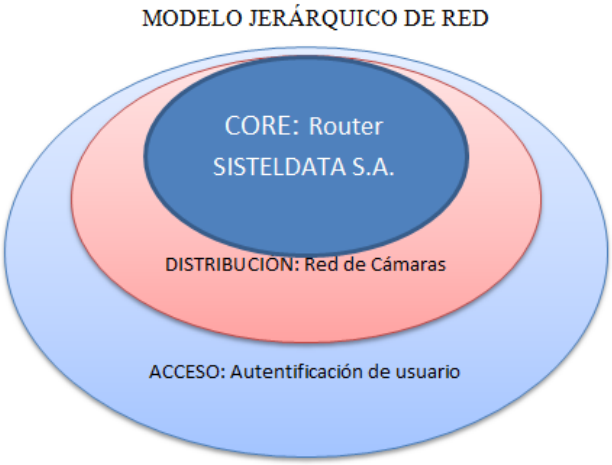


Figura 6.18: Modelo Jerárquico

Fuente: Investigador

Direcciones IP

Cada dispositivo de una LAN (*Local Area Network*, Red de Area Local) debe tener una dirección única. A esta se le denomina comúnmente dirección IP y a veces se la refiere como dirección Ethernet. Una dirección IP está formada por conjuntos de hasta tres números separados por un punto; cada número se halla comprendido entre el 0 y el 255. La dirección podría ser: 192.168.10.2.

Los primeros tres grupos de números son comunes a todos los dispositivos conectados al mismo segmento de red, todas las direcciones IP de las unidades conectadas a ese segmento de red empezarían por 192.168.10.

Cada dirección IP se divide en 65.535 puertos. Las diferentes aplicaciones emplean diferentes puertos IP. El protocolo que se usa para la navegación web, el HTTP, usa habitualmente el puerto 80. Normalmente los usuarios finales no necesitan preocuparse de los números de puerto.

Paquete de datos

Todos los datos se envían como paquetes de datos y todos ellos incorporan lla etiqueta de la dirección de destino. En una red Ethernet, se transmite un paquete cada 0,1 milisegundos aproximadamente. Esto significa que se pueden transmitir hasta 10.000 paquetes en un segundo.

Dado que los ordenadores modernos y los dispositivos de red poseen una elevada capacidad, pueden comunicarse simultáneamente con varios dispositivos. Una cámara IP, por ejemplo, puede enviar imágenes a 5 ordenadores simultáneamente, como mínimo.

Seguridad y Vigilancia

Las cámaras de red se usan en sistemas de seguridad profesionales y permiten vídeo en directo para que sea visualizado por personal autorizado.

Las cámaras de red se integran fácilmente en sistemas mayores y más complejos, pero también pueden funcionar como soluciones aisladas en aplicaciones de vigilancia de bajo nivel.

Las cámaras de red pueden usarse para vigilar áreas sensibles como pueden ser edificios, casinos, bancos, puertos deportivos y tiendas. Las imágenes en vídeo de estas áreas pueden ser monitorizadas desde salas de control, dependencias policiales y/o por directores de seguridad desde diferentes localizaciones.

Las cámaras de red han mostrado igualmente ser efectivos sustitutos de las cámaras analógicas en aplicaciones tradicionales de refuerzo a las fuerzas de seguridad, como por ejemplo para mantener seguros determinados lugares públicos.

Las cámaras de red pueden igualmente emplearse para el control de accesos.

Las personas, al igual que los vehículos, pueden grabarse junto con la información de la fecha y la hora de entrada de forma que sea sencilla su revisión y localización.

Las imágenes pueden almacenarse en un lugar remoto, imposibilitando el robo de esta valiosa información.

Monitorización Remota

Las cámaras de red se conectan fácilmente a las redes IP existentes y permiten actualizaciones en tiempo real de vídeo de alta calidad para que resulte accesible desde cada uno de los ordenadores de una red. Las áreas sensibles como son la sala de servidores, la recepción o cualquier lugar remoto pueden ser monitorizadas detalladamente de una forma única y económica, a través de la red de área local o de Internet.

Las cámaras de red mejoran la monitorización de un establecimiento comercial para asegurar que todo está en orden. (Quality of Service)

Una cámara de red es una herramienta útil en la oficina. Áreas como la recepción y las salas de conferencias pueden estar monitorizadas para controlar su actividad. Además los usuarios pueden hacer seguimiento de quién ha entrado en la sala de informática, por ejemplo, y tomar las acciones pertinentes cuando haya problemas.

Planimetría y ubicación de elementos

Planta Baja

Como se muestra en el plano de la figura6.19 se tiene la estancia para la cual se requiere de una cámara para su cobertura, ventas requiere de dos cámaras por ser un área importante, la recpción requiere de dos cámaras para su completa cobertura, el pasillo necesita una sola cámara para cubrir conjuntamente las gradas de acceso a las plantas superiores y finalmente el área externa que necesita cuatro cámaras, una para cada costado de la edificación

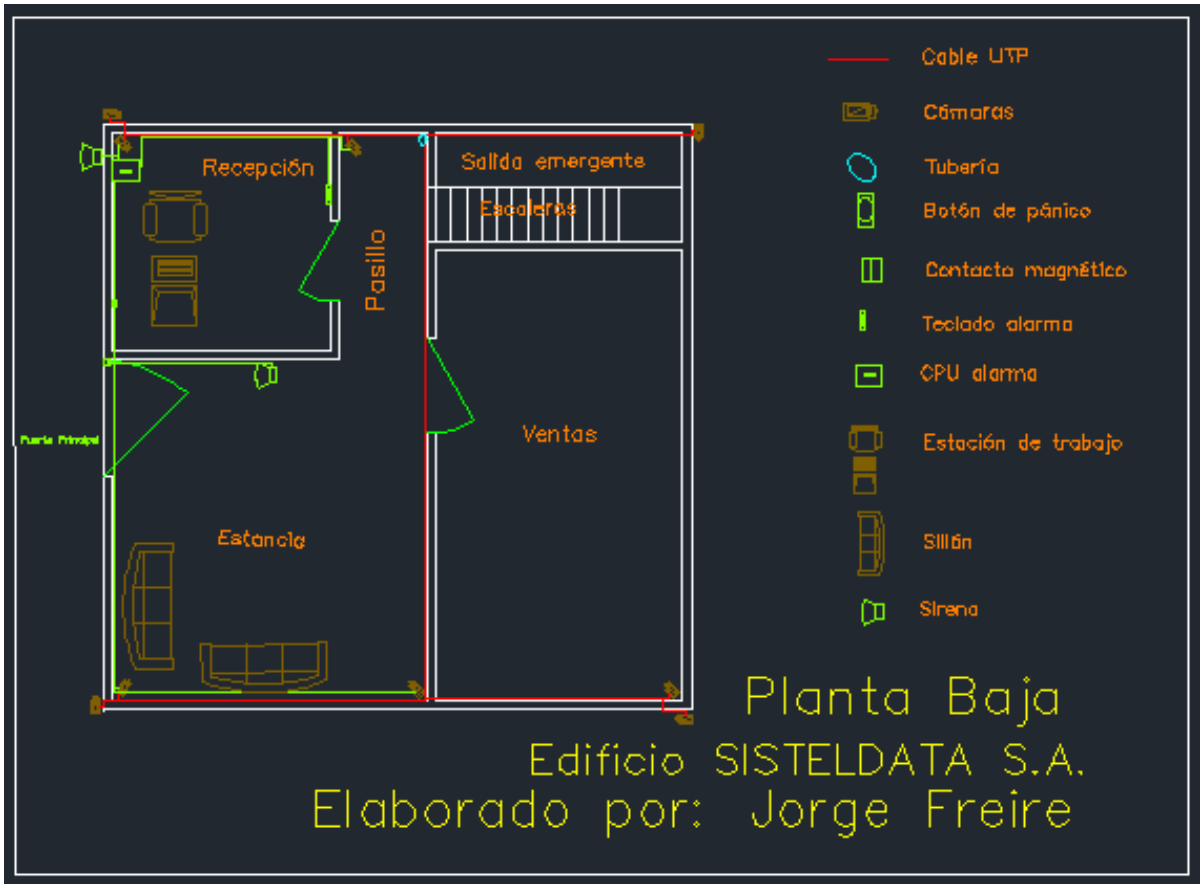


Figura 6.19: Planta baja

Elaborado por: Investigador

Fuente: SISTELDATA S.A.

Planta Alta 1

En esta planta se tiene dos áreas de riesgo como muestra la figura 6.20, que son la bodega que requiere de tres cámaras para cubrir toda el área y el pasillo que necesita una sola cámara para cubrir conjuntamente las gradas de acceso a las plantas superiores e inferior

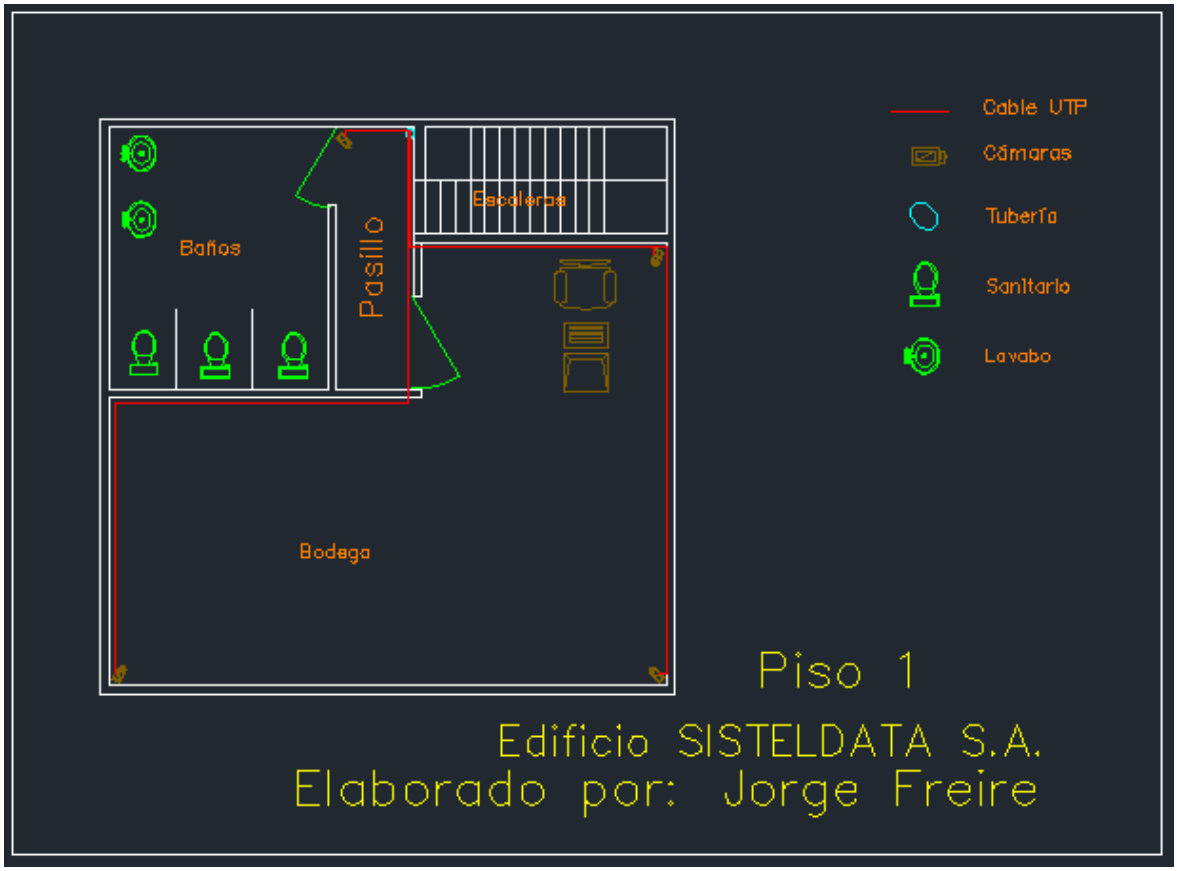


Figura 6.20: Planta alta 1

Elaborado por: Investigador

Fuente: SISTELDATA S.A.

Planta Alta 2

Como la figura 6.21 indica existen cuatro áreas a proteger, el área de técnicos que requiere de dos cámaras para su cobertura al igual que la cafetería, mientras que el área de monitoreo y equipos, como el pasillo requieren de una cámara para cada área

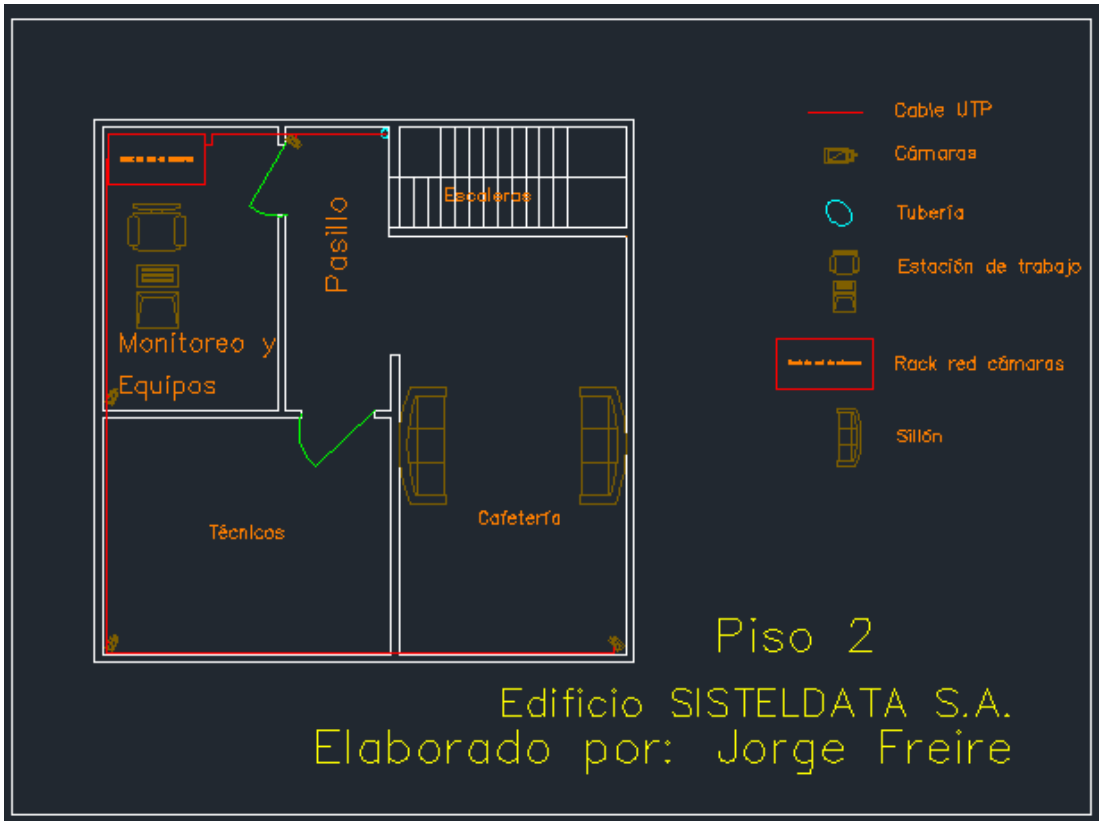


Figura 6.21: Planta alta2

Elaborado por: Investigador

Fuente: SISTELDATA S.A.

PLANTA ALTA 3

La figura 6.22 muestra el área administrativa de la empresa para la cual se necesitan dos cámaras para cada área como son Gerencia, Jefe de operaciones, Secretaría y Pasillo

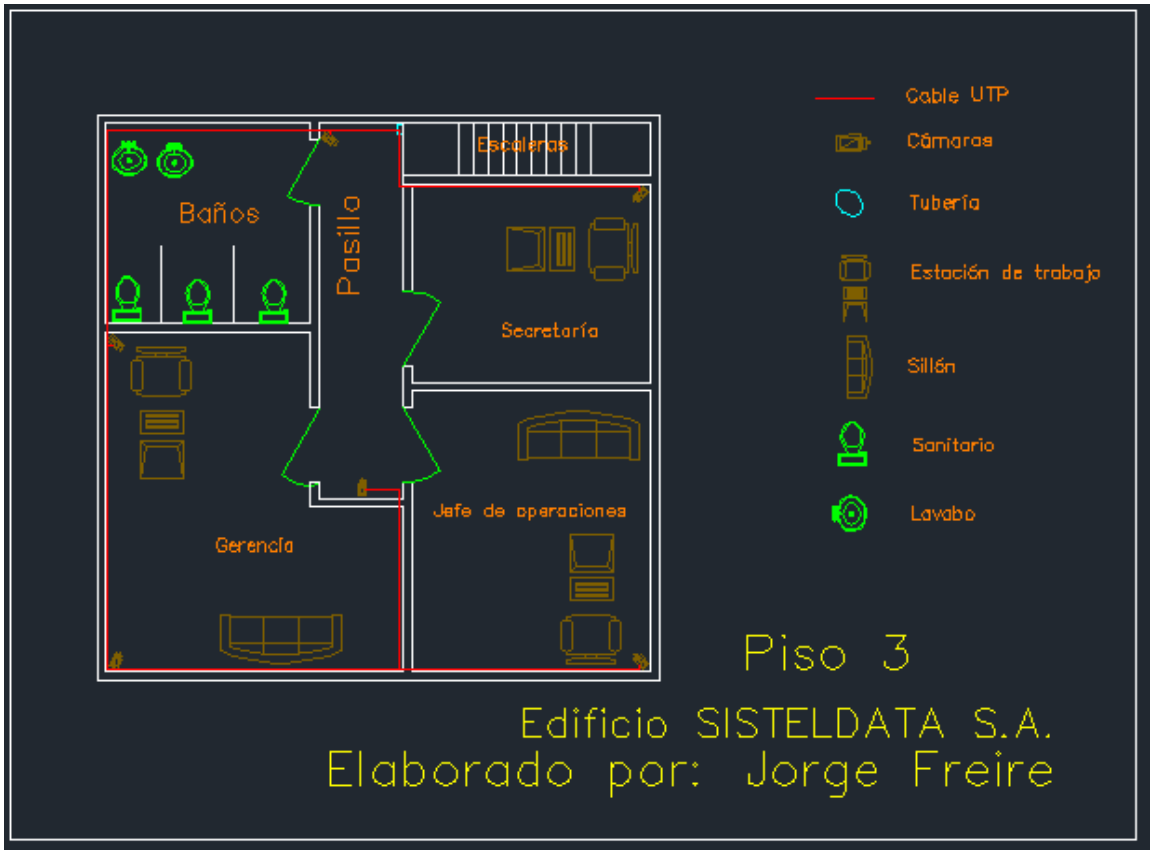


Figura 6.22: Planta alta3

Elaborado por: Investigador

Fuente: SISTELDATA S.A.

Enrutamiento de las cámaras

El enrutamiento del sistema de seguridad se lo realizará en una red virtual creada específicamente para la red de cámaras IP como se muestra en la tabla 6.6:

Figura 6.23: Red VLAN de cámaras

Fuente: Investigador

RED VLAN DE CÁMARAS IP			
Equipo	**Zona**	**Dirección IP**	**Máscara**
Switche	Monitoreo	192.168.10.1	**255.255.255.224**
Switche	Monitoreo	192.168.10.2	**255.255.255.224**
Servidor NVR	Monitoreo	192.168.10.3	**255.255.255.224**
Cámara	Exterior C1	192.168.10.4	**255.255.255.224**
Cámara	Exterior C2	192.168.10.5	**255.255.255.224**
Cámara	Exterior C3	192.168.10.6	**255.255.255.224**
Cámara	Exterior C4	192.168.10.7	**255.255.255.224**
Cámara	Estancia	192.168.10.8	**255.255.255.224**
Cámara	Pasillo PB	192.168.10.9	**255.255.255.224**
Cámara	Recepción C1	192.168.10.10	**255.255.255.224**
Cámara	Recepción C2	192.168.10.11	**255.255.255.224**
Cámara	Ventas C1	192.168.10.12	**255.255.255.224**
Cámara	Ventas C2	192.168.10.13	**255.255.255.224**
Cámara	Pasillo 1	192.168.10.14	**255.255.255.224**
Cámara	Bodega C1	192.168.10.15	**255.255.255.224**
Cámara	Bodega C2	192.168.10.16	**255.255.255.224**
Cámara	Bodega C3	192.168.10.17	**255.255.255.224**
Cámara	Pasillo 2	192.168.10.18	**255.255.255.224**
Cámara	Técnicos C1	192.168.10.19	**255.255.255.224**
Cámara	Técnicos C2	192.168.10.20	**255.255.255.224**
Cámara	Monitoreo	192.168.10.21	**255.255.255.224**
Cámara	Cafetería C1	192.168.10.22	**255.255.255.224**
Cámara	Cafetería C2	192.168.10.23	**255.255.255.224**
Cámara	Pasillo 3 C1	192.168.10.24	**255.255.255.224**
Cámara	Pasillo 3 C2	192.168.10.25	**255.255.255.224**
Cámara	Secretaría C1	192.168.10.26	**255.255.255.224**
Cámara	Secretaría C2	192.168.10.27	**255.255.255.224**
Cámara	Jefe Op. C1	192.168.10.28	**255.255.255.224**
Cámara	Jefe Op. C2	192.168.10.29	**255.255.255.224**
Cámara	Gerencia C1	192.168.10.30	**255.255.255.224**
Cámara	Gerencia C2	192.168.10.31	**255.255.255.224**

Tabla6.6: Enrutamiento de equipos

Elaborado por: Investigador

Diseño del cableado de la red de cámaras y sensores de las cuatro plantas

En la figura 6.24 se muestra el cableado de la red de cámaras de la planta baja, identificado con las líneas de color rojo, y la conexión de los sensores de alarma como las bocinas y los elementos de la alarma con líneas de color verde claro

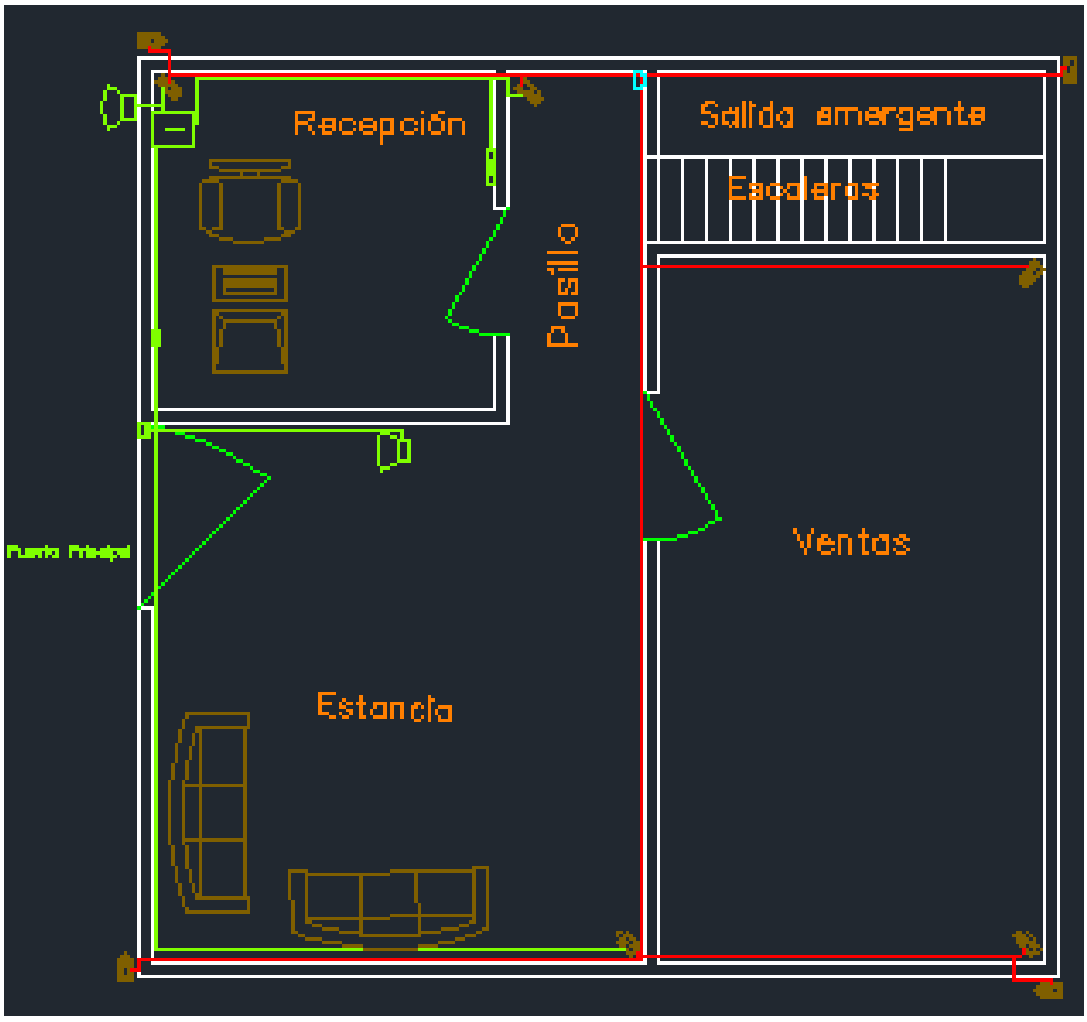


Figura 6.24 Cableado planta baja

Elaborado por: Investigador

Fuente: SISTELDATA S.A.

En la figura 6.25 se muestra el cableado de la red de cámaras de la planta alta 1, identificado con las líneas de color rojo

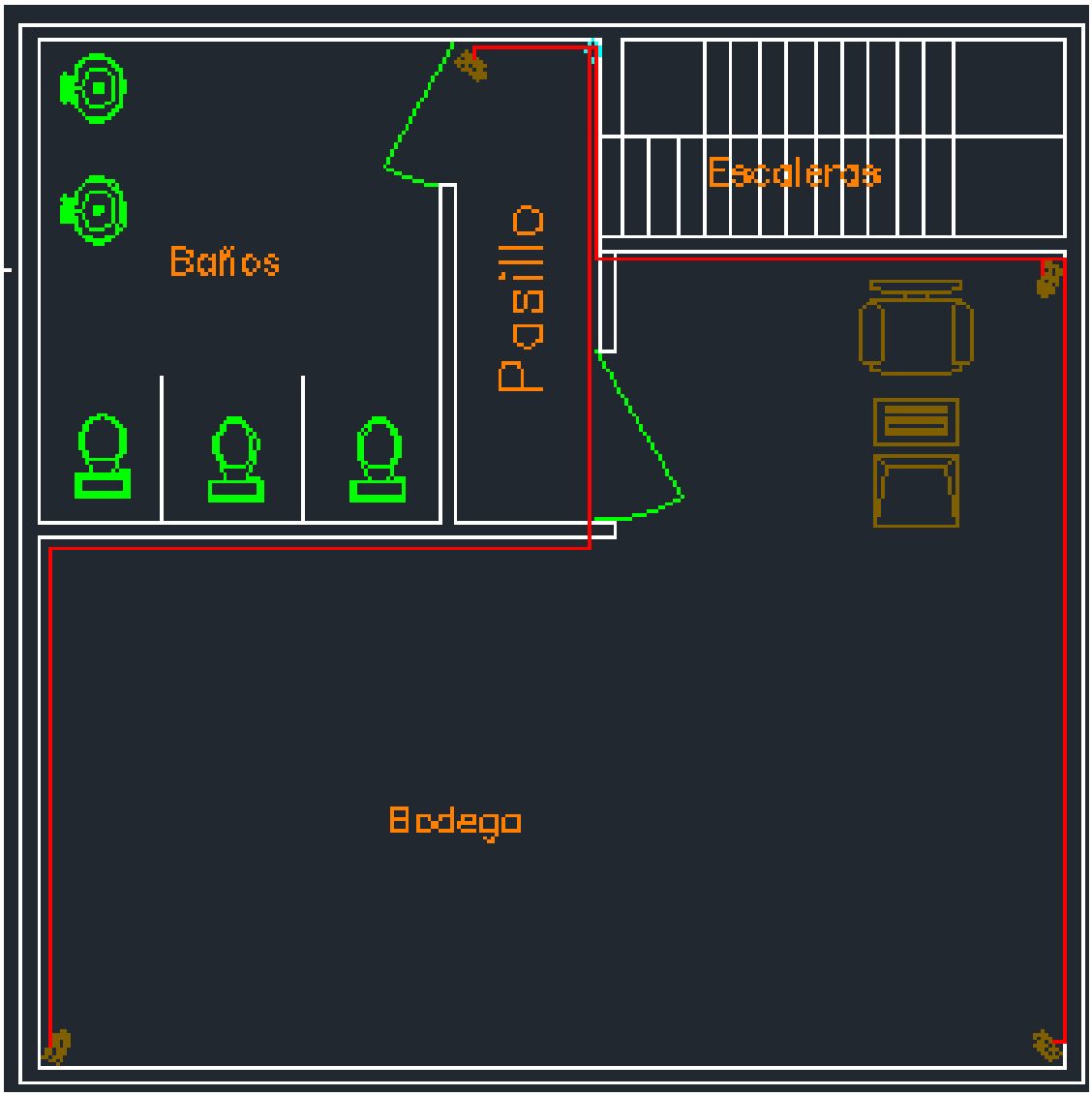


Figura 6.25 Cableado planta alta 1

Elaborado por: Investigador

Fuente: SISTELDATA S.A.

En la figura 6.26 se muestra el cableado de la red de cámaras de la planta alta 2, identificado con las líneas de color rojo

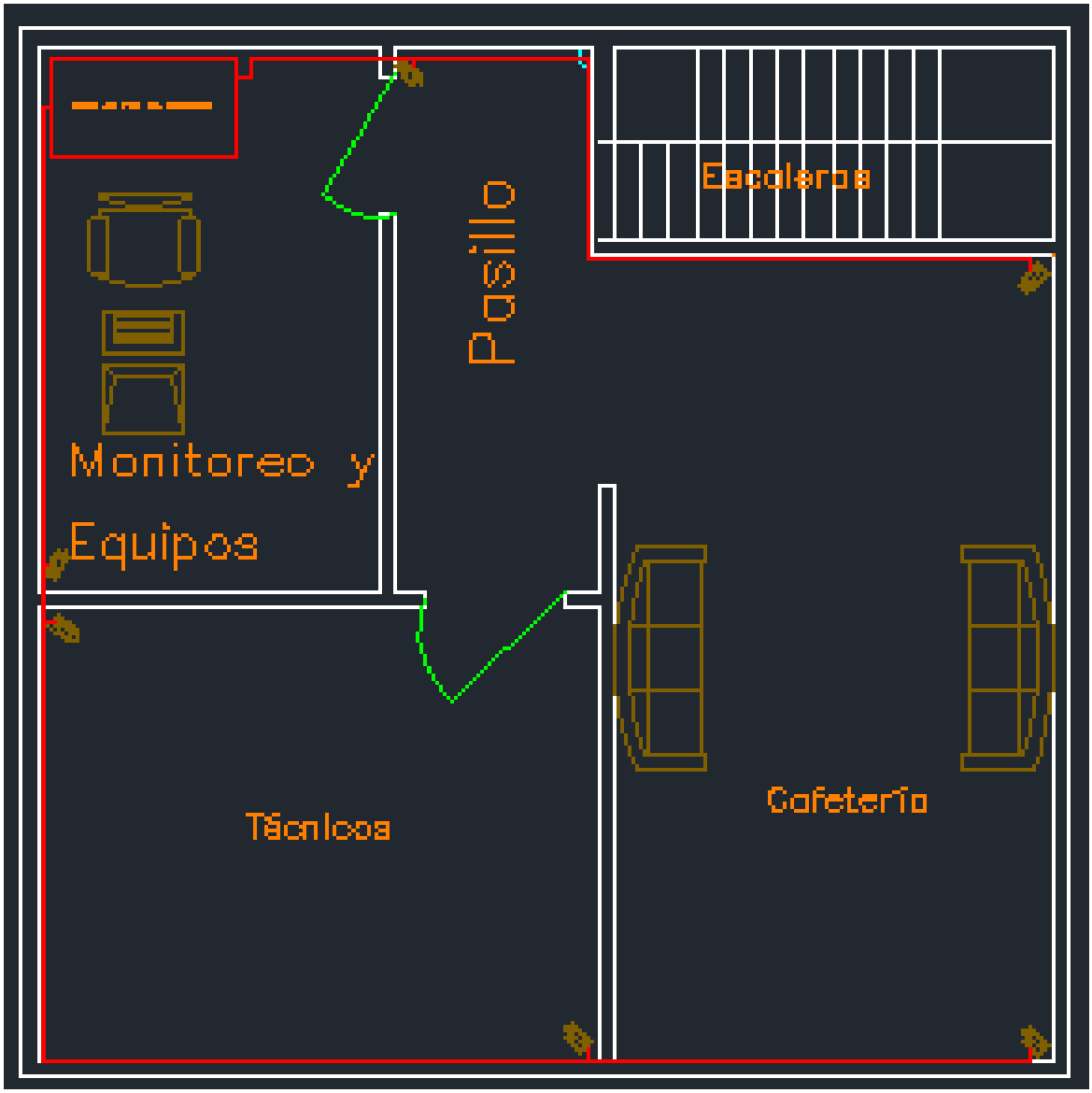


Figura 6.26 Cableado planta alta 2

Elaborado por: Investigador

Fuente: SISTELDATA S.A.

En la figura 6.27 se muestra el cableado de la red de cámaras de la planta alta 3, identificado con las líneas de color rojo

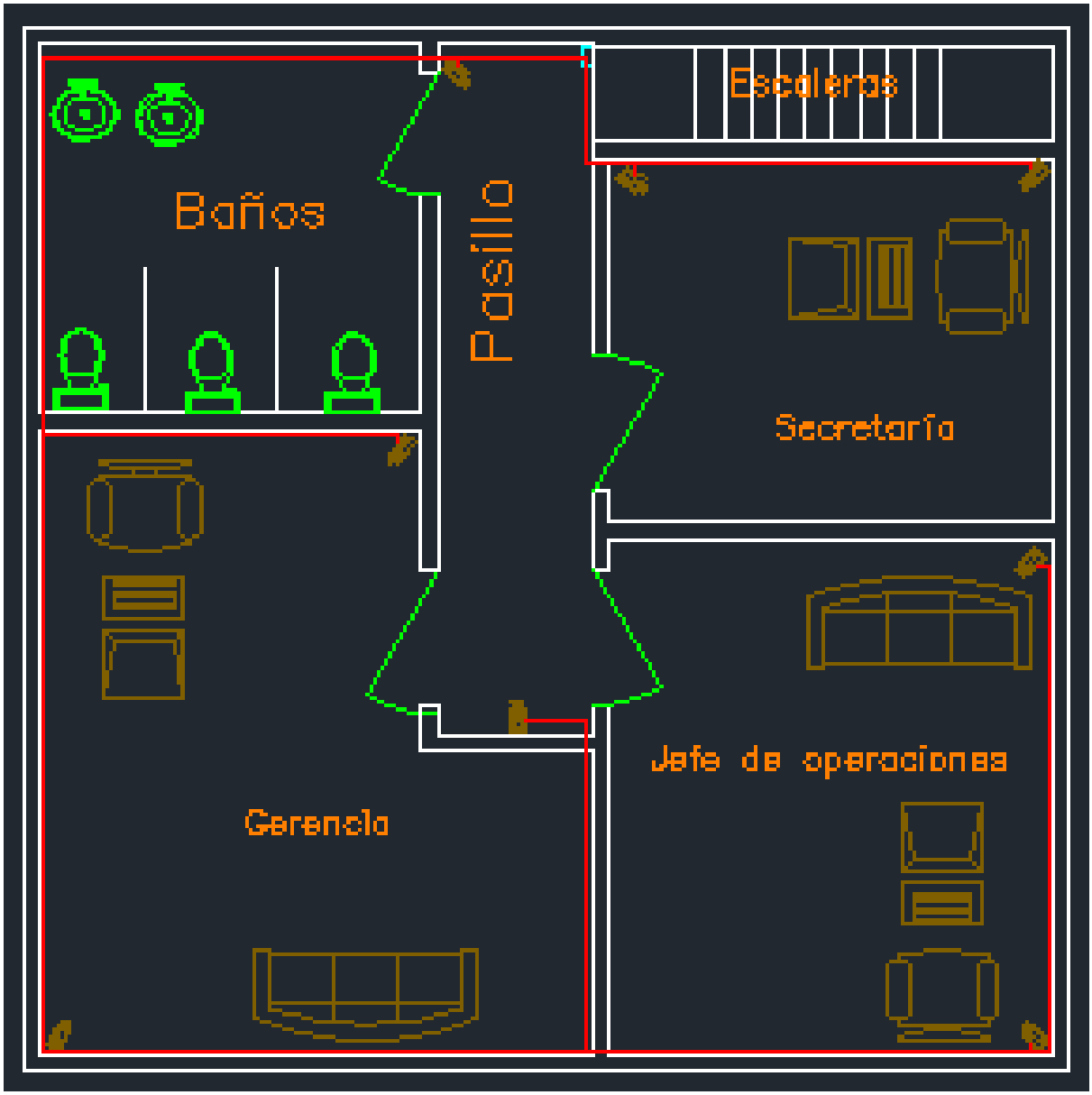


Figura 6.27 Cableado planta alta 3

Elaborado por: Investigador

Fuente: SISTELDATA S.A.

6.6.6 Diseño del sistema de Video Vigilancia IP

Una cámara IP, también conocida como cámara Web o de Red, es una videocámara especialmente diseñada para enviar las señales de video, y en algunos casos audio, a través de Internet desde un explorador (por ejemplo el *Internet Explorer*) o a través de un concentrador (un Hub oun switch) en una Red Local (LAN, abreviatura de Local Area Network).En las cámaras IP pueden

integrarse aplicaciones como detección de presencia, incluyendo el envío de mail si detectan movimiento, grabación de imágenes o secuencias en equipos informáticos, tanto en una Red Localcomo en una Red Externa (WAN, abreviatura de Wide Area Network), de manera que se pueda comprobar por qué se produjo la detección de presencia y a consecuencia se graben imágenes de lo sucedido. Por lo tanto, una cámara IP puede describirse como una cámara y un ordenador combinados para formar una única unidad, que capta y transmite imágenes directamente a través de una red IP, permitiendo a los usuarios autorizados visualizar, almacenar y gestionar video de forma local o remota mediante una infraestructura de red que se basa en una tecnología IP.

Análisis según el ángulo de cobertura de las cámaras IP

Las cámaras IP VIVOTEK modelo VI-IP7153 tienen un ángulo de cobertura horizontal de 71°, como la altura de cada piso es de 3,5m las cámaras se colocarán a una altura de 3m por la colocación del gypsun (techo falso), por lo que se ha adecuado la ubicación de las cámaras según este ángulo de cobertura de la siguiente manera:

Planta Baja:

La figura 6.28 muestra el área de cobertura de las cámaras IP, denotada por las líneas amarillas en el plano de diseño de la planta baja.

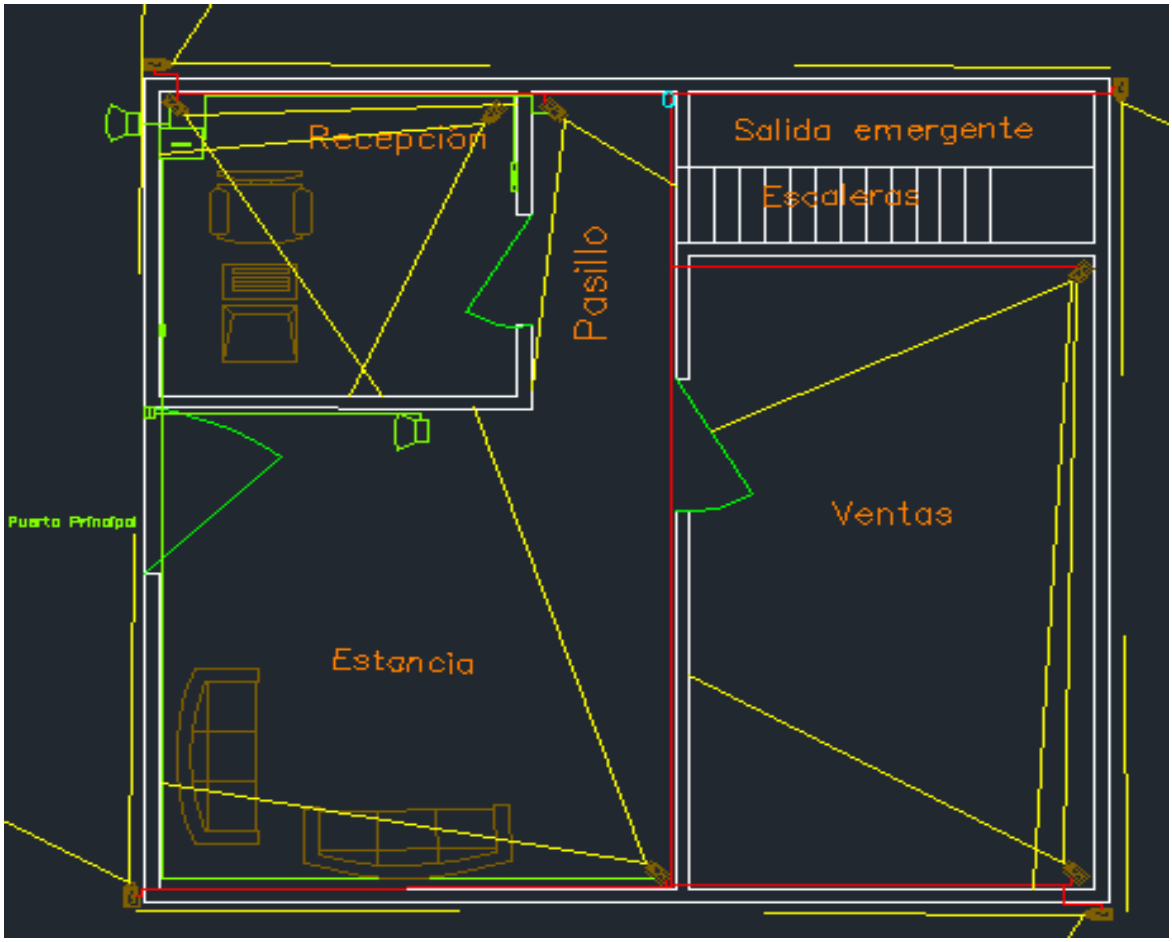


Figura 6.28 Cobertura planta baja

Elaborado por: Investigador

Fuente: SISTELDATA S.A.

Plata Alta 1:

La figura 6.29 muestra el área de cobertura de las cámaras IP, denotada por las líneas amarillas en el plano de diseño de la planta alta1

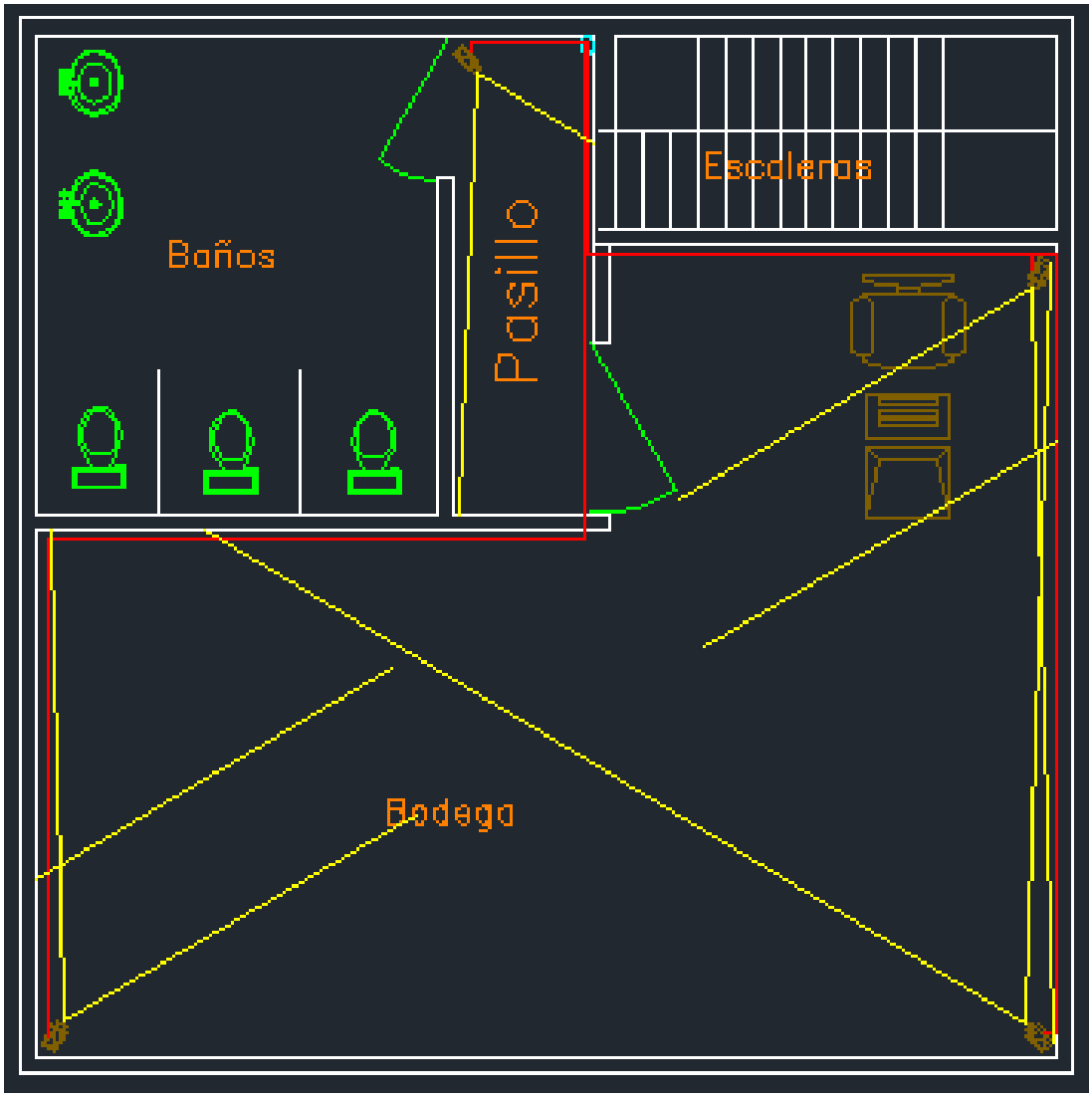


Figura 6.29 Cobertura planta alta 1

Elaborado por: Investigador

Fuente: SISTELDATA S.A.

Planta Alta 2:

La figura 6.30 muestra el área de cobertura de las cámaras IP, denotada por las líneas amarillas en el plano de diseño de la planta alta 2

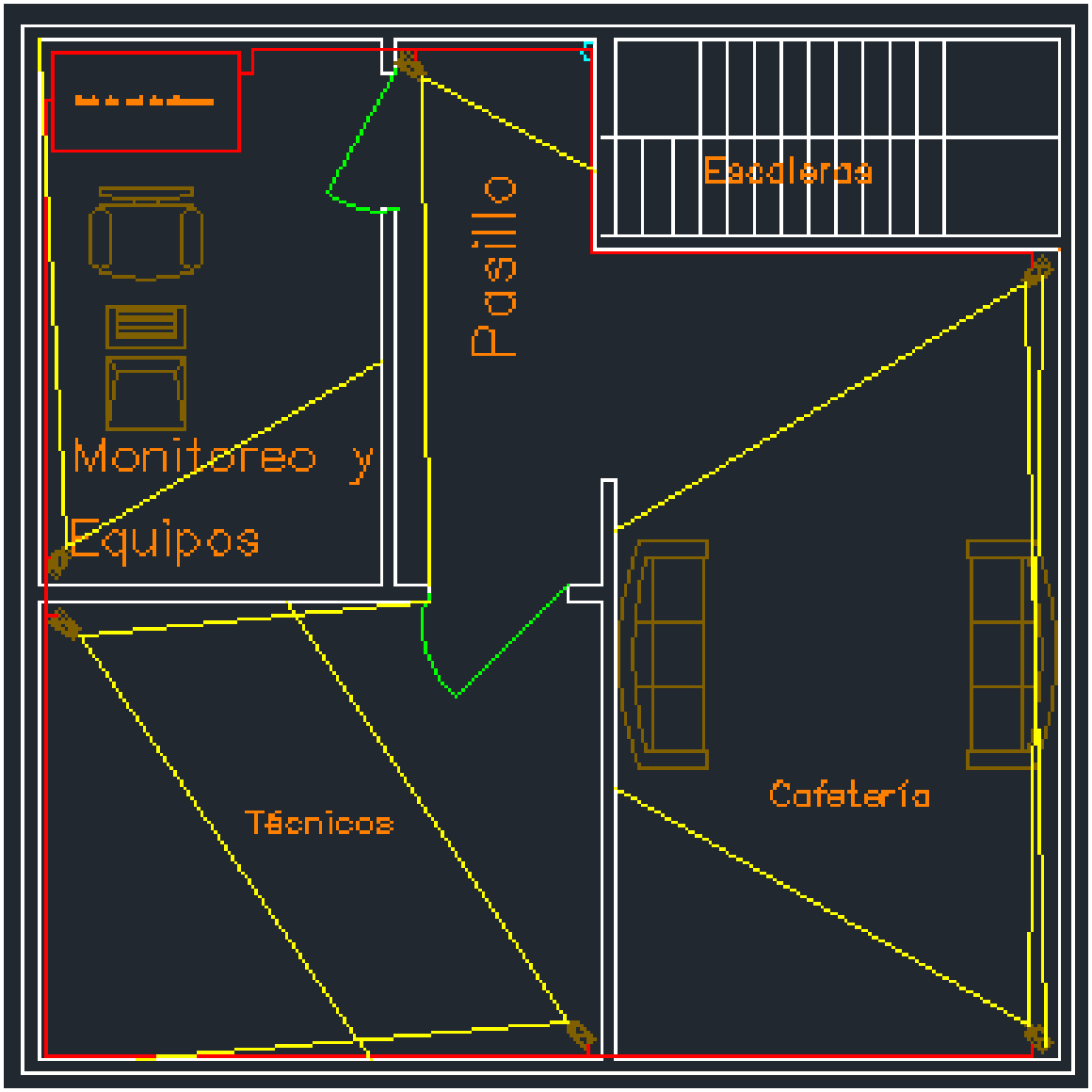


Figura 6.30 Cobertura planta alta 2

Elaborado por: Investigador

Fuente: SISTELDATA S.A.

Planta Alta 3:

La figura 6.31 muestra el área de cobertura de las cámaras IP, denotada por las líneas amarillas en el plano de diseño de la planta alta 3

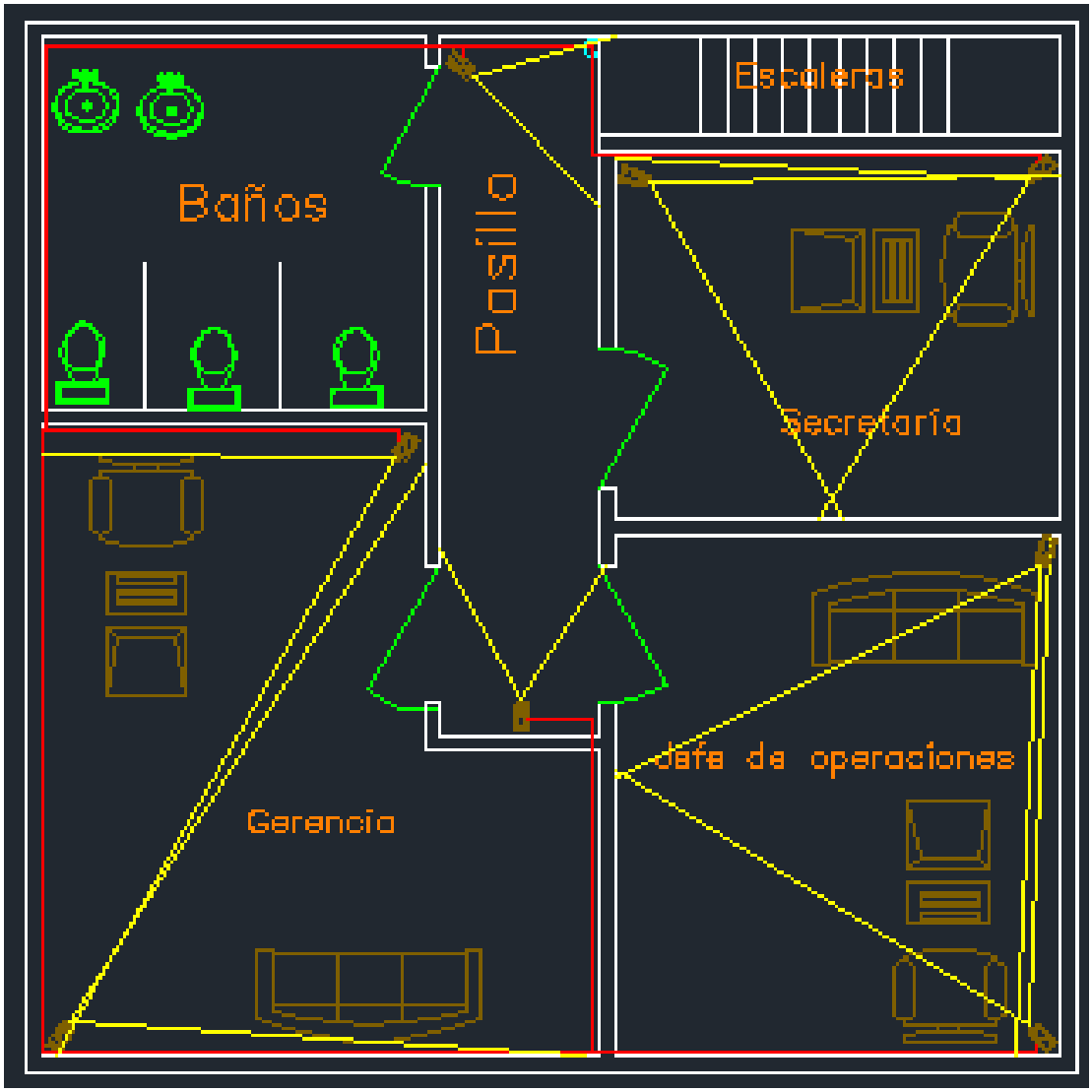


Figura 6.31 Cobertura planta alta 3

Elaborado por: Investigador

Fuente: SISTELDATA S.A.

Instalación

Se conectan todos los dispositivos a una fuente de alimentación y entre sí, mediante el conmutador si es un dispositivo con tecnología PoE(Alimentación sobre Ethernet).

Asignación de dirección IP a la cámara

Debe asignar una dirección IP a la cámara de red para poder acceder a ella desde un navegador web en el ordenador local. Puede elegir entre una dirección IP automática o estática. Se recomienda usar una dirección IP estática, ya que impedirá que la dirección IP cambie. Para configurar la dirección IP de la cámara de red, es muy fácil, puede usar el programa de utilidades, fue generalmente encontrará en el CD que acompaña al producto.

Finalización de la instalación de la cámara

Una vez asignada la dirección IP, abra el navegador Web de la PC local y escriba la dirección IP asignada a la cámara de red. Para los usuarios que utilicen este sistema por primera vez con Internet Explorer, el producto de video en red les pedirá automáticamente si desean descargar un programa de software proporcionado por el fabricante. Este programa es básico para ver video en directo desde una cámara de red. También proporciona controles para Mpeg2, Mpeg-4, audio, detección de movimiento y movimiento horizontal, vertical y zoom en la páginaLive View para los productos de video en red compatibles con estas características. (Es posible que otros navegadores web tengan compatibilidad nativa con la transmisión de video que no requiera ningún componente Active-X.)

Una vez instalado el software, la página de inicio de la cámara de red mostrará vídeo en directo desde la cámara, junto con hiperenlaces para cambiar las opciones de configuración de la cámara, como la resolución de imagen y los valores de red y correo electrónico.

Requisitos del sistema

La propiedad, donde debe ubicar la cámara, ya está conectada con cableado Ethernet y a un proveedor de servicios de Internet (ISP)sólo tiene que suscribirse a una cuenta, conectar la cámara de red a un conmutador o switch (que a su vez se

conecta a la toma de red) y, normalmente, recibirá una dirección IP pública asignada de forma dinámica a la cámara de red.

Siga las instrucciones de instalación de la cámara de red. Al respecto, existen en el mercado programas basados en Windows que le resultarán útiles para identificar la dirección IP de la cámara.

Cambio de la dirección IP asignada a la cámara

Debido a una cantidad limitada de direcciones IP que comparten sus clientes, averigüe como puede seguir manteniendo una única dirección para acceder a la cámara de red

Dirección IP a la cámara

Normalmente, un enrutador de banda ancha asigna direcciones IP privadas automáticas a los dispositivos de la red de área local, por lo que estas direcciones IP pueden cambiar por lo tanto se recomienda tener una dirección IP fija para la cámara de red. Para asignar una dirección IP fija, tendremos en cuenta el intervalo de direcciones IP del enrutador, que podría ser, por ejemplo, de 192.168.10.4 a 192.168.10.31.

Si utiliza una dirección IP superior a ese intervalo, como 192.168.10.100, como dirección IP fija para la cámara, es probable que evite arriesgarse a tener conflictos con otros dispositivos que reciben direcciones automáticas.

La configuración de la dirección IP de la cámara puede hacerse de tres formas distintas, tal y como se explica en el manual de la cámara. Una vez asignada la dirección IP, defina la subred y la puerta de enlace (esta información se puede obtener del enrutador)y configure la cámara como desee.

Defina contraseñas y usuarios autorizados para proteger el acceso a la cámara.

Renvío de puertos

El enrutador de banda ancha, como se mencionó anterior- mente, proporciona la interfaz entre Internet/ISP (área pública)y la red de área local (área privada). El enrutador recibe una dirección IP pública del ISP y proporciona direcciones IP locales a los dispositivos de la red de área local. Para poder tener acceso a una cámara de red que se encuentre en una red de área local, debe identificar la dirección IP pública del enrutador (consulte el manual del enrutador)y configurar el enrutador para que la dirección IP pública se dirija a una dirección IP local fija para la cámara de red. Este proceso se denomina "reenvío de puertos", es decir, cuando escriba la dirección IP pública del enrutador desde cualquier ordenador en red, Internet localiza el enrutador que, a su vez, reenvía la solicitud a la dirección IP asignada a la cámara de red. Consulte la figura 6.32.

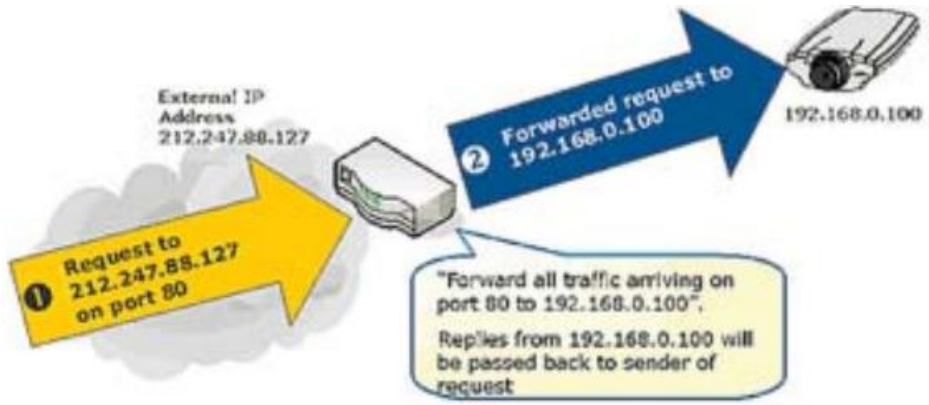


Figura 6.32: Renvío de puertos

Fuente:http://www.casadomo.com/casadomo/biblioteca/axis_las_redes_ip.pdf

Inicie un navegador Web y vaya a las páginas Web integradas del enrutador. Inicie sesión en las páginas de configuración del enrutador. Busque el elemento de menú "renvío de puertos" (o una opción parecida), que tiene una tabla como la que se muestra a continuación.

Nombre del servicio	Puerto de inicio	Puerto final	Dirección IP del servidor
FTP	21	21	Sin configurar
HTTP (web)	80	80	Sin configurar
			Sin configurar

Tabla 6.7: Configuración enrutador

Fuente: Investigador

Como la cámara envía video a través de HTTP, debe configurar el servicio HTTP según los valores consignados en la siguiente tabla.

Nombre del servicio	Puerto de inicio	Puerto final	Dirección IP del servidor
FTP	21	21	Sin configurar
HTTP (web)	80	80	192.168.0.100
Puerto no oficial	80xx	80xx	192.168.0.10x

Tabla 6.8: Configuración servicio HTTP

Fuente: Investigador

Guarde la configuración en el enrutador y salga de las páginas de configuración. La configuración ha finalizado. Cualquiersolicitud que llegue a la dirección IPexternadel enrutadoren el puerto 80se renviará a la dirección IPde la cámara:192.168.0.100.Si desea acceder a través de Internet a más de una cámarade red,deberá usarlos puertos no oficiales del enrutador,como 80xx, y enlazarlosa la dirección IPde las cámarasde red.

Conexión de sensores externos

• **Entradas y salidas digitales (E/S):** Una característica única de los productos de video IP son sus entradas y salidas digitales integradas -ubicadas en la parte posterior que se pueden manejar en la red.

La salidapuede utilizarse para activar mecanismos, bien sea desde una PC remota o automáticamente, haciendo uso de la lógica incorporada a la cámara, mientras que *las entradas* pueden configurarse para reaccionar ante sensores externos como un infrarrojo pasivo o pulsar un botón que inicie las transferencias de video.

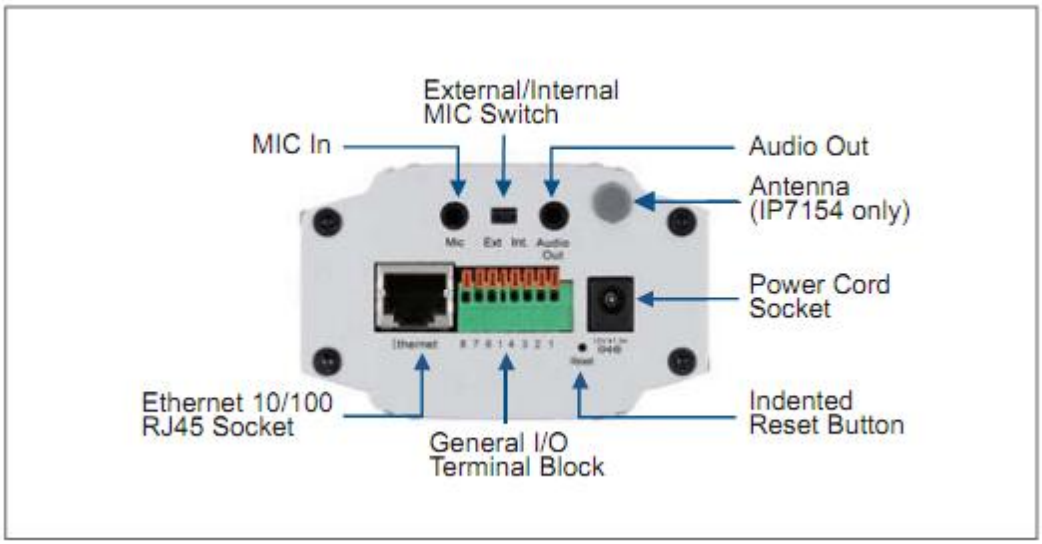


Figura 6.33: Entradas y salidas digitales

Las E/S pueden usarse, por ejemplo, junto con sensores de alarma para eliminar transferencias de video innecesarias, a menos que el sensor conectado a la cámara se active.

Figura 6.34: Conexión de sensores externos

Fuente:http://www.casadomo.com/casadomo/biblioteca/axis_las_redes_ip.pdf

Entradas digitales: La gama de los dispositivos quese pueden conectar al puerto de entrada de una cámarade red o de un servidor de video es casi infinita. La reglabásica es que cualquier dispositivo pueda abrir o cerrarun circuito.

Tipo de Dispositivo	Uso
Contacto Magnético	Cuando un circuito se rompe (la puerta se abre) la cámara actúa produciendo una imagen animada a pantalla completa y enviando notificaciones.
Detector de infrarrojos pasivo (PIR)	Cuando se detecta movimiento, el PIR rompe el circuito y la cámara actúa produciendo una imagen animada a pantalla completa y enviando notificaciones.
Detector de rotura de cristales (DRV)	Cuando se detecta una bajada de la presión del aire, el detector rompe el circuito y la cámara actúa produciendo una imagen animada a pantalla completa y enviando notificaciones.

Tabla 6.9: Entradas digitales

Fuente: Investigador

Salidas digitales: La función principal del puerto de salida es permitir que la cámara active los dispositivos externos, bien sea de forma automática o mediante control remoto por parte de un operador humano o una aplicación de software.

Tipo de Dispositivo	Uso
Relé en las puertas	La apertura/cierre con llave de una puerta de entrada puede controlarse mediante un operador remoto (a través de la red)
Sirena	La cámara puede activar la sirena cuando se detecte un movimiento usando el VMD integrado o usando *"información"* procedente de la entrada digital.
Sistema de alarma/ intrusión	La cámara puede actuar como una parte integrada del sistema de alarma sirviendo de sensor y mejorando el sistema de alarma con transferencias de vídeo activadas por eventos.

Tabla 6.10: Salidas digitales

Fuente: Investigador

Las cámaras IP y los servidores de video suelen disponer de un sistema de detección de movimiento utilizando el análisis instantáneo y continuado de los cambios que se producen en los fotogramas registrados por el sensor óptico. Con este sistema de detección puede graduarse el nivel de detección de movimiento de las imágenes y diferenciar si en el sistema ha entrado un coche o un peatón, incluso pudiendo diferenciar áreas dentro de una misma imagen, en algunos modelos de cámaras, y cada área con diferente sensibilidad de movimiento.

Usuarios conectados simultáneamente

El número de usuarios que admite una cámara IP o un servidor de video dependen del tipo de cámara, pero en general oscila entre los 10 y 20 usuarios. También pueden enviarse "snapshots" automáticamente con un período de refresco establecido a una Web determinada para que el público en general pueda ver esas imágenes.

Protección de accesos

Una cámara IP, al igual que los servidores de video, dispone de un software interno para resolver cuestiones de seguridad que permite establecer niveles de acceso:

- Administrador: Necesario para poder configurar el sistema. Pide un nombre de usuario y una contraseña
- Usuario: Para visualizar las imágenes, manejar la cámara y el relé de salida. Solicita un usuario y una contraseña.
- Demo: Permite un acceso libre y no pide ningún tipo de identificación.

Transmisión de audio

En general, la mayoría de cámaras IP disponen de micrófonos de alta sensibilidad incorporados con el objetivo de poder transmitir audio mediante el protocolo de conexión UDP (UserDatagramProtocol*)*

Sistemas de compresión

El sistema de Compresión de Imagen de las cámaras IP sirve para hacer que la información obtenida de la cámara pueda ser enviada por los cables de una red Local (LAN) o de las líneas telefónicas.

Al comprimir, se trata de que las imágenes tengan el menor tamaño posible sin que al ser enviadas sufran pérdidas en la calidad o en la visualización. En resumen, los sistemas de compresión tienen como objetivo ajustar la información captada por la cámara a los anchos de banda de los sistemas de transmisión, como por ejemplo el ADSL. Los estándares de compresión actuales son el *MJPEG y MPEG4*, este último es más reciente y potente.

Software de acceso

Para la visualización de las Cámaras IP lo único que se necesita es que en el sistema operativo de la PC se encuentre instalado el *Internet Explorer*, gracias al cual puede accederse a la dirección propia de la cámara IP, que mostrará las

imágenes de lo que en ese momento esté sucediendo en cualquier parte del mundo, sin necesidad de instalar un software especifico. Y en las 3GPP, pueden verse desde un móvil con posibilidad de RTSP *(Protocolo de streaming en tiempo real)*. No obstante, pueden adquirirse software específico según el mercado donde se quiera implementar el sistema.

Configuración remota

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

Análisis Económico

Ahorro energético y amortización de instalación de cámaras IP

Estimación de ahorro de costes energéticos y valoración del coste del material de instalación (para cálculos de amortización) con cámaras IP en instalaciones realizadas en el edificio

Los beneficios que se obtienen con cámaras IP a nivel de edificaciones tienen mayor importancia a nivel de seguridad. No obstante voy a hacer una aproximación estimativa de lo que podría ser el ahorro energético. Se realiza una estimación aproximada de ahorros para una planta de 100 m2 útiles en la que se dispone un sistema de seguridad remota con cámaras IP.

Gracias a que las cámaras IP tienen conexión POE no será necesaria otra fuente de energía para el funcionamiento de las mismas lo cual reduce el consumo de energía,

El consumo de energía de los equipos podemos apreciarlo en la tabla 6.11.

EQUIPO	CONSUMO UNITARIO (W/h)	CANTIDAD	CONSUMO EQUIPOS	COSTE KW/H por día	COSTE KW/H por año
Switche	100	2	200	0,0172	6,278
Cámara	0	23	0	0	0
Alarma	75	1	75	0,00645	2,35425
NVR	101	1	101	0,008686	3,17039
Monitor	100	1	100	0,0086	3,139
UPS	160	1	160	0,01376	5,0224
COSTE TOTAL POR AÑO					19,96404

Tabla 6.11 Coste energético

Elaborado por: Investigador

Lógicamente la mejor forma de realizar una comparación es ver el antes y el después de una instalación de este tipo, de tal modo que se pueda tener los gastos desglosados de la parte que interesa de la factura eléctrica. En cualquier caso, no cabe duda que el ahorro energético siempre se va a producir en mayor o menor medida y en función de todos los factores de control o de gestión que introduzcamos en el sistema así como de la eficiencia del mismo.

Costos Referenciales

Luego de realizar una búsqueda exhaustiva de equipos y materiales para el diseño del sistema de Video y vigilancia IP se decidió optar por los siguientes materiales los cuales cumplen con todas las características técnicas necesarias pata el correcto funcionamiento del sistema y obviamente su precio fue el mejor en comparación a otros equipos que encontramos dentro del mercado mostrados en la tabla 6.12.

EQUIPOS	COSTO UNITARIO	UNIDADES	COSTO TOTAL
Cámara IP VIVOTEK VI-IP7130	230,85	28	6463,8
NVR VioStar VS8032U	5326,49	1	5326,49
Switch Tp Link Tl-sl3428	323	2	646
Monitor LG W1943SS-PF	109	1	109
Mouse y Teclado Logitech Mk260	37	1	37
Rollo de cable Liberty Cables	129	3	387
Plub RJ-45	0,15	62	9,3
Alarma DSC	126	1	126
Sirena Brielco	12,5	2	25
Sensor Magnético Honeywell	21	1	21
Canaleta Plástica Decorativa DEXON	2,7	70	189
TOTAL			13339,59

Tabla 6.12 Coste de equipos

Elaborado por: Investigador

Fuente: Distribuidores de equipos de tecnología

ANÁLISIS DEL CONSUMO DE ANCHO DE BANDA

Calculopara una resolución de 640x480 (43 Kbytes) pixeles en el formato MJPEG, a 30 imágenes por segundo y con una compresión de imagen de 10 Kbits que son las características que la cámara VIVOTEK IP 7130 ofrece, para este cálculo tomaremos en cuenta los valore de gran importancia de la trama de Ethernet que tenemos en la tabla 6.13:

Cabecera IP	Cabecera TCP	Campo de datos
20 bytes	20 bytes	1460 bytes

Tabla 6.13 Formato trama Ethernet

Elaborado por: Investigador

Por lo tanto los datos que serán transmitidos serán 1460 bytes, seguidamente calcularemos la sobrecarga total en la tabla 6.14:

Preámbulo	SOF	MAC destino	MAC origen	Longitud	Cabecera IP	Cabecera TCP	FCS
7 bytes	1 bytes	6 bytes	6 bytes	7 bytes	20 bytes	20 bytes	4 bytes

Tabla 6.14Campo de datos trama Ethernet

Elaborado por: Investigador

Sobrecarga total por cada trama = (7+1+6+6+2+20+20+4) bytes

Sobrecarga total por cada trama = 66 bytes.

Datos trama Ethernet: 1460 bytes

Sobrecarga total: 66 bytes

Total: 1526 bytes

A continuación realizamos el cálculo del ancho de banda tomando en cuenta los datos anteriores

1. Determinamos el número de tramas

$$\#t = \frac{tamaño\ de\ la\ aplicación}{datos\ trama\ ethernet}$$

$$\#t = \frac{43\ Kbytes}{1460\ bytes}$$

$$\#t = 29,85$$

$$\#t = 30$$

2. Determinamos la sobrecarga del paquete transmitido

$$sobrecarga\ total = \#t * sobrecarga\ ethernet$$

$$sobrecarga\ total = 30 * 66\ bytes$$

$$sobrecarga\ total = 1980\ bytes$$

3. Calculamos los datos transmitidos en una imagen

$$datos\ transmitidos = tamaño\ de\ la\ aplicación * sobrecarga\ \ total$$

$$datos\ transmitidos = 43\ Kb * 1,98Kb$$

$$datos\ transmitidos = 44,98\ Kbytes$$

$$datos\ transmitidos = 359,84Kbits$$

4. Por último establecemos el ancho de banda requerido por una sola cámara para una frecuencia de 10 imágenes por segundo, que es el parámetro promedio admisible en aplicaciones de video vigilancia

$$AB\ cámara = \frac{359{,}84Kbits}{1\ cámara} * \frac{10\ imágenes}{1\ seg}$$

$$AB\ cámara = 3{,}5984Mbps$$

$$AB\ total = \#cámaras * AB\ cámara$$

$$AB\ total = 28 * 3{,}598\ Mbps$$

$$AB\ total = 100{,}744\ Mbps$$

Resolución	IPS	Nivel de Actividad	Rata de Bits (Kbps)	Almcto. (GB/sem.)
CIF	3	Medio	160	12
CIF	7	Medio	185	13
CIF	15	Medio	200	14
CIF	30	Medio	500	36
2 CIF	3	Medio	320	23
2 CIF	7	Medio	370	27
2 CIF	15	Medio	400	29
2 CIF	30	Medio	1,000	72
4 CIF	3	Medio	640	46
4 CIF	7	Medio	740	53
4 CIF	15	Medio	800	58
4 CIF	30	Medio	2,000	144

Tabla 6.15 Consumo de ancho de banda de las cámaras a utilizar en el diseño del sistema de seguridad remota

Fuente:http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf

El consumo de ancho de banda de las cámaras a utilizar se puede observar en la tabla 6.16:

Cámara	Resolución	Imágenes por segundo (IPS)	Rata de bits (Kbps)	Gb/semana
1	2 CIF	15	400	29
2	2 CIF	15	400	29
3	2 CIF	15	400	29
4	2 CIF	15	400	29
5	2 CIF	15	400	29
6	2 CIF	15	400	29
7	2 CIF	15	400	29
8	2 CIF	15	400	29
9	2 CIF	15	400	29
10	2 CIF	15	400	29
11	2 CIF	15	400	29
12	2 CIF	15	400	29
13	2 CIF	15	400	29
14	2 CIF	15	400	29
15	2 CIF	15	400	29
16	2 CIF	15	400	29
17	2 CIF	15	400	29
18	2 CIF	15	400	29
19	2 CIF	15	400	29
20	2 CIF	15	400	29
21	2 CIF	15	400	29
22	2 CIF	15	400	29
23	2 CIF	15	400	29
24	2 CIF	15	400	29
25	2 CIF	15	400	29
26	2 CIF	15	400	29
27	2 CIF	15	400	29
28	2 CIF	15	400	29

Tabla 6.16 Consumo ancho de banda y almacenamiento de las cámaras

Elaborado por: Investigador

El sistema trabajará todo el día y mediante sensores durante la noche y fines de semana

La tabla sugiere una rata de bits de 400 Kbps por cámara, lo que la red debe esperar 28 cámaras, es decir:

28 x 400 Kbps = 11.2 Mbps

Almacenamiento:

La tabla también indica que una sola cámara necesitará 29Gb por semana,tomando en cuenta los tiempos muertos será cerca del 60% de 29Gb, es decir 17Gb, para cuatro semanas una cámara consumirá:

17Gb x 4Semanas = 68Gb por mes

23 cámaras necesitarán:

28 x 68Gb por mes = 1904 Gb por mes

Backup del servidor de video:

Dado que la red a implementarse en la empresa SISTELDATA S.A. maneja gran cantidad de información es necesario un sistema de almacenamiento por separado tipo NAS el cual tendrá un Grabador de video digital, las grabaciones se realizara cada semana para garantizar respaldo de la información.

Coste de Instalación y configuración de equipos

En la tabla 6.17 se muestra el costo que tiene esta instalación:

INSTALACIÓN Y CONFIGURACIÓN			
Requerimiento	**Cant.**	**Precio U.**	**Total**
Instalación de puntos de red	28	25	700
Punto de Instalación Servidor y equipo de grabación	3	25	75
Programación, Configuración y Puesta en Marcha del Sistema	1	200	200
Costo total		975	

Tabla 6.17: Coste de instalación

Elaborado por: Investigador

Coste total del proyecto

En la tabla 6.18 se muestra el coste total del proyecto

COSTE		
Instalación y configuración	**Equipos utilizados**	**TOTAL**
975	13339,59	14314,59

Tabla 6.18: Coste Total

Elaborado por: Investigador

Conclusiones y recomendaciones finales

Conclusiones:

- Para el diseño de un sistema de video vigilancia y monitoreo en tiempo real sobre una red IP, se ha realizado la investigación de diversos productos, marcas, normas, criterios y tendencias los cuales en conjunto forjan este proyecto.
- Una vez comparada la tecnología, se estableció que la mejor alternativa para un sistema de vigilancia es la digital, ya que es compatible con los diferentes servicios manejados actualmente.
- El diseño del Sistema de seguridad remota, prevee ser escalable es decir que se adapte con facilidad a nuevas tecnologías y que pueda fácilmente expandirse en el futuro, facilitando actualizaciones

Recomendaciones:

- Utilizar equipos que brinden mayores prestaciones a bajos costos sin que esto perjudique a la calidad de los mismos
- Para la selección de equipos se debe tener en cuenta la tecnología de los mismos ya que puede ser analógica o digital
- Adquirir equipos de última tecnología para que pueda actualizarse el sistema de seguridad remota conforme al avance de la tecnología

6.7 Referencia Bibliográfica

Libros:

- WILLIAM, Stallings (2000) "*Comunicaciones y redes de computadores*" 6ta ed.
- BETHENCOURT, Tomás (1993) "*Sistemas de vídeo en componentes colorimétricas*" THOMSON PARANINFO, S.A. p.p. 85,89
- GARCÍA, Jesús; RAYA, José; RAYA, Víctor "*Alta velocidad y calidad de servicio en redes IP*"
- RAY, John, "*Edición Especial TCP/IP*"
- PAREJA, Emilio (1991) "*Sensores y cámaras CCD*" Creaciones Copyright p.150
- WATKINSON, John (1993) "*El arte del vídeo digital*" Ediciones TELEVES p.p. 25,29.

Internet:

- http://www.monografias.com/trabajos33/telecomunicaciones/telecomunicaciones.shtml
- http://definicion.de/seguridad/
- http://www.elprisma.com/apuntes/curso.asp?id=7673
- http://www.casadomo.com/casadomo/biblioteca/axis_las_redes_ip.pdf
- http://www.plusformacion.com/Recursos/r/Sistemas-telecomunicaciones-Concepto-IP-nuevas-redes-Integradas
- http://usuarios.multimania.es/janjo/janjo1.html
- http://www.edukits.com.ar/data/sistemas_comunicaciones_r35_silica.pdf
- http://pdf.rincondelvago.com/sistemas-de-comunicaciones.html
- http://www.slideshare.net/ronaldreales/direccionamiento-ip-basico-i
- http://www.monografias.com/trabajos29/direccionamiento-ip/direccionamiento-ip.shtml
- http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf
- http://www.casadomo.com/noticiasDetalle.aspx?c=29&idm=37

- http://www.sistemasdeseguridad.com.ec/pdf/AV-AVC796ZD.pdf
- http://www.sistemasdeseguridad.com.ec/usuarios/Listado_precios.pdf
- http://www.boschsecurity.com.mx/_archivos_productos_sitios_la/boletines_informativos/ebrief/2006/Estimando_Ancho_de_Banda.pdf
- http://www.axis.com/es/products/video/about_networkvideo/bandwidth.htm
- http://www.millenium.net.mx/anchobanda.html
- http://www.ciscoredes.com/ccna3/90-vlan.html

6.8 GLOSARIO

ADSL	Equipo de comunicación
CCTV	Circuito cerrado de televisión
CoS	Clase de servicio
DHCP	Protocolo de comunicación
FTP	Protocolo de comunicación
Gb/s	Gigabit por segundo
HTTP	Protocolo de comunicación
IETF	Internet EngineeringTaskForce
IP	Protocolo de Internet
ISP	Proveedor de servicios de Internet
ITU-T	Estándar de comunicación
JPEG	Formato de compresión de imágenes
LAN	Red de área local
MAN	Red de área metropolitana
MPEG	Formato de compresión de imágenes
MPLS	MultiProtocolLabelSwitching
NVR	Grabador de video
PSTN	Red tradicional de voz
QoS	Calidad de servicio
RX	Receptor
TCP/IP	Protocolo de comunicación
TIP	Telefonía IP
TX	Transmisor
VoIP	Voz sobre IP
VPN	Red virtual privada
WAN	Red de área extensa

6.9 ANEXOS

Anexo 1: Encuesta

ENCUESTA SOBRE SEGURIDAD PARA LA EMPRESA SISTELDATA S.A.

OBJETIVO DE LA ENCUESTA:

Conocer a través de esta encuesta cual es el pensamiento de los empleados acerca de la seguridad en la empresa.

FUENTE DE RECOLECCION: Empleadores y empleados de la empresa

Fecha:

PREGUNTAS:

1. ¿La empresa cuenta con un sistema de seguridad?

   SI( ) NO( )

2. ¿Debería la empresa contar con un sistema de seguridad?

   SI( ) NO( )

3. ¿El monitoreo del sistema de seguridad se lo debería realizar desde cualquier lugar?

   SI( ) NO( )

4. El sistema de seguridad tendría que contar con:

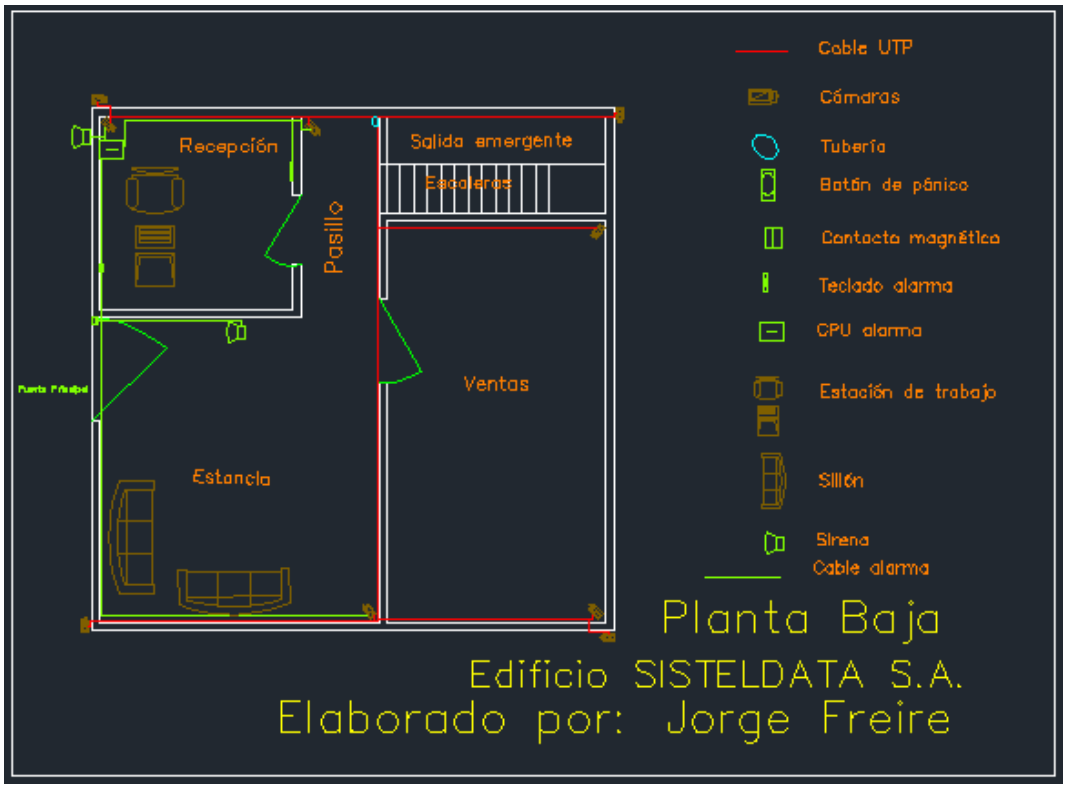
a. Cámaras ( )
b. Sensores ( )
c. Cámaras y sensores ( )

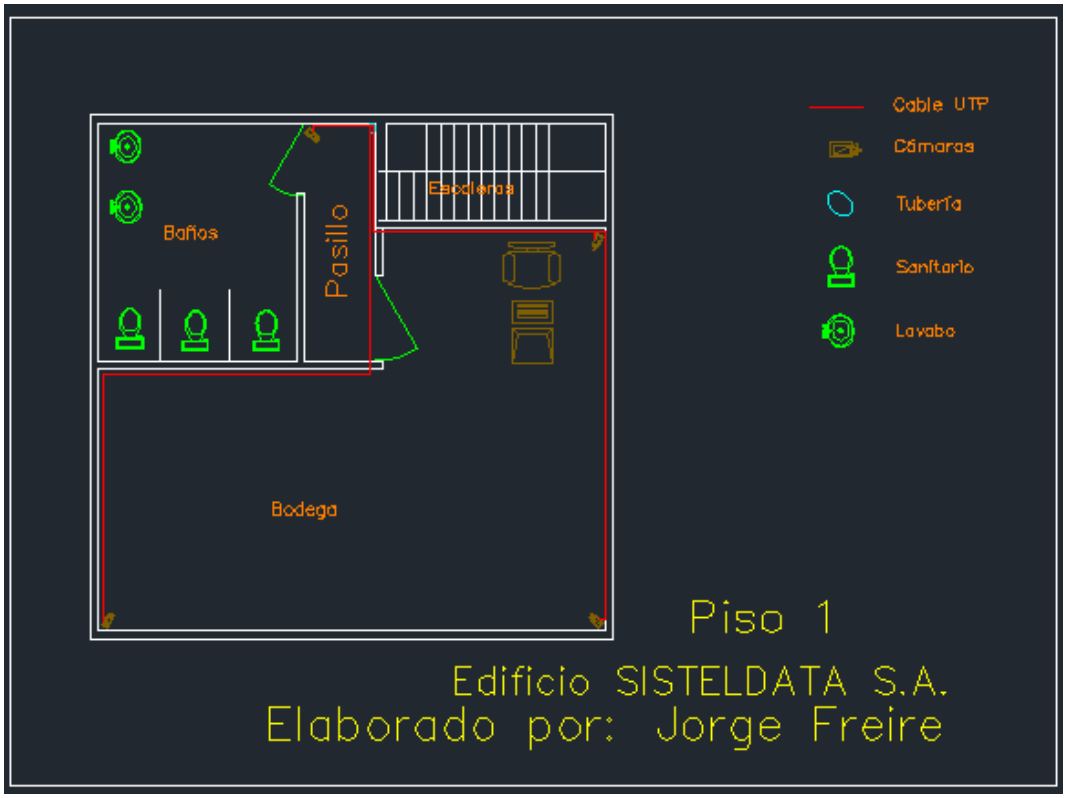
5. ¿Se debería utilizar un sistema de seguridad IP para brindar seguridad remota a la empresa?

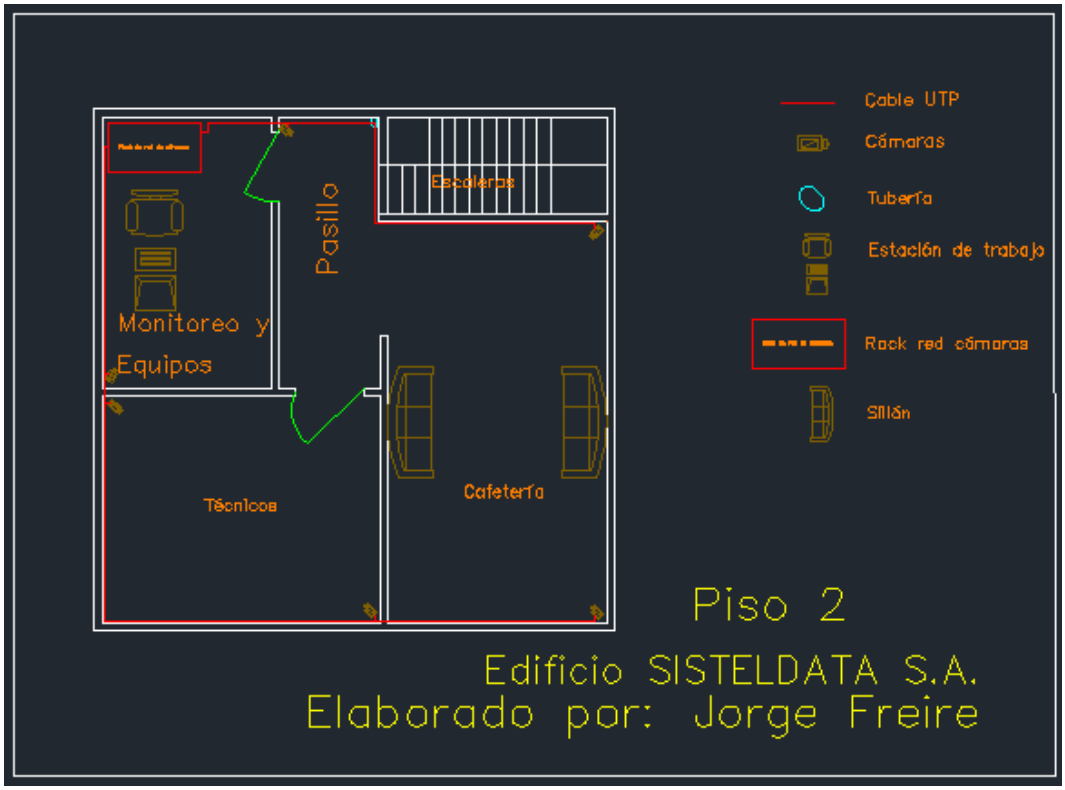
   SI( ) NO( )

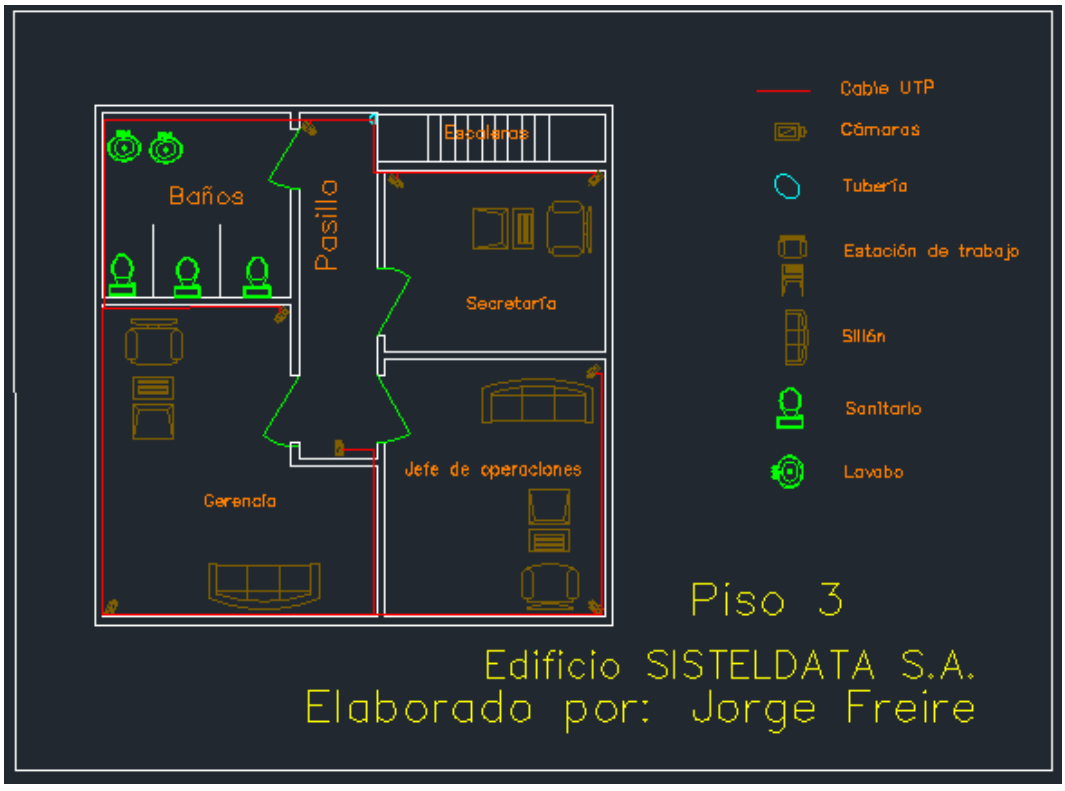
Encuestador: Jorge Freire

Anexo 2: Cableado de las cámaras IP de las cuatro plantas

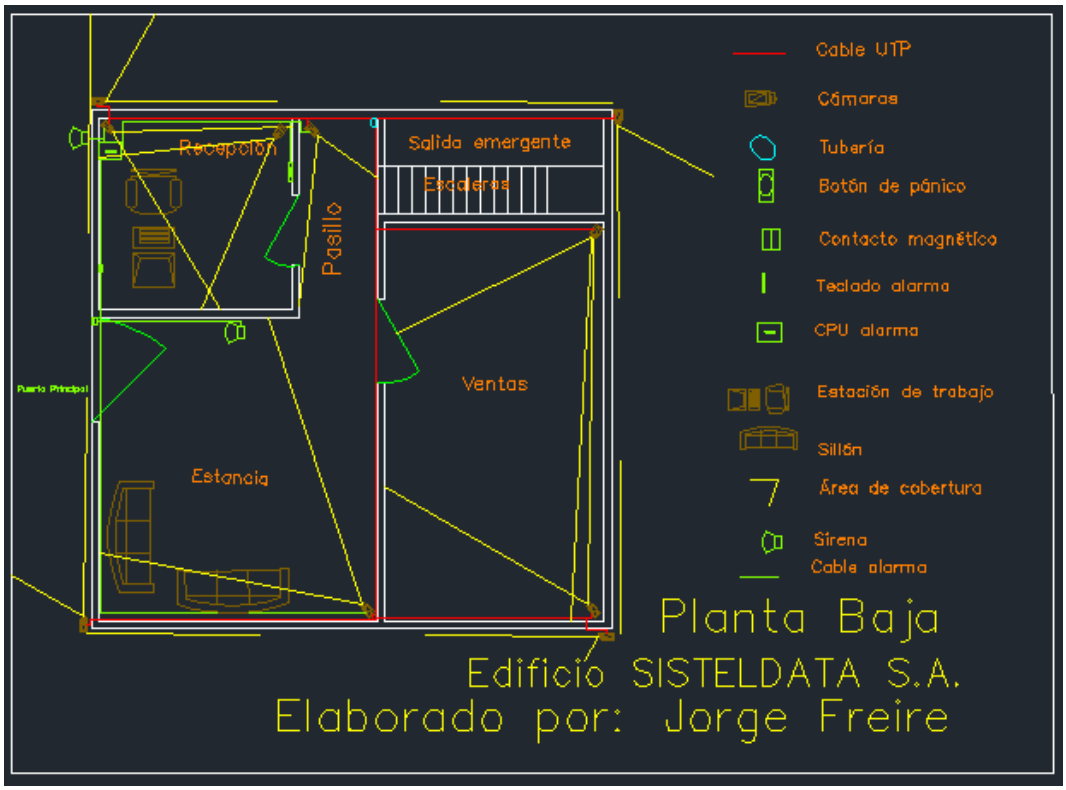


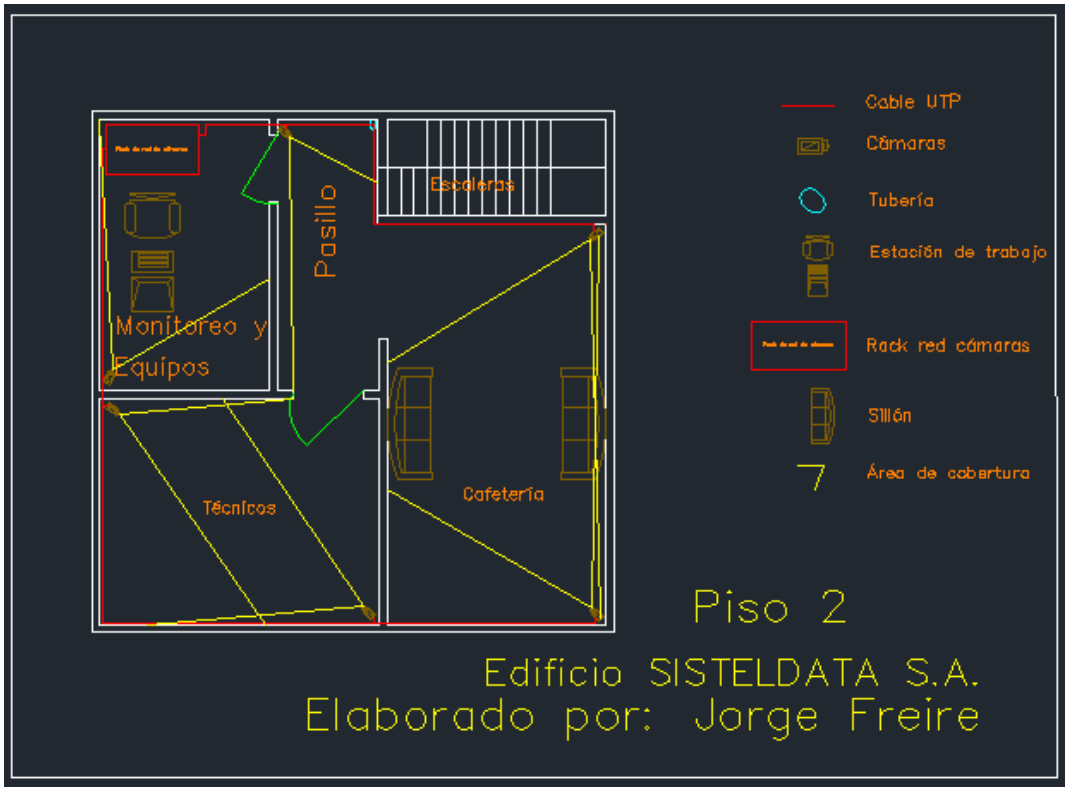


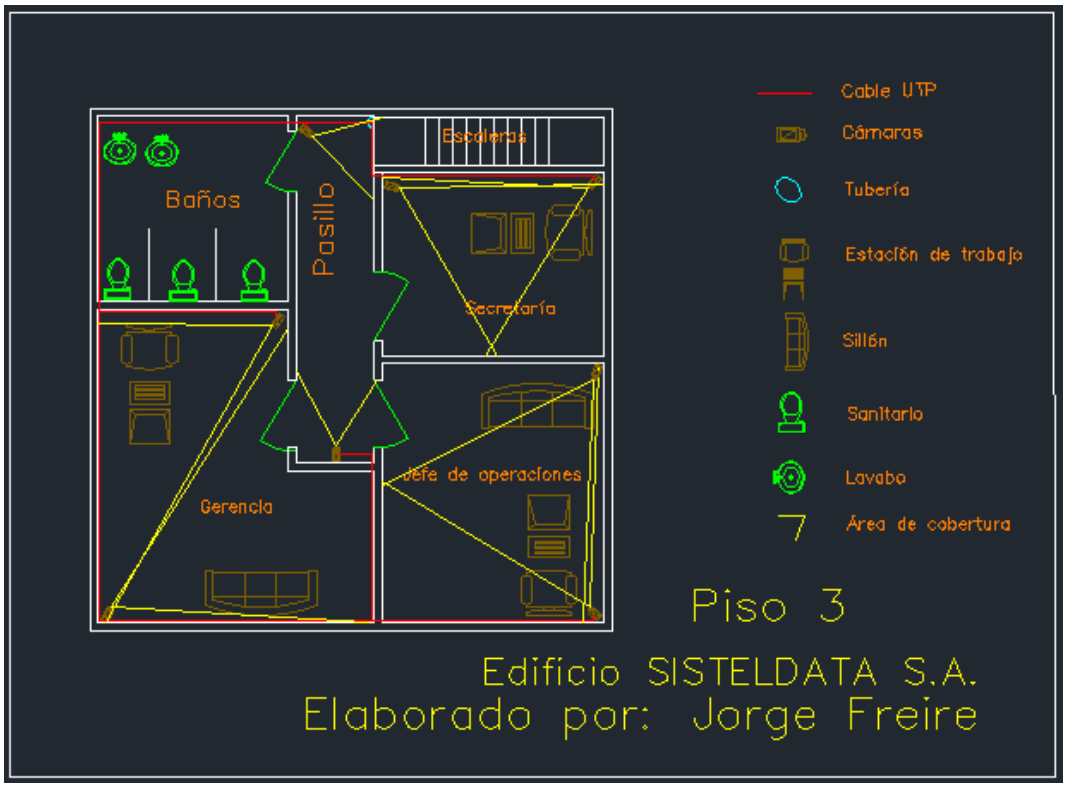

Escaleras
Pasillo
Monitoreo y
Equipos
Técnicos
Cafetería
Cable UTP
Cámaras
Tubería
Estación de trabajo
Rack red cámaras
Sillón
Piso 2
Edificio SISTELDATA S.A.
Elaborado por: Jorge Freire


Escaleras
Baños
Pasillo
Secretaría
Jefe de operaciones
Gerencia
Cable UTP
Cámaras
Tubería
Estación de trabajo
Sillón
Sanitario
Lavabo
Piso 3
Edificio SISTELDATA S.A.
Elaborado por: Jorge Freire

Anexo 3: Cobertura de las cámaras IP de las diferentes áreas de las cuatro plantas




Escaleras
Pasillo
Monitoreo y
Equipos
Técnicos
Cafetería
Cable UTP
Cámaras
Tubería
Estación de trabajo
Rack red cámaras
Sillón
Área de cobertura
Piso 2
Edificio SISTELDATA S.A.
Elaborado por: Jorge Freire


Escaleras
Baños
Pasillo
Secretaría
Gerencia
Jefe de operaciones
Cable UTP
Cámaras
Tubería
Estación de trabajo
Sillón
Sanitario
Lavabo
Área de cobertura
Piso 3
Edificio SISTELDATA S.A.
Elaborado por: Jorge Freire

Anexo 3: Características Técnicas de los equipos

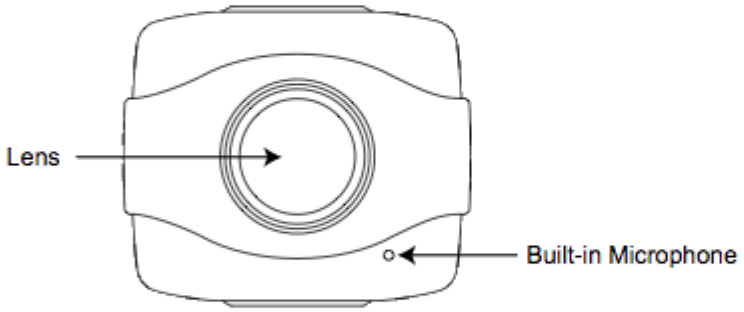
Cámara IP7130

::Ficha Técnica::

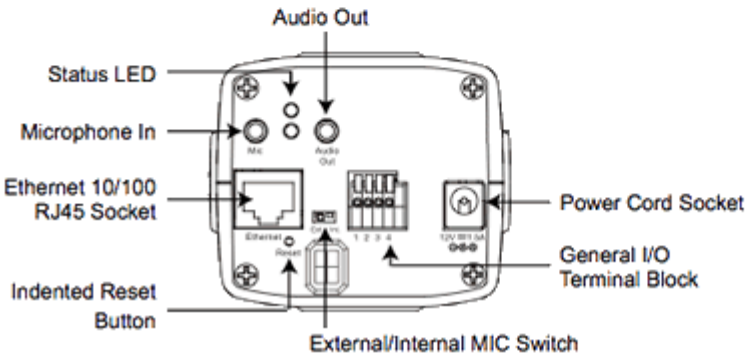
Caracteristicas

- Sensor de imagen CMOS 1/4" con resolución VGA
- Compresión en tiempo real MPEG-4 y MJPEG (Dual Codec)
- Soporta stream dual simultáneo
- Detección antisabotaje de bloqueo, redireccionamiento o pintada con spray
- Soporta vigilancia Móvil 3GPP
- PoE compatible 802.3af integrado
- Soporta audio bidireccional mediante protocolo SIP
- E/S Digitales para Sensor y Alarma
- Transmisión de Datos Criptografados HTTPS
- Software libre ST7501 de gestión central de 32 canales

Vista Frontal



Vista Posterior

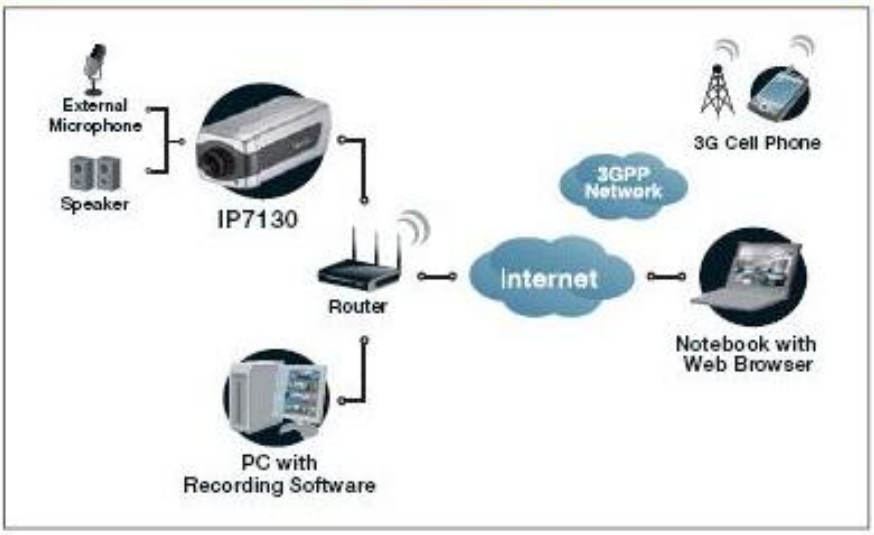


System	· CPU: Mozart 120 SoC · Flash: 8MB · RAM: 64MB + 64MB · Embedded OS: Linux 2.6
Lens	· CS-mount, f = 4.0 mm, F1.6, Fixed
Angle of View	· 71° (horizontal)
Shutter Time	· 1/5 sec. to 1/15,000 sec.
Image Sensor	· 1/4" CMOS sensor in VGA resolution
Minimum Illumination	· 0.1 Lux / F1.6
Video	· Compression: MJPEG & MPEG-4 · Streaming: Simultaneous dual streams MPEG-4 streaming over UDP, TCP, HTTP or HTTPS MPEG-4 multicast streaming MJPEG streaming over HTTP or HTTPS · Supports 3GPP mobile surveillance · Frame rates: MPEG-4: Up to 30/25 fps at 640x480 MJPEG: Up to 30/25 fps at 640x480
Image Settings	· Adjustable image size, quality and bit rate · Time stamp and text caption overlay · Flip & mirror · Configurable brightness, contrast, saturation, sharpness, white balance and exposure · AGC, AWB, AES · BLC (Backlight Compensation) · Supports privacy masks
Audio	· Compression: GSM-AMR speech encoding, bit rate: 4.75 kbps to 12.2 kbps MPEG-4 AAC audio encoding, bit rate: 16 kbps to 128 kbps · Interface: Built-in microphone External microphone input Audio output External/Internal microphone switch · Supports two-way audio via SIP protocol · Supports audio mute

Networking	· 10/100 Mbps Ethernet, RJ-45 · Protocols: IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS and PPPoE
Alarm and Event Management	· Triple-window video motion detection · Tamper detection · One D/I and one D/O for external sensor and alarm · Event notification using HTTP, SMTP or FTP · Local recording of MP4 file
Security	· Multi-level user access with password protection · IP address filtering · HTTPS encrypted data transmission
Users	· Live viewing for up to 10 clients
Dimension	· 154 mm (D) x 72 mm (W) x 62 mm (H)
Weight	· 623 g
LED Indicator	· System power and status indicator · System activity and network link indicator
Power	· 12V DC · Power consumption: Max. 6 W · 802.3af compliant Power-over-Ethernet
Approvals	· CE, LVD, FCC, VCCI, C-Tick
Operating Environments	· Temperature: 0 ~ 50 °C (32 ~ 122 °F) · Humidity: 90% RH

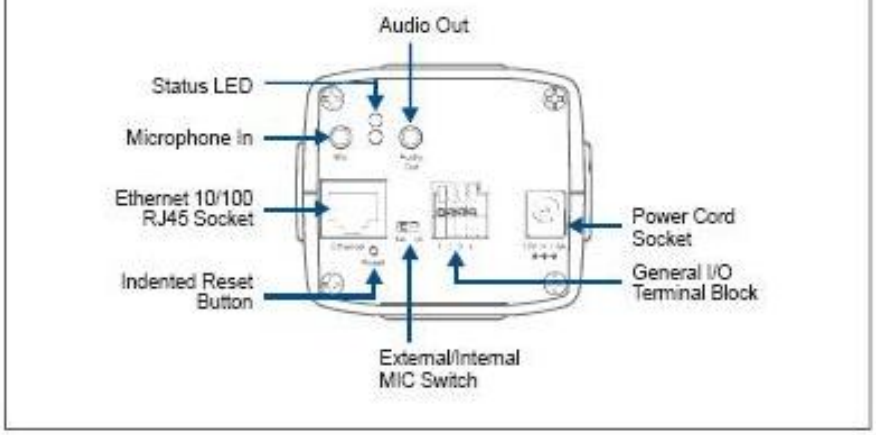
Viewing System Requirements	· OS: Microsoft Windows 2000/XP/Vista · Browser: Mozilla Firefox, Internet Explorer 6.x or above · Cell phone: 3GPP player · Real Player: 10.5 or above · Quick Time: 6.5 or above
Installation, Management, and Maintenance	· Installation Wizard 2 · 32-CH ST7501 central management software · Supports firmware upgrade
Applications	· SDK available for application development and system integration
Warranty	· 12 months

System Overview



External View

External View



NVR QNAPVioStar VS8032U

DETALLES DEL PRODUCTO

::Ficha Técnica::

Especificaciones de hardware

Procesador	Procesador de 2,8 GHz de Intel Core 2 Duo
Memoria	2 GB DDRII memoria RAM, 128 MB flash (DOM)
Capacidad de disco duro	8 x 3,5 "o SATA de 2,5" I / II HDD **NOTA:** El sistema se suministra sin unidad de disco duro.
Bandeja de la unidad de disco duro	8 x bandeja de hot-swap y pueden cerrar con llave
Puerto LAN	2 x puerto RJ-45 Ethernet de Gigabit

Indicadores LED	Estado, LAN, USB, disco duro 1, 2, de la unidad de disco duro 3, de la unidad de disco duro HDD 4, 5, de la unidad de disco duro HDD6, HDD7, HDD8
USB	4 x puerto USB 2.0 Dispositivo de USB UPS de soportes
Botones	Alimentación, restablecimiento
Panel LCD	Pantalla LCD con iluminación de fondo introduzca el botón, seleccione el botón de configuración
Aviso acústico de alarma	Sistema de advertencia
Factor de forma	Montaje en rack de 2U
Dimensiones	88.9(H) x 482.6(W) x 531.5(D) mm 3.5(H) x 19(W) x 20.93(D) mm
Peso	Peso neto: 12.15 kg / 26.79 lbs Bruto de peso: 16,7 kg / 36.82 lbs
Operación en medio ambiente	Temperatura 0 ~ 40°C / 32 ~ 104°F Humedad 0 ~ R.H. 95%
Fuente de alimentación	Entrada: 100-240 v CA, 47-63 Hz, salida: intercambios
Consumo de energía	101W escritura/lectura
VGA	Reservado
Ventilador	ventilador de refrigeración inteligente de 3 x 8 cm

Certificación	CE, FCC, VCCI, BSMI
	Caracteristicas de Software
Modo de visualización	1 / 4 / 6 / 8 / 9 / 10 / 12 / 16 / 20 / 25 / 36 / 42-canal visualización, modo de imagen en imagen, secuencial, modo de multipantalla
Número de canales compatibles (grabación)	Hasta 32
Formato de compresión	MxPEG H.264/ / MPEG-4 / M-JPEG (varían según los modelos de cámara)
Configuración de vídeo	Resolución, calidad, velocidad de fotogramas
E-mapa	Cargar E-mapa (JPEG)
	Grabación
Modo de grabación	Continua / manual / grabación de programación Grabación de alarma / alarma múltiples programaciones de grabación * Hasta 15 horarios son compatibles para cada cámara
Almacenamiento de información de búfer para imágenes de alarma (antes y después de eventos)	Pre-Recording: hasta 300 s / post–recording: hasta 300 seg (total 600 seg/10 min.)
Rendimiento de grabación	Hasta 30 fps en D1 o VGA para cada canal
Grabación de megapíxeles	Es compatible con cámaras de megapíxeles (hasta 8 megapíxeles)
Formato de archivo	AVI (códec QNAP es necesario para la reproducción)
	Reproducción
Canal de reproducción	Reproducción de 4 canales de Max al mismo tiempo
Modo de reproducción	Reproducir, pausar, detener, revertir el juego, marco siguiente / anterior, archivo de vídeo siguiente / anterior, control de velocidad diferente
Modo de visualización	Vista de reproducción única, 4 puntos de vista de reproducción
Modo de búsqueda	Por fecha & tiempo, línea de tiempo, eventos y análisis inteligente de vídeo (IVA)
Análisis inteligente de vídeo (IVA)	Detección de movimiento, el objeto que falta, el objeto extraño, fuera de foco y oclusión de la cámara
Mejora de la reproducción	Pantalla completa, la instantánea de video, el zoom digital, la marca de agua digital
Exportación	Convertir varios archivos de registro a un archivo de avi
Descargar	Descargar grabaciones a través de la web

Almacenamiento de información	
Administración de discos	• Único disco, RAID 0 (División de disco), RAID 1 (duplicación de disco), RAID 5, RAID 5 + hot spare, RAID 6, RAID 6 + hot spare y JBOD (volumen de disco lineal) • Expansión de capacidad RAID en línea • Migración en línea de nivel de RAID • S.M.A.R.T. DE LA UNIDAD DE DISCO DURO • Análisis de bloques defectuosos • Apoyar el programa de instalación de PC-menos RAID a través de panel LCD para la primera instalación • Servicios: Administrador de archivos Web, FTP, SMB/CIFS
Panel LCD	
	• Configuración de RAID de PC-menos para la primera instalación de tiempo • Cuando el sistema está listo, los usuarios pueden comprobar o configurar la configuración IP, información de disco físico, información de volumen, información del sistema, apagar o reiniciar la NVR, etc..
Red	
Apoyo	HTTP, TCP/IP, SMTP, DHCP, Static IP, DNS, DDNS, FTP, NTP, UPnP, Failover, balanceo de carga, configuración de Multi-IP
Cámara IP Address & Port	Permite establecer la dirección IP de LAN/WAN de cada cámara
Dual Gigabit LAN	• Conmutación por error: en caso de que se produce un error en uno de la red LAN, los paquetes enviados a la NVR serán tratados por la otra interfaz de LAN • Balanceo de la carga: Agregación de enlaces es compatible para aumentar la velocidad de transferencia • Configuración de Multi-IP: The NVR puede servir grupos de red diferentes en dos subredes diferentes
Seguridad	
Sistema de operación	Embebido en Linux, libre de los ataques de virus y accidente de PC
Lista de usuarios en línea	Registro de los usuarios conectados actualmente y anteriormente ha iniciado sesión en el NVR
Control de acceso de host	Especifique las conexiones a ser permitido y negó a acceder a NVR
Administración de usuario	El derecho a supervisar y la reproducción de que cada cámara puede definirse por separado para cada usuario (hasta 32 usuarios)
Notificación de alerta	Correo electrónico, timbre, registros de sucesos
UPS	Soporte de APC / MGE (USB tipo UPS)
Registros de sucesos	Registros de sucesos detallados del sistema de advertencia, error de disco duro, desconexión de red, estado de UPS y servicios de red de los usuarios y acceso a los datos
Soporte de idiomas	
	Inglés / francés / alemán / italiano / japonés / español / simplificado chino / tradicional chino / danés / holandés / finlandés / húngaro / coreano / Noruega / polaco / portugués / ruso / sueco
Requisitos de PC cliente	
CPU	• Formato M-JPEG (hasta 32 canales): Dual core CPU 2,2 GHz o superior • MPEG-4 / MxPEG / formato H.264 (hasta 32 canales): Núcleo cuádruple CPU 2,2 GHz o superior * Para un mayor rendimiento de vigilancia, por favor, seleccione los modelos más avanzados de la PC.
Memoria	1 GB o superior
Sistema de operación	Windows XP / Vista / 7
Explorador de Web	Internet Explorer 6.0 o posterior
Interfaz de red	10/100 Mbps o superior
Resolución de la vista	Sugerida 1024 x 768 píxeles o superior
Software utilidad	
Buscador de QNAP	Busca y establece una configuración rápida para NVR mediante el QNAP Finder
VioStor Player	Escuchar los archivos de grabación en su equipo con Windows fácilmente
Prueba de marca de agua	Compruebe si los archivos de grabación de VioStor NVR se modifican o no

SwitchTP LINK TL-SL3428

Interface	24 Puertos RJ45 de 10/100Mbps (Auto Negociación/Auto MDI/MDIX) 4 Puertos RJ45 de 10/100/1000Mbps (Auto Negociación/Auto MDI/MDIX) 2 Ranuras SFP de 100/1000Mbps 1 Puerto de Consola
Medios de Red	10BASE-T: Cable UTP categoría 3, 4, 5 (máximo 100m) 100BASE-TX/1000Base-T: cable UTP categoría 5, 5e, 6 o mayor (máximo 100m) 1000BASE-X: MMF, SMF
Dimensiones (W X D X H)	17.32 x 8.7 x 1.73 pulg. (440 x 220 x 44 mm)
Suministro de Energía Eléctrica	100～240VAC, 50/60Hz

RENDIMIENTO	
Banda Ancha / Tarjeta madre posterior	12.8Gbps
Tabla de Direcciones MAC	8k
Velocidad de Reenvío del Paquete	9.5Mpps
Estructura Jumbo	10240 Bytes

CARACTERÍSTICAS DEL SOFTWARE	
Características de Conmutación L2	IGMP Snooping V1/V2/V3 802.3ad LACP (Hasta 8 puertos de agregación, que contienen 8 puertos por grupo) Árbol de Expansión STP/RSTP/MSTP Aislamiento de Puerto Filtrado / protección BPDU Protección de TC/Raíz Detección de Conexión de Bucle Control de flujo 802.3x
Calidad de Servicio	Soporta prioridad 802.1p CoS/DSCP Soporta 4 colas de prioridad Programación de colas: SP, WRR, SP+WRR Límite de Velocidad basada en el Puerto / flujo VLAN de Voz
VLAN	Soporta IEEE802.1Q con grupos VLAN 4K y 4K VIDs Port/ MAC/ VLAN basada en el Protocolo GARP/GVRP Configuración VLAN de Administración

Lista de Control de Acceso	Filtrado de paquete L2~L4 basado en la dirección MAC origen y destino, dirección IP, Puertos TCP/UDP, 802.1p, DSCP, protocolo y ID de VLAN Rango Basado en el Tiempo
Security	Vínculo P-MAC-Puerto-VID Autentificación Basada en MAC / Puerto IEEE 802.1X , Radius, VLAN Invitado Defensa de DoS DAI (Dynamic ARP inspection – Inspección ARP Dinámica) SSH v1/v2 SSL v2/v3/TLSv1 Seguridad de Puertos Control de Tormentas Broadcast / Multicast / Unicast Desconocido

Management	Administración GUI y CLI basada en la Web SNMP v1/v2c/v3, compatible MIBs públicos y MIBs privados de TP-LINK RMON (grupos 1, 2, 3, 9) DHCP/BOOTP Client, DHCP Snooping, DHCP Opción 82 Monitoreo de CPU Duplicación de Puertos Configuración de Tiempo: SNTP Característica NDP/NTDP Integrada Actualización del Firmware: TFTP & Web Diagnóstico del sistema: VCT SYSLOG y MIBS Público

OTROS	
Certificación	CE, FCC
Contenido del Paquete	Switch; Cable de alimentación; Guía de Instalación; CD de Recursos; Kit de Base de Soporte; Patas de Goma
Requisitos del Sistema	Microsoft® Windows® 98SE, NT, 2000, XP, Vista™ or Windows 7, MAC® OS, NetWare®, UNIX® or Linux.
	Temperatura de Operación: 0℃~40℃ (32℉~104℉);

SIRENA PARA ALARMA DE 1 TONO

Características técnicas:

- Sirena electrónica de gran potencia.
- Acabado en ABS.
- Color: negro.
- Sirena con cables.
- Tensión de trabajo: 6-15Vdc.
- Alimentación: 12Vdc.
- Frecuencia de de oscilación: 0.9-4kHz.
- Dimensiones: 100 x Ø110mm.
- Peso: 430g.

- Consumo a 12V: 1300mA.
- Nivel de sonido: 125dB.
- Agujeros de montaje: 52 x 49mm.

CONTACTO MAGNÉTICO

Características técnicas:

- Contacto magnético blindado NA y NC de 70 mm. de rango.
- Reforzado para portones.
- Conducto flexible de acero inoxidable de 61 cm.
- Para ser montado sobre superficie, precableado enfundado.
- Montaje conto tornillo semi-empotrados.
- Abertura: 70mm.Enforcer, Seco-larm USA Inc.