DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA

TEMA: "ANÁLISIS Y ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN PARA EL CAMPUS POLITÉCNICO Y UN SISTEMA DE CONTROL DE ACCESOS PERIMETRAL DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO (ESPE - SANGOLQUÍ)".

AUTOR: OCAMPO ANDRADE, ÍTALO BAYARDO

DIRECTOR: ING. DUQUE CAJAS, MANUEL DARÍO
CODIRECTOR: ING. HARO BÁEZ, RAÚL VINICIO

SANGOLQUI

2017

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERIA EN ELECTRÓNICA Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que el trabajo de titulación, ***"ANÁLISIS Y ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN PARA EL CAMPUS POLITÉCNICO Y UN SISTEMA DE CONTROL DE ACCESOS PERIMETRAL DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO (ESPE - SANGOLQUÍ)"***, realizado por el señor ***ITALO BAYARDO OCAMPO ANDRADE***, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar al señor ***ITALO BAYARDO OCAMPO ANDRADE*** para que lo sustente públicamente.

Sangolquí, 19 de mayo del 2015

ING. DUQUE CAJAS MANUEL DARIO

DIRECTOR

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERIA EN ELECTRÓNICA Y TELECOMUNICACIONES

AUTORIA DE RESPONSABILIDAD

Yo, ***ITALO BAYARDO OCAMPO ANDRADE***, con cédula de identidad N°1708517188, declaro que este trabajo de titulación ***"ANÁLISIS Y ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN PARA EL CAMPUS POLITÉCNICO Y UN SISTEMA DE CONTROL DE ACCESOS PERIMETRAL DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO (ESPE - SANGOLQUÍ)"*** ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 19 de mayo del 2015

ITALO BAYARDO OCAMPO ANDRADE

C.C. 1708517188

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERIA EN ELECTRÓNICA Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, ***ITALO BAYARDO OCAMPO ANDRADE***, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación ***"ANÁLISIS Y ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN PARA EL CAMPUS POLITÉCNICO Y UN SISTEMA DE CONTROL DE ACCESOS PERIMETRAL DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO (ESPE - SANGOLQUÍ)"*** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolquí, 19 de mayo del 2015

ITALO BAYARDO OCAMPO ANDRADE

C.C. 1708517188

DEDICATORIA

A mis padres, hermanos y sobrinos, por su incansable e ilimitado apoyo y amor incondicional a lo largo de toda mi vida estudiantil y compartir conmigo cada tristeza y alegría.

A mis seres queridos Marcelio y Guillermo, que están junto a Dios, quienes me bendicen y me protegen en cada actividad de mi vida.

A todos, quienes han confiado en mí y me han motivado para concluir esta etapa de mi vida y me han incentivado para crecer y desarrollarme profesionalmente.

AGRADECIMIENTO

A Dios y a mi familia, quienes me han apoyado cada instante para que este reto de superación se convierta en realidad.

A mis tutores, quienes me ha guiado durante en el desarrollo del presente proyecto.

A la ESPE que me permitió desarrollar el proyecto, por la confianza y su colaboración durante la recolección de la información.

A mis amigos, quienes han compartidos los momentos más importantes de mi vida, me han brindado su apoyo durante todo el camino para conseguir mis metas.

ÍNDICE DE CONTENIDO

CERTIFICADO ii
AUTORÍA DE RESPONSABILIDAD iii
AUTORIZACIÓN iv
DEDICATORIA v
AGRADECIMIENTO vi
ÍNDICE DE CONTENIDO vii
ÍNDICE DE TABLAS xi
ÍNDICE DE FIGURAS xii
RESUMEN xiv
ABSTRACT xv
GLOSARIO xvi
PRÓLOGO xviii
JUSTIFICACIÓN xix
IMPORTANCIA xx
ALCANCE DEL PROYECTO xxi
OBJETIVOS xxii
CAPÍTULO 1 1
INTRODUCCIÓN 1
1.1 Historia de los Sistemas de CCTV y Control de Accesos. 2
1.2 Evolución de los Sistemas de Seguridad 6
1.3 Regulaciones para la Utilización de Videocámaras para Video Vigilancia en Lugares Públicos en Ecuador 8
1.4 Control de Accesos 11
1.5 Control de Acceso Vehicular 13
1.5.1 Beneficios y Ventajas 14
CAPITULO 2 16
SISTEMA CCTV Y CONTROL DE ACCESOS 16
2.1 Conceptos Básicos De Un Sistema Cctv Y Control De Accesos 16
2.1.1 Sistema CCTV 16

2.1.2 Control de Accesos....17
2.2 Estructura de los Sistemas CCTV y Control de Accesos....18
2.2.1 Componentes de un CCTV IP....18
2.2.2 Componentes de un Control de Acceso....20
2.3 Aplicaciones Del Cctv Y Control De Accesos....23
2.3.1 Aplicaciones para el CCTV....23
2.3.2 Aplicaciones para el Control de Accesos....24
2.4 Conceptos De Redes....26
2.4.1 Modelo de Comunicación....26
2.4.2 Concepto de Red....26
2.4.3 Topología de red....27
2.4.4 Tipos de redes....29
2.4.5 Red de Área Local....29
2.4.6 Red de Área Metropolitana....30
2.4.7 Red de Área Extendida....30
2.4.8 Redes Vlans....31
2.4.9 Tipos de Redes Ethernet....32
2.5 Hardware De Redes....33
2.6 Protocolos De Transmisión Datos, Voz Y Video....34
2.6.1 Modelo OSI/ISO....35
2.6.2 Modelo TCP/IP....36
2.6.3 Internet....36
2.6.4 Direcciones IP....37
2.6.5 Dirección IPv4....37
2.6.6 Plataformas de Hardware para CCTV....38
2.6.8 Plataforma NVR....39
2.6.9 Switch o Conmutador....40
2.6.10 Servidores o Codificadores de Video....41
2.6.12 Servidores de Video Montados en Rack.....44
2.6.13 Codificadores de vídeo independientes....44
2.7 Sistemas Inalámbricos De Transmisión....45
2.8 Sistemas Alámbricos De Transmisión....67
2.9 Sistemas Híbridos....74
CAPITULO 3....77
ESTUDIO Y SITUACIÓN ACTUAL DE LA ESPE....77

3.1 Descripción Física le las Instalaciones del Campus Politécnico (ESPE - Sangolquí).....77
3.2 Descripción De Los Sistemas Disponibles.....82
3.3 Análisis De Los Servicios Y Necesidades De Las Instalaciones.....86
CAPITULO 4.....96
ESTUDIO Y DISEÑO DEL SISTEMA DE COMUNICACIONES DEL CIRCUITO CERRADO DE TELEVISIÓN Y CONTROL DE ACCESOS DEL CAMPUS ESPE-SANGOLQUI.....96
4.1 Arquitectura Del Sistema.....96
4.2 Sistema De Transmisión De La Señal De Video 104
4.2.2. Sistema De Transmisión De Las Señales De Video Y Datos..... 106
4.3 Diseño Y Cobertura Del Sistema..... 109
4.4 Control De Accesos Al Campus Espe – Sangolquí 113
4.4.1 Detalle Del Equipamiento Básico Para El Control De Los Parqueadero . 117
4.4.2 Reconocimiento De Matriculas Para Control De Acceso Vehicular. 121
4.5 Red De Integración Del Sistema Del Cctv Y Control De Accesos En La Espe -Sangolquí..... 124
CAPITULO 5.....129
COSTOS DEL SISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN Y CONTROL DE ACCESOS.....129
5.1 Bases Técnicas..... 129
5.1.1 Generalidades..... 129
5.1.2 Especificaciones Funcionales 130
5.1.3 Especificaciones Del Radio 132
5.1.4 Especificaciones Físicas..... 134
5.2 Especificaciones De Los Dispositivos De Captura Video..... 134
5.2.1 Especificaciones Del Sistema 135
5.2.3 Especificaciones Fisicas Y Funcionales..... 135
5.2.4 Especificaciones De Sistema De Respaldo De Energía 136
5.2.5 Especificaciones Físicas Y Funcionales 136
5.3 Especificaciones Tecnicas De Productos 137
5.4 Costos De Los Equipos. 145
5.5 Análisis Costo Beneficio 150
CAPITULO 6.....153
CONCLUSIONES Y RECOMENDACIONES.....153
6.1 Conclusiones..... 153

6.2 Recomendaciones. 154

BIBLIOGRAFÍA.....158

ÍNDICE DE TABLAS

TABLA 1 DISTRIBUCIÓN CÁMARAS POR SECTORES EN EL CAMPUS ESPE 98
TABLA 2 SUBCONTRATOS Y SERVICIOS 146
TABLA 3 EQUIPOS INSTALACIÓN Y CONFIGURACIÓN 146
TABLA 4 INVERSION DE EQUIPOS DE PARKING ESPE.....147

ÍNDICE DE FIGURAS

FIGURA 1 SISTEMA CCTV 2
FIGURA 2 CÁMARA IP 4
FIGURA 3 CCTV ANALÓGICO 6
FIGURA 4 EVOLUCIÓN DEL SISTEMA CCTV 8
FIGURA 5 LEY ORGÁNICA 15/1999 PROTECCIÓN DE DATOS 8
FIGURA 6 OJOS DE ÁGUILA- MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO 9
FIGURA 7 LABORATORIOS – ZONAS PROTEGIDAS 12
FIGURA 8 SISTEMA ELECTROMECÁNICO DE VALLAS 13
FIGURA 9 SISTEMA CCTV IP 17
FIGURA 10 ESTRUCTURA SISTEMA CCTV IP 18
FIGURA 11 CONTROL DE ACCESO VEHICULAR 20
FIGURA 12 SOFTWARE DE GESTIÓN 22
FIGURA 13 N4S PARKING ES UNA SOLUCIÓN RFID 25
FIGURA 14 TIPOS DE TOPOLOGÍAS FÍSICAS 28
FIGURA 15 TIPOS DE REDES DE COMUNICACIÓN 29
FIGURA 16 ESQUEMA DE UNA RED LOCAL 30
FIGURA 17 ESQUEMA DE UNA RED DE ÁREA METROPOLITANA 31
FIGURA 18 ESQUEMA DE UNA RED VLAN 32
FIGURA 19 ESQUEMA HARDWARE DE RED DE CCTV 34
FIGURA 20 CAPAS DEL PROTOCOLO MODELO OSI 35
FIGURA 21 CAPAS DEL PROTOCOLO MODELO TCP/IP 36
FIGURA 22 SISTEMA DE CÁMARA CON PLATAFORMA NVR 40
FIGURA 23 SISTEMA DE VIGILANCIA CON SWITCH 41
FIGURA 24 SISTEMA DE VIGILANCIA CON SERVIDOR DE VIDEO 42
FIGURA 25 CODIFICADOR DE VIDEO 43
FIGURA 26. RED ETHERNET HÍBRIDA 57
FIGURA 27. COMUNICACIÓN BLUETHOOTH 58
FIGURA 28. COMUNICACIÓN HOMERF 59
FIGURA 29. COMUNICACIÓN WIFI 61
FIGURA 30. PUNTOS DE ACCESO RED INALÁMBRICA 63
FIGURA 31. PC CARD 64
FIGURA 32. MEDIOS DE TRANSMISIÓN ALÁMBRICO 68
FIGURA 33. CABLE COAXIAL 68
FIGURA 34. CABLE UTP PAR TRENZADO SIN BLINDAJE 71
FIGURA 35. CABLE PAR TRENZADO BLINDADO 72
FIGURA 36. CABLE FIBRA ÓPTICA 73
FIGURA 37. LUZ EN EL INTERIOR DE LA FIBRA ÓPTICA MULTIMODO 73
FIGURA 38. LUZ EN EL INTERIOR DE LA FIBRA ÓPTICA MONOMODO 74
FIGURA 39. SISTEMAS HÍBRIDOS 75
FIGURA 40. UBICACIÓN GEOGRÁFICA DE LA ESPE- SANGOLQUÍ 77
FIGURA 41. RED ORGANIZACIONAL DE LA ESPE- SANGOLQUÍ 78
FIGURA 42. EDIFICIOS/BLOQUES ESPE- SANGOLQUÍ 78

FIGURA 43. ZONIFICACIÓN ESPE- SANGOLQUÍ 80
FIGURA 44. DISTRIBUCIÓN DE EDIFICACIONES ESPE- SANGOLQUÍ 83
FIGURA 45. ACCESO PRINCIPAL ESPE- SANGOLQUÍ 88
FIGURA 46. MEJORA DE PROCESOS 89
FIGURA 47. ÁRBOL DE PROBLEMAS ESPE-SANGOLQUÍ 90
FIGURA 48. PARQUEADEROS FRONTALES ESPE-SANGOLQUÍ 92
FIGURA 49. PARQUEADERO EDIFICIO ADMINISTRATIVO ESPE-SANGOLQUÍ 94
FIGURA 50. DESCRIPCIÓN GENERAL SISTEMA CCTV 96
FIGURA 51. ÁREAS DE INFLUENCIA DE LA ESPE PARA EL CCTV 97
FIGURA 52. CENTRO DE CONTROL CCTV - ESPE 98
FIGURA 53. CÁMARA CCTV INALÁMBRICA 99
FIGURA 54. ARREGLO ANTENAS SECTORIALES WIFI 99
FIGURA 55. DISTRIBUCIÓN CÁMARAS POR SECTORES EN EL CAMPUS ESPE 103
FIGURA 56. CÁMARA IP CCTV 104
FIGURA 57. ENLACES WIFI CÁMARAS POR SECTORES EN EL CAMPUS ESPE 104
FIGURA 58. : IPTV ENCODER DE 24 CANALES 105
FIGURA 59. ACCES POINT CCTV 106
FIGURA 60. ENLACES INALÁMBRICOS CON MARGEN DE SEGURIDAD 107
FIGURA 61. ANTENAS WIFI 109
FIGURA 62. ACCESO/SALIDA PRINCIPAL VEHICULAR ESPE 110
FIGURA 63. ACCESO/SALIDA PEATONAL ESPE 111
FIGURA 64. CONFIGURACIÓN CONTROL DE ACCESO VEHICULAR 114
FIGURA 65. ACCESO PEATONAL ESPE 115
FIGURA 66. ACCESO VEHICULAR Y PEATONAL ESPE 116
FIGURA 67. PUNTO PAGO PARQUEADERO 119
FIGURA 68. ESQUEMA TELEPEAJE ACCESO VEHICULAR 121
FIGURA 69. SOFTWARE RECONOCIMIENTO DE MATRICULA VEHICULAR 121
FIGURA 70. FLUJO GRAMA DE RECONOCIMIENTO DE MATRÍCULA VEHICULAR EN PC 123
FIGURA 71. INTEGRACIÓN CCTV Y ACCESO VEHICULAR/PEATONAL 124
FIGURA 72. INTEGRACIÓN DE SISTEMAS CCTV 125
FIGURA 73. RACK PRINCIPAL 125
FIGURA 74. RACK PRINCIPAL 126
FIGURA 75. : RESPALDO DE ENERGÍA UPS PARA CCTV 128

RESUMEN

La Escuela Politécnica del Ejército-ESPE, ha emprendido un plan ampliación de obras de sus instalaciones, aulas y laboratorios, debido la gran demanda de alumnos que acoge para la formación de profesionales de pregrado y postgrado. Debido a esto el tráfico peatonal y vehicular se ha incrementado de manera exponencial en estos últimos años. El proyecto de analiza y estudia la factibilidad de implementar de un CCTV, que permitirá tener un monitoreo y control del Campus Universitario en Sangolquí, durante las 24 horas del día. El ingreso/salida de personas y vehículos no es una tarea fácil de manejar solamente con el recurso humano. El estudio permite la ubicación e implementación de un sistema electrónico de control de accesos del Campus de la ESPE. El CCTV inalámbrico, cumplirá la función de controlar a través de las cámaras de video, el sector perimetral de la ESPE, así como también parqueaderos y entradas principales de este centro de educación superior. La tecnología de punta que se requiere en este proyecto, permitirá disponer de información rápida y confiable de los eventos que se susciten en el interior de la Universidad, logrando con esto coadyuvar a la seguridad integral de la institución y que será complementada con la respuesta humana.

PALABRAS CLAVE:

- **AMENAZA A LA SEGURIDAD**
- **IMPACTO TECNOLÓGICO**
- **RIESGO**
- **VULNERABILIDAD**
- **SISTEMA DE GESTIÓN DE SEGURIDAD INTEGRAL.**

ABSTRACT

The Polytechnic School of the Army-ESPE, has embarked on an expansion plan works facilities, classrooms and laboratories, because of the high demand for hosting students for training professionals and graduate. Because of this pedestrian and vehicular traffic it has increased exponentially in recent years. The project analyzes and studies the feasibility of implementing a CCTV, which will have a monitoring and control in Sangolquí Campus, 24 hours a day. The entry / exit of people and vehicles is not an easy task to manage the human resources only. The study allows the location and implementation of an electronic access control system Campus of the ESPE. The wireless CCTV, will act to control through video cameras, the perimeter ESPE sector, as well as parking and main entrances of this center of higher education. The technology that is required in this project will enable to have fast and reliable information about events that arise within the university, thus achieving contribute to the overall security of the institution and will be complemented with human response .

KEY WORDS:

- **MENACE TO SECURITY**
- **TECHNOLOGY IMPACT**
- **RISK**
- **VULNERABILITY**
- **INTEGRAL MANAGEMENT SYSTEM SECURITY**

GLOSARIO

Amenaza: es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Impacto: consecuencia de la materialización de una amenaza.

Riesgo: combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas

Vulnerabilidad: posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

Ataque: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

SGSI (Sistema de Gestión de la Seguridad Informática): Sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información.

SI (Seguridad Informática): Se denomina seguridad informática al conjunto de métodos y herramientas destinados a proteger la información y por ende

los sistemas informáticos ante cualquier amenaza, se trata de un proceso en el cual participan personas.

PDCA (Plan, Do, Check, Act): El círculo PDCA o también conocido como ciclo de Deming, es una estrategia de mejora continua de la calidad en cuatro pasos: Planificar, hacer, verificar y actuar.

PRÓLOGO

La Escuela Politécnica del Ejército-ESPE acorde a sus planes de seguridad y control de sus instalaciones, bienes (muebles e inmuebles), personal administrativo, profesores y estudiantes, pretende implementar sistemas modernos control y vigilancia, a través del monitoreo permanentemente de las diferentes instalaciones del Campus Universitario, satisfaciendo así sus necesidades y expectativas.

En la Escuela Politécnica del Ejército-ESPE, el bienestar y buen vivir de las personas que lo conforman, es el insumo más importante y la razón de ser para el accionar diario de la institución, por lo que permanentemente se realiza estudios y se ejecuta planes para un buen manejo de todos los procesos académicos y administrativos.

La exigencia académica, el bienestar y la seguridad de todos quienes conforman la comunidad universitaria, así como el respeto al medio ambiente son las prioridades, que dentro de un marco de principios y valores, se desarrollar una cultura de calidad institucional.

En el proyecto se realiza el análisis y estudio de factibilidad para implementar un sistema de CCTV para incrementar la seguridad de los diferentes grupos de personas que tiene la Escuela Politécnica del Ejército-ESPE, así como también el manejo mediante un control de acceso a ciertas áreas y edificios del campus, ingreso/salida de vehículos y personal, contempla este sistema la protección sobre la propiedad privada y el respeto interpersonal, el mismo que debe extenderse a proporcionar un servicio eficiente y adecuado, a precio módico con responsabilidad legal.

JUSTIFICACIÓN

La Escuela Politécnica del Ejército-ESPE, está situada geográficamente en el cantón Rumiñahui, en la ciudad de Sangolquí y limita: al Norte con instalaciones de recreación (PetroEcuador), al Sur las fábricas de artículos militares (FAME), por el Este, la Av. El progreso, la urbanización La Colina y al Oeste se encuentra con la vía boulevard Santa Clara y propiedades privadas de Sangolquí.

La Escuela Politécnica del Ejército-ESPE, es un centro educativo de nivel superior con recursos tanto humano como materiales de cuantiosa valía económica y al estar ubicada en un sitio central de la ciudad, donde se genera el movimiento económico e industrial de Sangolquí, factores que provocan que exista movimiento continuo de personas por todo el Campus Universitario, lo que ha incrementado las actividades delictivas a la propiedad pública y privada, mismas que se suscitan tanto en el día como en la noche, detectándose falencias en lo que respecta a la seguridad integral de la Universidad, ya sea por la falta de cultura en este aspecto o por que no se haya aplicado medidas preventivas para disminuir estos actos delictivos.

Por lo anterior expuesto, es indispensable la implementación de medidas de seguridad electrónicas que permitan detectar y eliminar las actividades irregulares en el Campus Politécnico de la ESPE-Sangolquí.

IMPORTANCIA

El concepto seguridad significa disponer de herramientas preventivas y correctivas para proteger un bien o patrimonio personal, particular o institucional. De la existencia de un sistema de seguridad dependerá que dicha protección se cumpla al ciento por ciento. La ESPE dispone de un sinnúmero de elementos a ser protegidos como son: instalaciones, equipos de laboratorios, vehículos, personal, etc. Este estudio de factibilidad para la instalación de un sistema de seguridad perimetral constituye el primer paso para una posterior ejecución de su adjudicación e implementación como parte de un sistema Integrado.

Actualmente la ESPE ha adquirido un sistema integrado de control de seguridad para el edificio Administrativo. La protección en la Institución debe ser interna y externa, siendo de suma importancia la custodia de los bienes a través del monitoreo de áreas aledañas a los edificios, laboratorios y demás instalaciones que dispone la ESPE, por lo que se hace importante complementar con equipos modernos los sistemas ya instalados tanto en el edificio administrativo, biblioteca y residencia.

El control de accesos accionara paralelamente al CCTV. Esto permitirá tener un monitoreo del ingreso/salida vehicular y peatonal a nivel perimetral y de todo el Campus Politécnico.

ALCANCE DEL PROYECTO

El proyecto contempla el análisis y estudio de factibilidad de un sistema de CCTV, para el campus de la Escuela Politécnica del Ejercito E.S.P.E - Sangolquí), a nivel perimetral. Será necesario realizar y estudiar soluciones hibridas, es decir sistemas cableados e inalámbricos para su implementación y definir de manera óptima la ubicación de los equipos.

Respecto al control de accesos, el interés de su implementación es de prioridad para los sectores este y oeste del campus Politécnico, lo que permitirá a vehículos y personas ejercer sobre ellos el respectivo control y monitoreo, mediante un sistema de vallas, chip's integrados, sticker de identificación, etc. Con una mejor definición de las áreas de parqueo para optimizar la gestión y administración de la seguridad integral. Realizar un análisis del ingreso peatonal a nivel de accesos principales, es una de las tareas que se llevó a cabo en este proyecto.

Toda la información de seguridad recopilada por los diferentes entes de control, se concentrara en un cuarto de gestión, mediante un sistema robusto de comunicación e incorporando un software capaz de administrar y monitorear todos los equipos instalados.

Para el sistema de comunicación se analizó la mejor opción, involucrando un para ello el estudio de topologías, protocolos, tecnologías, accesos a los medios, arquitecturas, entre otros.

OBJETIVOS

General:

Establecer el análisis y estudio de factibilidad para la implementación de un sistema de circuito cerrado de televisión para el Campus Politécnico y un sistema de control de accesos perimetral de la Escuela Politécnica del Ejército (E.S.P.E. - Sangolquí).

Específicos:

- Realizar el levantamiento de información relativa a la infraestructura eléctrica, electrónica y de telecomunicaciones de las instalaciones.

- Analizar las necesidades de seguridad física dentro y fuera de las instalaciones.

- Realizar el estudio y análisis de factibilidad de un sistema de control de acceso y circuito cerrado de televisión (CCTV) para el campus Escuela Politécnica del Ejército (E.S.P.E. - Sangolquí).

- Realizar el análisis de las características técnicas de los equipos de los sistemas de control de acceso y circuito cerrado de televisión (CCTV).

- Realizar el presupuesto referencial y su costo beneficio.

CAPÍTULO 1

INTRODUCCIÓN

El concepto de una moderna automatización de un conjunto de instalaciones que conforman una organización, empresa o campus universitario, tiene ya algunos años de investigación y desarrollo, el avance vertiginoso de la ciencia en general y en particular de la electrónica y la informática, nos permiten actualmente contar con nuevas herramientas que facilitan y complementan la labor del ser humano, el software y hardware de los sistemas se han ido actualizando paralelamente al avance tecnológico, al punto que podemos hablar de sistemas automatizados e inteligentes.

La más alta tecnología es utilizada en instalaciones convirtiéndolas en inteligentes, que ha base de una estación central (generalmente un servidor), controla básicamente todos los sistemas instalados, para proporcionar los beneficios que el cliente desea.

Dependiendo de la calidad y el número de los servicios ofrecidos tendrá una determinada capacidad. En la actualidad, existen variedad de sistemas tanto en el área de automatización de procesos como en la transmisión de señales por diferentes medios, por lo tanto hay gran cantidad de empresas dedicadas a esta actividad, tanto en el ámbito industrial como en el doméstico.

1.1 Historia de los Sistemas de CCTV y Control de Accesos.

Figura 1 Sistema CCTV

En los últimos años, las diferentes ramas de la tecnología han tenido un gran auge y su capacidad de aplicación ha crecido considerablemente.

Si integramos todos estos componentes y los servicios que pueden ofrecernos, puede traer grandes ventajas para sus usuarios. Pero si a esto le agregamos un control central para que manipule todo, libera a los usuarios de realizar tareas como prender y apagar la iluminación, controlar la temperatura del aire acondicionado, entre otros y al ocurrir esto, éstos pueden dedicar más tiempo y esfuerzo a realizar sus actividades cotidianas, contando con mayor confort y seguridad.

Actualmente los edificios e instalaciones de una organización incorporan sistemas de información, ofreciendo servicios avanzados de la actividad y de las telecomunicaciones, con control automatizado, monitorización, gestión y mantenimiento de los distintos subsistemas o servicios del edificio de forma óptima e integrada; local y remotamente, diseñados con suficiente

flexibilidad como para que sea sencilla y económicamente rentable la implementación de futuros sistemas.

Un circuito cerrado de televisión CCTV, es el uso de cámaras de video para transmitir una señal a un lugar específico, en un conjunto limitado de monitores. Se diferencia de la televisión en el que la señal no se transmite abiertamente, aunque se puede emplear punto a punto, punto a multipunto o malla de enlaces inalámbricos. Aunque casi todas las cámaras de video se ajustan a esta definición, el término se aplica con mayor frecuencia a los utilizados para la vigilancia en las zonas que pueden necesitar supervisión, tales como bancos, casinos, aeropuertos, instalaciones militares y tiendas de conveniencia. Videotelefonía rara vez se llamó "CCTV", pero el uso del vídeo en la educación a distancia es una herramienta importante.

En las plantas industriales, equipos de circuito cerrado de televisión puede ser utilizado para observar las partes de un proceso desde una sala de control central, por ejemplo, cuando el medio ambiente no es adecuado para los seres humanos. Pueden funcionar de forma continua o sólo cuando sea necesario para monitorear un evento en particular. Una forma más avanzada de un CCTV es utilizando grabadoras de vídeo digital, ofrece grabación para posiblemente muchos años, con una variedad de opciones de calidad y rendimiento y funciones adicionales.

Las cámaras de circuito cerrado de televisión basados en IP descentralizadas, algunas equipadas con sensores, resolución en megapíxeles, grabación de apoyo directamente a los dispositivos de almacenamiento conectados a la red, flash interna para completamente stand-alone.

La vigilancia de circuito cerrado de televisión es particularmente común en muchos lugares del mundo, incluyendo el Reino Unido, donde se dice que hay más cámaras por persona que en cualquier otro país en el mundo. Allí y en otros lugares, su uso creciente ha desencadenado un debate sobre la seguridad frente a la privacidad.

La expresión CCTV es una abreviación de “Circuito Cerrado de Televisión”, que significa textualmente video a distancia en una red cerrada. La expresión existe desde hace mucho tiempo, pero cuando se usa la expresión hoy en día se habla normalmente de una red que ya NO es "cerrado", significando que es una red de visión remota más abierta, con acceso vía redes locales o globales como Internet.

Figura 2 Cámara IP

La historia de CCTV empezó con cámaras cableadas a un monitor remoto, cuyo objetivo era limitado para poder ver un área desde un sitio alejado. La ventaja era impresionante, poder monitorear varias áreas desde un sitio, mejorando la seguridad y reduciendo personal que antes era necesario para vigilar.

El primer sistema de circuito cerrado de televisión fue instalado por Siemens AG en el banco de pruebas VII en Peenemnde, Alemania, en 1942, para observar el lanzamiento de cohetes V-2. El señalado ingeniero alemán Walter Bruch fue responsable del diseño tecnológico y la instalación del sistema.

En los EE.UU. el primer sistema de circuito cerrado de televisión comercial llegó a estar disponible en 1949, llamado Vericon. Muy poco se sabe sobre Vericon salvo que en el anuncio de que no exige un permiso del gobierno.

La historia de circuito cerrado de televisión en los Estados Unidos varía de la del Reino Unido. Una de sus primeras apariciones fue en 1973 en Times Square en la ciudad de Nueva York. No obstante, en 1980 comenzó a extenderse por todo el país dirigido específicamente a las zonas más peligrosas. Fue visto como una manera más barata para disuadir a la delincuencia en comparación con el aumento del tamaño de los departamentos de policía. Algunas empresas y sobre todo las que eran propensas al robo, empezaron a utilizar la video vigilancia.

Desde mediados de la década de 1990 se instalan un número cada vez mayor de cámaras en diferentes espacios públicos, incluidos los proyectos de viviendas, escuelas, edificios públicos y privados. Tras los ataques del 11 de septiembre, la utilización de la video vigilancia se ha convertido en algo común.

El CCTV llegó a ser muy común en bancos y tiendas para disuadir a los ladrones, mediante el registro de evidencia de actividad criminal, Su uso se popularizado en las últimas décadas, sobre todo con los temores de delitos que crecieron en los años 1990 y 2000, el uso en los espacios públicos de las cámaras de vigilancia ha tenido mucho éxito en todo el mundo.

1.2 Evolución de los Sistemas de Seguridad

Los sistemas de vigilancia por video se originaron entre los años 50s., y en los70s, empezaron siendo 100% sistemas analógicos y paulatinamente fueron digitalizándose. Los sistemas han avanzado mucho desde la aparición de las primeras cámaras analógicas con tubo conectadas a VCR (video cassette recorder).

Figura 3 CCTV Analógico

Hoy en día, los sistemas de vigilancia utilizan cámaras y servidores de PC para la grabación de video en un sistema completamente digitalizado. No obstante, entre los sistemas analógicos y los digitales existen diversas soluciones que son parcialmente digitales. Los sistemas de seguridad han venido evolucionando conforme las exigencias de los usuarios para solucionar sus problemas a la brevedad posible, con eficiencia y falla en un mínimo, y al desarrollo de nuevas tecnologías. Los sistemas se dividen en generaciones para poder clasificar su operatividad, esto garantiza al

usuario la confiablidad de que se cumplirán sus requerimientos con las últimas novedades tecnológicas.

Existe una gran variedad de sistemas de seguridad, donde se puede encontrar desde sencillos dispositivos en una red de seguridad poco compleja implementados para hogares, hasta edificios inteligentes con dispositivos capaces de tomar decisiones, estos están diseñados para cubrir las necesidades de empresas muy grandes y se desenvuelven en un ambiente distribuido.

Durante la historia de los sistemas de seguridad, han existido tres generaciones clasificadas por la complejidad que involucran. La primera generación se basaba en la implementación de un dispositivo capaz de dar aviso de cualquier actividad y un medio que lo controlará; es decir se trataba tan solo una alarma que emitía una señal sonora cuando existía una interrupción en el esquema que tenía determinado. El control muchas veces era manual ya que el usuario debía ingresar claves o parámetros para indicar que la situación que se iba a presentar era del todo normal. La segunda generación consistía en un medio con la capacidad de controlar eventos y podía tomar decisiones de acuerdo al escenario.

Esto permitió que el usuario deje de realizar eventos manuales, además disminuyó el número de falsas alarmas, pues los dispositivos eran capaces de interpretar una situación y definir si en realidad era una situación de alarma o simplemente una situación poco usual.

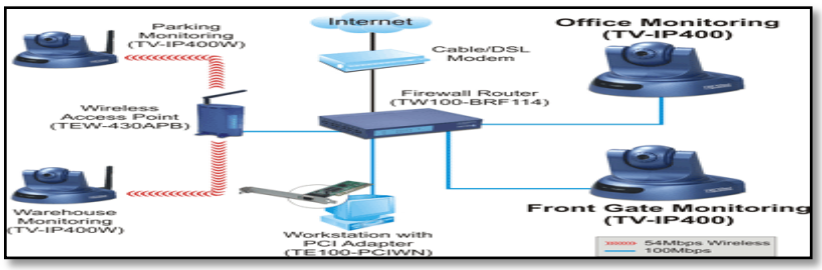

Figura 4 Evolución Del Sistema CCTV

Por último, en la tercera generación se implementaron medios para poder monitorear todos los acontecimientos que se realicen en un lugar, sin que el cliente tenga que estar presente en el sitio. Dándole más tiempo al usuario para que realice otras actividades y pueda estar revisando la situación en que se encuentra la empresa o su hogar.

Un sistema capaz de monitorear actividades, también puede llevar un registro de los eventos realizados durante un periodo de tiempo, permitiendo definir situaciones de riesgo o determinar ciertas acciones que mejoren el desempeño del sistema.

1.3 Regulaciones para la Utilización de Videocámaras para Video Vigilancia en Lugares Públicos en Ecuador

Figura 5 Ley Orgánica 15/1999 Protección De Datos

La implementación de video vigilancia tanto pública como privada ha venido ganando acogida a lo largo de los últimos años en Ecuador, de forma similar a lo ocurrido en Latinoamérica y otras partes del mundo.

Entre los proyectos más significativos y representativos al respecto dentro de entidades públicas o de gobierno se puede citar “Ojos de Águila”, sistema financiado por el Municipio del Distrito Metropolitano de Quito (MDMQ) que constituye el primer proyecto de video vigilancia operado con recursos públicos, implementado por el Consejo de Seguridad Ciudadana

de Cuenca (CSC) y el Sistema Ojos de Águila de la Ciudad de Guayaquil administrado por la corporación para la Seguridad Ciudadana de Guayaquil (CSCG).

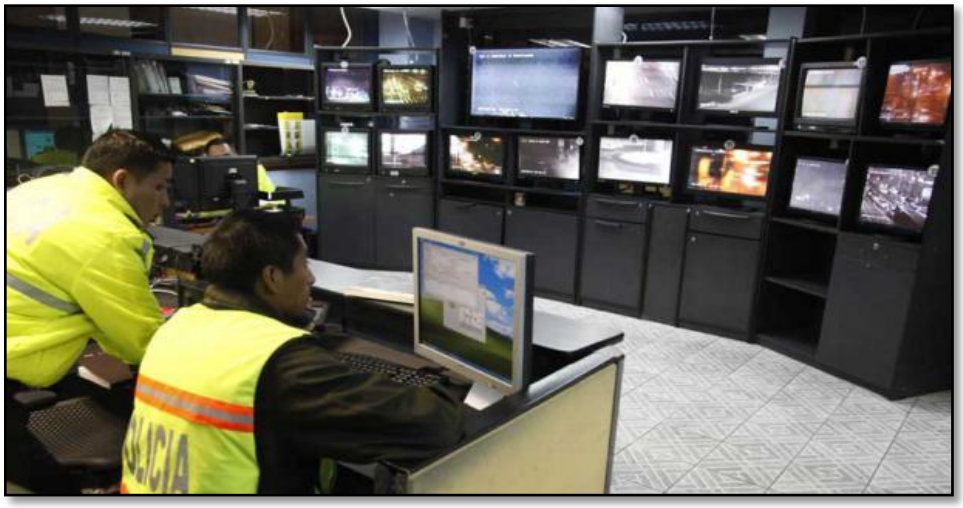

Figura 6 Ojos De Águila- Distrito Metropolitano De Quito

A su vez el hecho de contar con sistemas de video vigilancia pública, trae consigo la inquietud de si estos llegan a afectar las garantías que son precisas para que el ejercicio de los derechos y libertades reconocidos en la Constitución sea máximo y no pueda verse perturbado con un exceso de celo en la defensa de la seguridad pública.

Es decir tomar en cuenta la inviolabilidad de imagen y video que como derecho corresponde a todo ciudadano. Pese a las cualidades positivas que puede presentar la video vigilancia en términos de seguridad pública, también puede convertirse en una invasión a los derechos de privacidad y al libre ejercicio de las libertades.

Debido a esto, en correspondencia con el incremento de los sistemas públicos de video vigilancia algunos gobiernos han trabajado en el hecho de regular o regir el proceso y tratamiento de la información obtenida de estos medios y su posible utilización dentro de diferentes instancias.

Ampara un reglamento de desarrollo y ejecución de las videocámaras de manera que éstas sean utilizadas para los fines específicos de seguridad y no transgredan los límites de la privacidad. Esto incluye el hecho de consideraciones respecto a la ubicación de las cámaras de forma tal que las mismas permitan únicamente plasmar imágenes de vías públicas, limitando las zonas de privacidad establecidas, por ejemplo debe considerarse el no incurrir en visibilidad dentro de áreas o departamentos residenciales o similares que sean privados.

De este contexto planteado queda pues en evidencia que los sistemas de video vigilancia deben operar enmarcados dentro de leyes o reglamentos que regulen su uso y el tratamiento adecuado de la información captada.

En Ecuador no existe hasta el momento un Reglamento o ley que se encargue directamente de los sistemas de video vigilancia, existen algunas consideraciones básicas en donde se deja en claro la inviolabilidad de la imagen y voz, pero la tendencia en muchos de los casos es aplicar normativas de otros países entre ellas de las más reconocidas la Española.

A su vez también, los organismos suelen contar con reglamentos internos que permiten tener las consideraciones pertinentes del caso.

Así la Central Metropolitana de Atención Ciudadana (CMAC), no está regida actualmente (2008) bajo un reglamento ni una normativa sobre el uso de cámaras en espacios públicos y el uso/difusión de la información captada por las cámaras, tiene internamente, el Reglamento Orgánico Funcional de la CMAC que permite indicarles a los operadores hasta dónde se puede llegar y cómo manejar el monitoreo. Sin embargo, es algo que se debe poner en el tapete tomando en cuenta muchas circunstancias: la privacidad de las personas y la privacidad de sus dominios si es que es el caso.

1.4 Control de Accesos

Un control de accesos es un dispositivo que tiene por objeto impedir el libre acceso del público en general a diversas áreas que denominaremos protegidas. Por lo tanto lo primero que se debe identificar, para justificar la instalación de un control de accesos, es la existencia de elementos que se desean proteger. En una empresa o comercio estos elementos a proteger pueden ser fácilmente identificables, como las zonas donde se manipula dinero, donde se guardan los registros del personal y planos de sus productos (propiedad intelectual), entre otras, y algunas no tan obvias, como los sectores del proceso productivo con técnicas de fabricación consideradas únicas o propias.

En nuestro país el control de accesos comenzó como tal con los proveedores internacionales tradicionales de equipos de seguridad. En esa época todas las marcas eran básicamente incompatibles, incluyendo elementos comunes como las tarjetas magnéticas, que eran

personalizadas con códigos especiales de cada fabricante y que hacían que dejaran de cumplir con la norma ABA (American Banking Asociation).

Figura 7 Laboratorios – Zonas Protegidas

Esto no fue privativo de los controles de accesos, sino que las demás áreas de la seguridad hicieron más o menos lo mismo. Originalmente se usaron con frecuencia los teclados PIN, los cuales fueron paulatinamente reemplazados por los sistemas con tarjetas magnéticas y de código de barras. En la década del ‘90, la proximidad se hizo presente y en pocos años se estableció como estándar. En los últimos tiempos es notable de ver como todos los fabricantes del mercado de seguridad están ofreciendo soluciones integradas. Hoy el control de accesos ofrece un número de funcionalidades típicas de otras áreas de la seguridad electrónica y la domótica. Así es que permiten integrar funciones de alarmas, control básico (manejo de iluminación, etc.) y circuito cerrado de televisión (CCTV).

Analizando el mercado de control de accesos desde el punto de las aplicaciones pueden diferenciarse cuatro segmentos:

a- Residencial.

b- Comercial e industrial de pequeño y mediano porte.

c- Empresas corporativas y Gobierno.

d- Áreas aún no exploradas en nuestro mercado.

1.5 Control de Acceso Vehicular

Los sistemas de control de accesos vehicular se implementan para tener el control de los automotores que circulan por un espacio público o privado, asegurando el paso a los permitidos y restringiendo a aquellos que no estén autorizados. Al integrar un sistema de control de accesos vehicular, podemos tener la vigilancia integral, tanto de los residentes como de los visitantes.

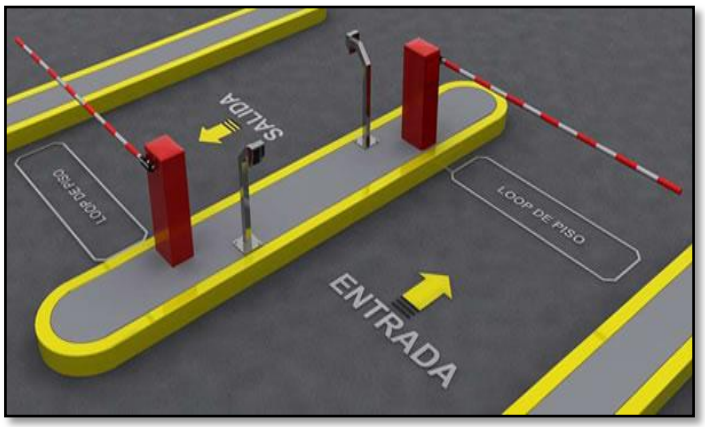

Figura 8 Sistema Electromecánico De Vallas

La automatización electromecánica para sistemas de parking y barreras de estacionamiento de medianas y grandes dimensiones, son soluciones potentes y versátiles que representa al máximo la fiabilidad y la tecnología de los mejores controles de acceso vehicular del mundo. Existen sistemas para las exigencias más complejas, tales como el uso intensivo, típico de las aplicaciones en las instalaciones comunitarias o industriales.

1.5.1 Beneficios y Ventajas

Todos los sistemas electromecánicos configurados para integrar una solución completa y robusta mediante un sistema de control de

accesos que satisface cualquier tipo de exigencia, permiten obtener las siguientes ventajas:

- Ahorro en personal extra dedicado a la vigilancia y control de acceso vehicular.
- Mayor seguridad con registros de entradas y salidas, horarios, grupos de acceso, zonas permitidas.
- Base de datos con toda la información necesaria: placas, descripción del vehículo, propietario, datos de contacto y todo lo que se considere necesario para un correcto control de acceso vehicular.
- Ingreso de automóviles de forma controlada y organizada.
- Sistema automatizado mejorando el acceso vehicular.
- Reconocimiento de placas para aplicaciones de avanzadas.
- Asociación de las placas con la identificación del conductor para mayor seguridad.
- Reconocimiento de TAGs RFID para aplicaciones manos libres.
- Alertas en caso de un intento de acceso sin autorización.

- Integración con todos los sistemas de seguridad para una gestión centralizada.
- Conexión e integración con la red IP para monitoreo desde diferentes puntos.

CAPITULO 2

SISTEMA CCTV Y CONTROL DE ACCESOS

2.1 Conceptos Básicos De Un Sistema Cctv Y Control De Accesos

2.1.1 Sistema CCTV

Que en sus siglas en inglés "Closed Circuit Televisión Internet Protocol" es una tecnología de video vigilancia diseñada para supervisar una diversidad de ambientes y actividades todas ellas fusionadas en la red de datos y controladas mediante un software.

Se le denomina circuito cerrado, ya que, todos sus componentes están enlazados. Además, a diferencia de la televisión convencional, este es un sistema pensado para un número limitado de espectadores.

Las cámaras de seguridad se encuentran fijas en un lugar determinado cómo su ángulo de captación, el movimiento en el área que se encuentre, las cámaras que se utilizan pueden estar controladas remotamente desde una sala de control, donde se puede configurar su panorámica, enfoque, inclinación y zoom. A este tipo de cámaras se les llama PTZ.

Elementos de un sistema de CCTV IP, describe cada uno de sus dispositivos e incluye características de visión nocturna, operaciones asistidas por ordenador y detecta movimiento, que facilita al sistema ponerse en estado de alerta cuando detectan movimiento delante de las cámaras.

La claridad de las imágenes puede ser excelente, se puede transformar de niveles oscuros a claros. Todas estas cualidades hacen que el uso del CCTV IP haya crecido extraordinariamente en estos últimos años y sean de gran ayuda en la seguridad de las personas y de sus pertenencias.

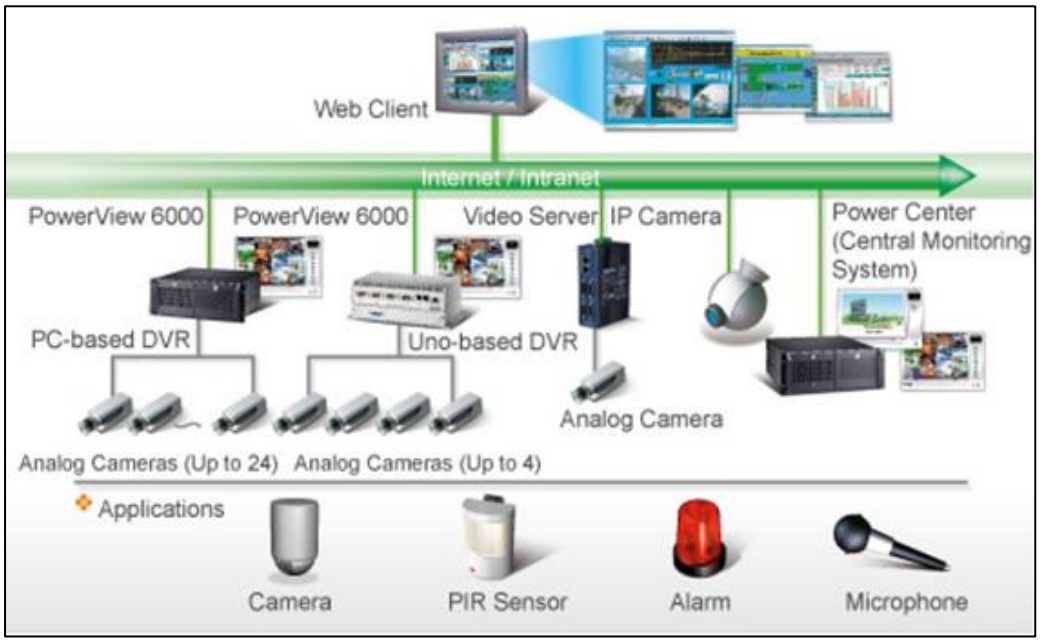

Figura 9 Sistema CCTV IP

2.1.2 Control de Accesos

Un sistema de control de acceso es aquel que junto al sistema de CCTV IP forman parte de un sistema integrado de seguridad en una empresa, los mismos que dependiendo de las exigencias del cliente que van de la mano con su precio.

Hoy en día un sistema de control de accesos es muy indispensable en una empresa, obteniendo así un control de entrada y salida de los empleados, registro de actividades y de control de aéreas restringidas donde solo personal autorizado puede ingresar.

2.2 Estructura de los Sistemas CCTV y Control de Accesos

2.2.1 Componentes de un CCTV IP

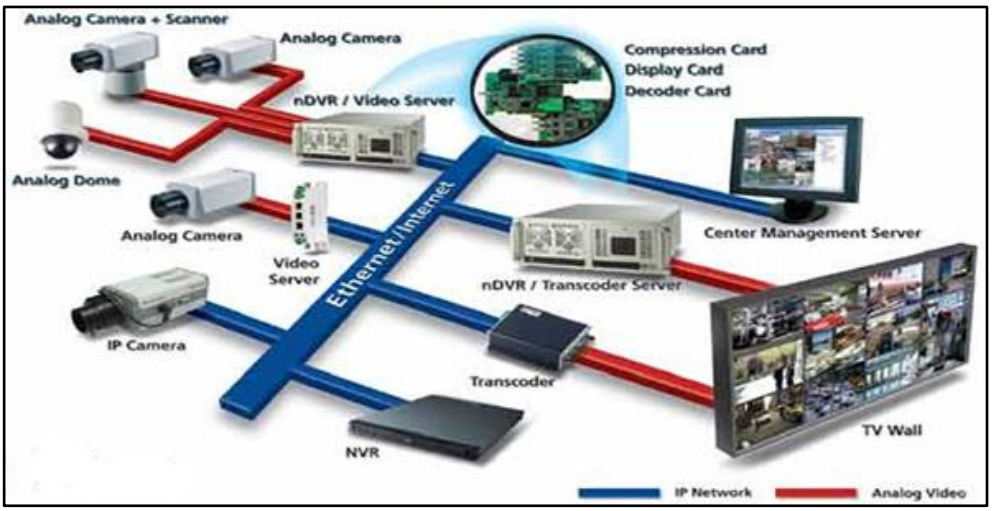

Figura 10 Estructura Sistema CCTV IP

- RED DE DATOS.

La red de datos está conformada por todos los elementos pasivos y activos, que forman parte del sistema de cableado estructurado.

- CÁMARAS SCANNER

Son dispositivos que ayudan en la seguridad de la empresa brindando mayor seguridad y confianza en su negocio al estar todo grabado y guardado en el ordenador.

Las cámaras al igual que los scanner tienen diferentes características, dependiendo de ello su precio puede ser bajo o elevado según las exigencias del cliente.

- DVR (DIGITAL VIDEO RECORDER) de 8, 16 ó 32 CÁMARAS.

El DVR es un grabador de video digital que cubre dos funciones básicas:

1) Multiplexor: que es mostrar hasta 32 cámaras en una sola pantalla.
2) Grabador: que es capturar y grabar imágenes dependiendo de su capacidad de almacenamiento.

- MONITOR

Para el monitoreo de las cámaras de vigilancia es indispensable un monitor desde 22' pulgadas, ya que se recomienda que sea de acuerdo al número de cámaras a ser instaladas en el CCTV IP.

- TRANSCODER.

Es dispositivo que convierte una forma de video codificado en otro.

- NDVR (NETWORK DIGITAL VIDEO RECORDER) SERVER TRANSCODER.

Un NDVR es un grabador de video digital de red que permite convertir el formato de video codificándolo a otro de las diferentes cámaras del CCTV IP en red.

- CUARTO DE CONTROL Y MONITOREO

Es el lugar donde se gestiona toda la información de seguridad. Permitiendo administrar y controlar de manera integral a la empresa o institución.

2.2.2 Componentes de un Control de Acceso

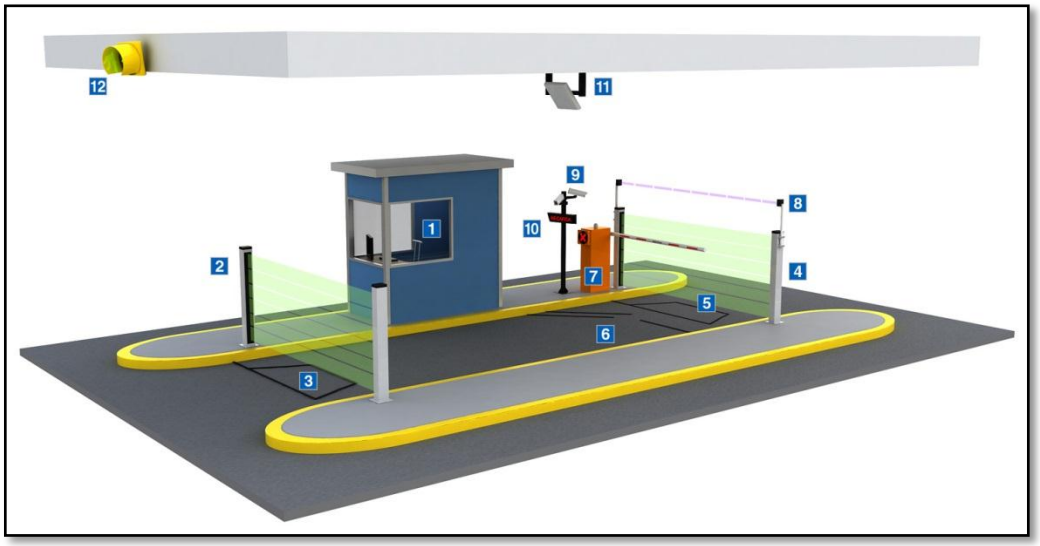

Figura 11 Control De Acceso Vehicular

1) PC de vía y periféricos

2) Cortina óptica de entrada*

3) Loop de entrada*

4) Cortina óptica de salida

5) Loop de salida

6) Contadores de ejes y ruedas duales

7) Barrera DAC (semáforo de paso + alarma visual + alarma sonora)

8) Detector de altura

9) Cámaras de video

10) Panel de usuarios

11) Antena RFID*

12) Semáforo de marquesina

*Elementos usados únicamente para las vías automáticas.

La vía es el corazón del sistema, con el cual se gestiona el cobro y se adquieren las variables primarias de control. Su arquitectura, extremadamente simple, asegura confiabilidad y estabilidad en el funcionamiento, así como muchas facilidades para el mantenimiento.

El enfoque de la esta novedosa concepción permite que una vía de peaje prácticamente se reduzca a sólo 3 grupos de elementos principales:

- PC de Vía y periféricos asociados
- Barrera DAC (5 funciones en 1)
- Elementos de campo

- INFRAESTRUCTURA INFORMÁTICA

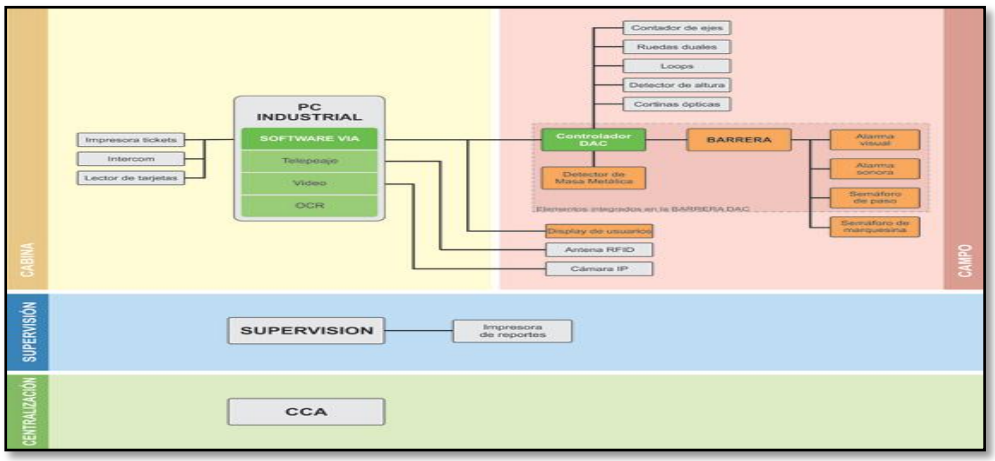

Figura 12 Software De Gestión

Consiste en una PC con un sistema operativo robusto, que integra una red Ethernet, con vinculación por cable o fibra óptica y donde se ejecuta la lógica de operación. A ella se conectan mediante puertos serie los demás componentes del sistema, como ser:

- Controlador de entradas/salidas de Campo basado en PLC
- Display de usuario

- Impresora de recibos
- Interfase para Telepeaje

El sistema incluye opcionalmente una placa para captura y digitalización de imágenes, y un software de reconocimiento automático de patentes, necesario cuando el sistema requiere control de Multipasaje.

- SISTEMA DE IDENTIFICACIÓN

Es un lector que transmite los datos identificativos al software que entonces permite o deniega el acceso.

2.3 Aplicaciones Del Cctv Y Control De Accesos

2.3.1 Aplicaciones para el CCTV

Probablemente el uso más conocido del CCTV está en los sistemas de vigilancia y seguridad, así como en aplicaciones tales como establecimientos comerciales, bancos, oficinas gubernamentales, edificios públicos, aeropuertos, etc. En realidad las aplicaciones son casi ilimitadas.

Se enlistan algunos ejemplos:

- Sondas médicas con micro cámaras introducidas en el cuerpo humano.
- Monitoreo del tráfico en un puente.
- Monitoreo de procesos industriales como Fundiciones, Panaderías,
- Ensamble manual o automático.

- Vigilancia en condiciones de absoluta oscuridad, utilizando luz infrarroja.
- Vigilancia en vehículos de transporte público.
- Vigilancia en áreas claves, en negocios, tiendas, hoteles, casinos, aeropuertos.
- Vigilancia del comportamiento de empleados.
- Vigilancia de los niños en el hogar, en la escuela, parques, guarderías.
- Vigilancia de estacionamientos, incluyendo las placas del vehículo.
- Vigilancia de puntos de revisión, de vehículos o de personas.
- Análisis facial para identificación de criminales en áreas públicas.

Lógicamente, en casi todos los casos el CCTV tiene que estar acompañado de la grabación o respaldo de los eventos que se vigila, con el objeto de obtener evidencia de todos los movimientos importantes y además el minimizar la vigilancia humana de los monitores.

2.3.2 Aplicaciones para el Control de Accesos

N4S Parking es una solución RFID de largo alcance que se puede integrar perfectamente con los sistemas de control de estacionamiento para que el proceso de estacionamiento de vehículos sea "más libre", "eficaz y

automático. Como N4S Parking puede detectar las etiquetas adheridas al parabrisas de vehículos autorizados con anticipación a la distancia, los conductores no tienen que bajar la ventanilla ni dejar su vehículo.

La operación de manos libres no sólo hace que el proceso de estacionamiento sea mucho más simple y más rápido, sino que mejora el

flujo y la seguridad, cuando se integra con los sistemas de gestión de estacionamiento, N4S Parking RFID de largo alcance.

Se puede utilizar para registrar y rastrear la entrada y salida de los vehículos, lo que permite la facilidad de estacionamiento para gestionar automáticamente las tarifas de estacionamiento y garantizar la seguridad de las instalaciones como:

- Conjuntos Residenciales
- Edificios de Oficinas
- Estacionamientos Comerciales
- Complejos Industriales

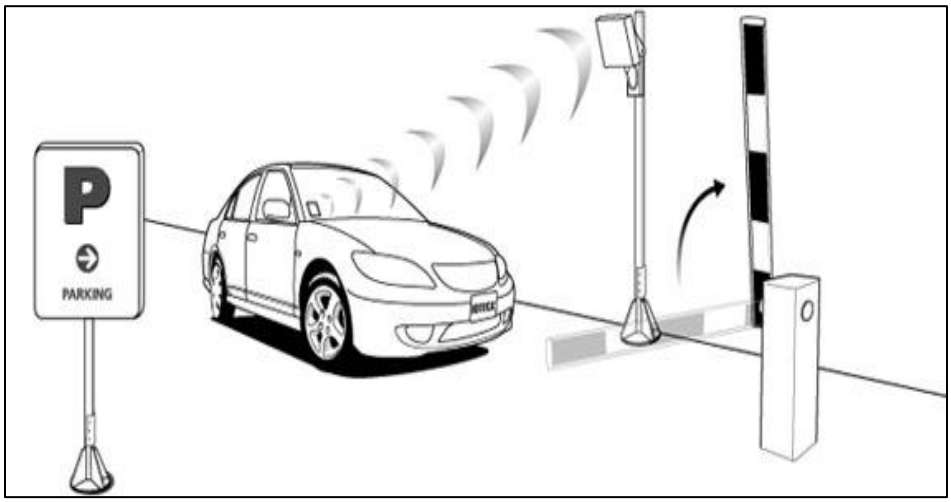

FIGURA 13 N4S Parking Es Una Solución Rfid

Largo Alcance y Bajos Costos – Implementando la tecnología RFID en sistemas de parqueaderos bajado sustancialmente los costos en compra de chips, controles o tarjetas de proximidad, permitiendo lecturas manos libres de hasta 20 metros de distancia.

Agilidad y Eficiencia – Con la tecnología RFID se disminuye sustancialmente el tiempo de lectura y respuesta del sistema permitiendo la

apertura de puertas en tiempos record, el sistema ofrece exactitud del 99.9% en la lectura de TAGS

Seguridad - El sistema permite solo la entrada de TAGS registrados, haciendo una verificación en milisegundos contra la base de datos, adicionalmente se pueden se puede combinar con verificación de activos permitiendo revisar si se está retirando de forma indebida un activo del lugar.

Localización - El sistema permite la localización de vehículos dentro del parqueadero permitiendo de esta forma con una acción simple determinar donde se encuentra un vehículo en determinado momento.

2.4 Conceptos De Redes

2.4.1 Modelo de Comunicación

Todo sistema de seguridad electrónica para poder trasmitir las imágenes y datos entre los dispositivos de control, almacenamiento y centro de monitoreo, es necesario un proceso que involucra la interconexión a servidores, teclados, estaciones de control, a esto se lo define como una red de comunicaciones que no es más que un conjunto de dispositivos con capacidad de interconexión.

2.4.2 Concepto de Red

Una red de datos es un conjunto de nodos, terminales y protocolos, que interconectados entre sí a través de medios físicos y/o lógicos, los mismos que se pueden comunicar para compartir recursos e información.

2.4.3 Topología de red

La topología de red define la estructura de una red. Existen dos tipos de topológica, la topología física es la que dispone de los cables o medios y la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos. Dentro de las topologías físicas más comúnmente usadas son:

- Topología de bus, esta usa un solo cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este backbone.

- Topología de anillo conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.
- Topología en estrella se conecta todos los cables con un punto central de concentración.
- Topología en estrella extendida se conecta estrellas individuales entre sí mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red.

- Topología jerárquica es equivalente a una estrella extendida. Pero en vez de conectar los hubs o switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.
- Topología de malla es implementada para proporcionar una mayor y mejor protección posible para así evitar una interrupción del servicio.
- La topología lógica de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast y transmisión de tokens.
- La topología broadcast simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. No existe una orden que las estaciones deban seguir para utilizar la red. Es por orden de llegada. Ethernet funciona así, tal como se explicará en el curso más adelante.
- La topología transmisión de tokens. La transmisión de tokens controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial. Cuando un host recibe el token, ese host puede enviar datos a través de la red.
- Si el host no tiene ningún dato para enviar, transmite el token al siguiente host y el proceso se vuelve a repetir. (CISCO-CCNA).

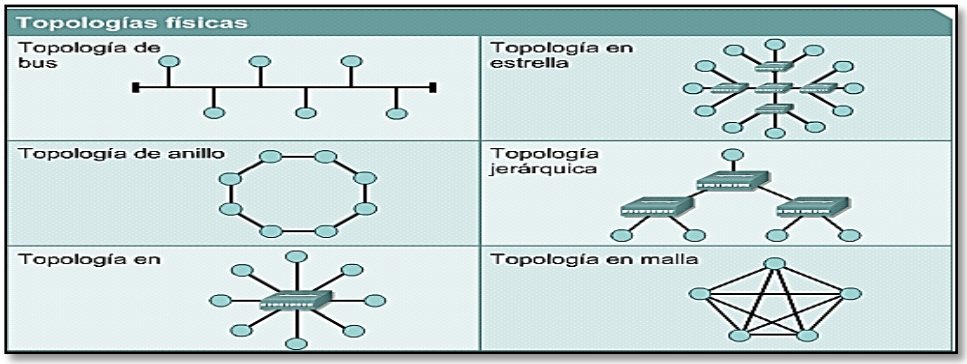

Figura 14 Tipos De Topologías Físicas

2.4.4 Tipos de redes

Las redes de clasifican según su extensión de área y por el tipo de acceso. Debido a la situación geográfica existen tres tipos de redes: LAN, WAN, MAN, y por la accesibilidad se clasifican en Redes Privadas y Públicas.

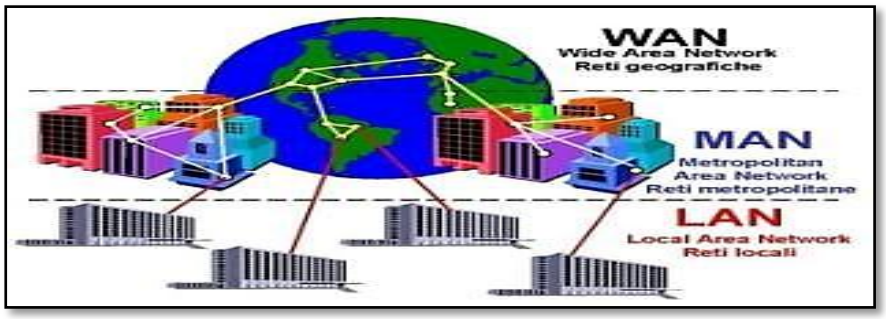

Figura 15 Tipos De Redes De Comunicación

2.4.5 Red de Área Local

Es un grupo de ordenadores conectados a un área local para comunicarse entre sí y compartir recursos, la información es enviada en forma de paquetes y cuya transmisión puede utilizar diversas tecnologías, además es una red privada ya que está ubicada en un área restringida, que

puede ser una empresa, colegio, u hogar. El concepto prevalece aun cuando se trata de varias redes conectadas entre sí, siempre y cuando se encuentren ubicadas dentro del mismo edificio o campo.

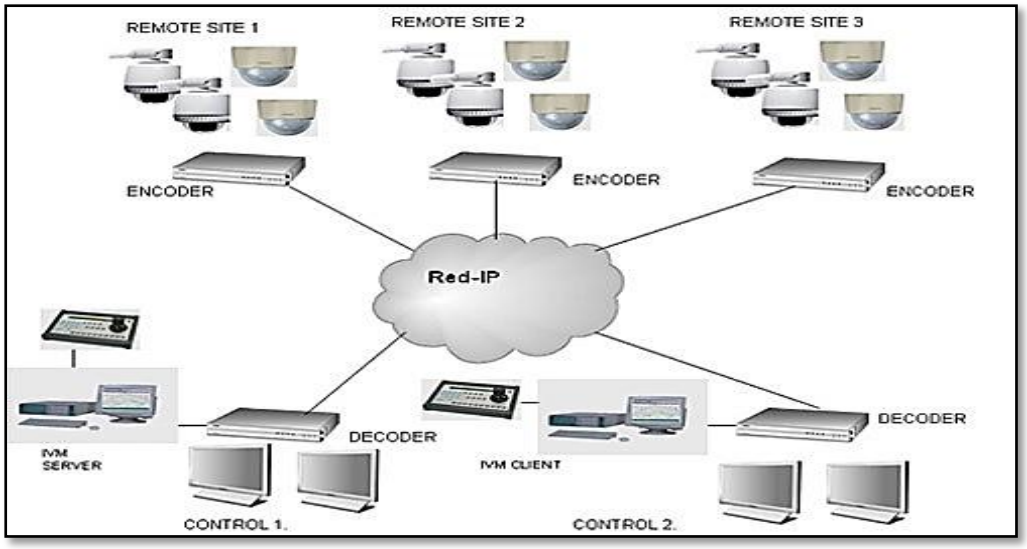

Figura 16 Esquema De Una Red Local

Este tipo de red utiliza la tecnología Ethernet y a su vez emplea una topología en estrella en la que los dispositivos están conectados unos con otros a través de un equipo de red activo como un conmutador. El número de dispositivos conectados a una LAN puede estar entre dos y varios miles. Utiliza como medio de transporte físico el cable par trenzado o la fibra óptica.

2.4.6 Red de Área Metropolitana

Se denomina así porque abarca un área metropolitana, como una ciudad, una red MAN consta de una o más redes LANs dentro de un área común. Se la conoce como red federalista y garantiza la comunicación a distancias más extensas y a menudo interconecta varias redes LAN".

2.4.7 Red de Área Extendida

"Una red WAN es una red que conecta una o varias redes LAN entre ciudades distinta del mismo país".

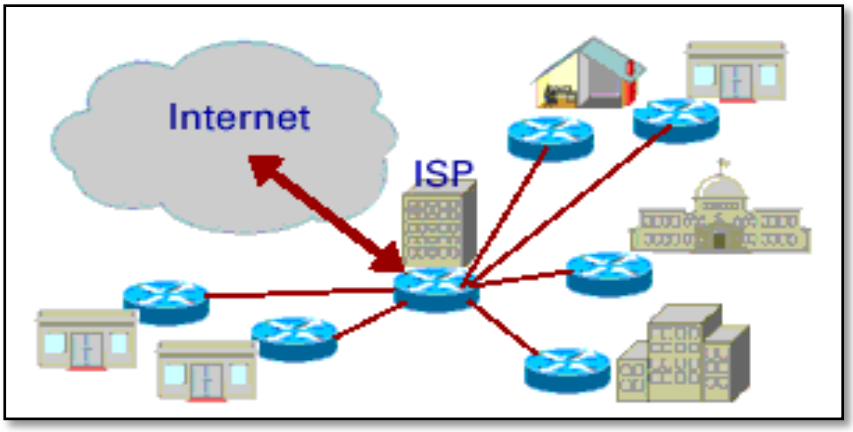

Figura 17 Esquema De Una Red De Área Metropolitana

"Una red WAN, abarca grandes distancias geográficas que van desde varios kilómetros hasta continentes enteros".

2.4.8 Redes Vlans

Una red VLAN es una tecnología que segmenta las redes de manera virtual, funcionalidad que admiten la mayoría de conmutadores de red. Esto se consigue dividiendo los usuarios de la red en grupos lógicos, donde sólo un grupo de usuarios específicos pueden intercambiar datos o acceder a determinados recursos en la red. Al momento de diseñar un sistema de vídeo en red, menudo se tiene el propósito de mantener la red sin contacto con otras redes, ya sea por la seguridad como por el rendimiento de la misma.

La primera opción sería construir una red independiente, los costos de adquisición, instalación y mantenimiento probablemente serían más elevados que si se utilizara una tecnología de red virtual de área local (VLAN). Si un sistema de vídeo en red es segmentado en una VLAN, sólo

los servidores ubicados en dicha LAN podrán acceder a las cámaras de red. El protocolo que se utiliza para configurar una red VLAN es IEEE 802.1Q, que etiqueta cada marco o paquete con bytes adicionales para indicar a qué red virtual pertenece.

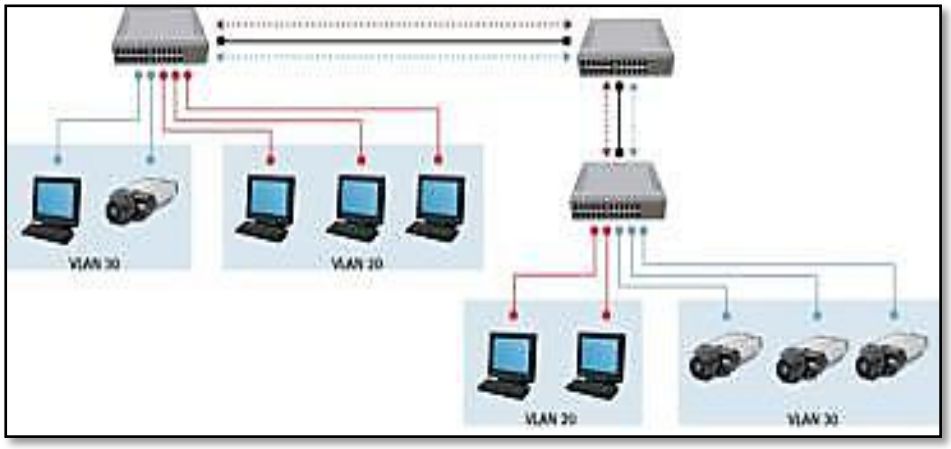

Figura 18 Esquema De Una Red Vlan

2.4.9 Tipos de Redes Ethernet

2.4.10 Red Fast Ethernet

Fast Ethernet es una red Ethernet que puede transferir datos a una velocidad de 100Mbit/s. Se puede usar cable de par trenzado o de fibra óptica. La mayoría de dispositivos que se conectan a una red, como un portátil o cámara de red, están equipados con una interfaz Ethernet 100BASE-TX/10BASE-T. El tipo de cable de par trenzado compatible con Fast Ethernet se denomina Cat-5.

2.4.11 Red Gigabit Ethernet

Gigabit Ethernet, también se puede usar un cable de par trenzado o de fibra óptica, proporcionando una velocidad de transferencia de datos de 1.000 Mbit/s (1 Gbit/s), este es el Cat-5e, en el que los cuatro pares de cables trenzados se utilizan para alcanzar la alta velocidad de transferencia de datos.

Para los sistemas de vídeo en red se recomienda Cat-5e u otras categorías de cable superiores. En la transmisión a larga distancia se puede

utilizar cable de fibra como el 1000BASE-SX y el 1000BASE-LX (hasta 550 m con fibras ópticas multimodo y hasta 5.000 m con fibras de modo único).

2.4.12 Red 10 Gigabit Ethernet

10 Gigabit Ethernet es la última generación, proporcionando una velocidad de transferencia de datos de 10 Gbit/s (10.000 Mbit/s) y puede ser utilizado con fibra óptica o cable de par trenzado. 10GBASELX4, 10GBASE

-ER y 10GBASE-SR, con la fibra óptica se puede utilizar para cubrir hasta distancias de 10.000 metros. Para este tipo de Ethernet se requiere un par trenzado de altísima calidad (Cat-6a o Cat-7).

2.5 Hardware De Redes

Es un término en inglés que hace referencia a cualquier componente físico tecnológico, que trabaja o interactúa de algún modo con la computadora. No sólo incluye elementos internos como el disco duro, CD-ROM, también hace referencia al cableado, circuitos, gabinete, incluso

elementos externos como la impresora, el mouse, el teclado, el monitor y demás periféricos.

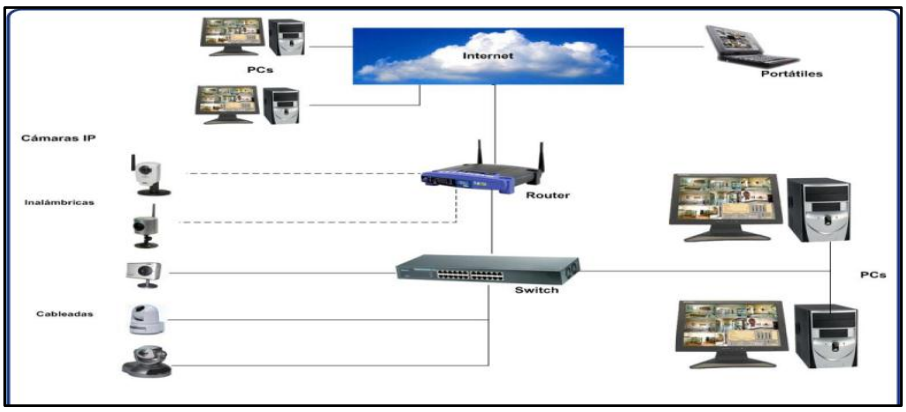

Figura 19 Esquema Hardware De Red De Cctv

2.6 Protocolos De Transmisión Datos, Voz Y Video

Los protocolos de datos es una serie de lineamientos de comunicación que sirven para administrar el intercambio ordenado de datos a través de una red y así mismo para suministrar la corrección de errores en la información incomprensible.

Es decir un protocolo es un conjunto de reglas y convenciones que rigen un aspecto particular de cómo los dispositivos de una red se comunican entre sí. Estos protocolos establecen el formato, la sincronización, la secuencia y control de errores en la comunicación de datos. Sin estos protocolos, los dispositivos electrónicos no puede comunicarse con otro computador.

Existen diversos tipos de protocolos que determinan el funcionamiento general de las redes, dentro de estos se destacan los Modelo OSI y TCP/IP, cada uno con una estructura de funcionamiento diferente.

2.6.1 Modelo OSI/ISO

El modelo OSI (Open Systems Interconnection) fue creado por la ISO y se encarga de la conexión entre sistemas abiertos, es decir, son

sistemas abiertos a la comunicación con otros sistemas. Los principios en los que basó su creación eran: una mayor definición de las funciones de cada capa, evitar agrupar funciones diferentes en la misma capa y una mayor simplificación en el funcionamiento del modelo en general.

El objetivo del modelo OSI es establecer estándares mundiales de diseños para los protocolos de datos con la finalidad de que todos los equipos sean compatibles al momento de comunicarse. Este modelo divide las funciones de red en siete capas diferenciadas:

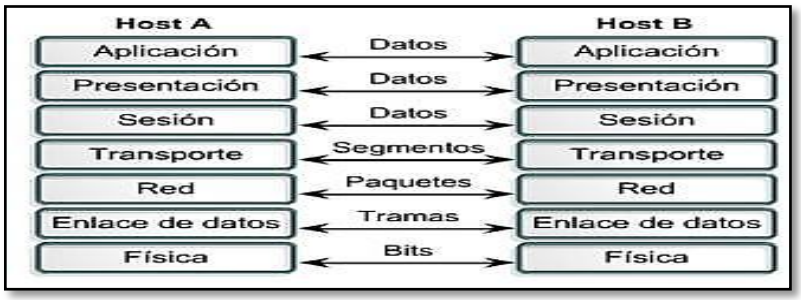

Figura 20 Capas Del Protocolo Modelo Osi

En el modelo OSI se explica cómo los paquetes de datos viajan a través de varias capas a otro dispositivo de una red, aun cuando el remitente y el destinatario poseen diferentes tipos de medios de red.

2.6.2 Modelo TCP/IP

Capa	*No.*	*Función*	*Propósito*
Física	1	Transmisión real de los datos a través de un medio físico	Lograr el intercambio de datos
De enlace de datos	2	Confiabilidad de la transmisión	Conseguir la transferencia útil de datos
De red	3	Enrutamiento de las conexiones a través de la red	Lograr la conexión entre terminales específicas de manera precisa y óptima
De transporte	4	Mantener la integridad entre extremos de los datos	Conseguir la comunicación completa y ordenada
De sesión	5	Controlar el diálogo entre dispositivos	Conseguir diálogos coherentes y con significado
De presentación	6	Codificación y formateo de datos	Conseguir la compatibilidad de sistemas y mayor eficiencia de los canales de comunicación
De aplicación	7	Proporcionar servicios	Actuar como administrador general de la red

Figura 21 Capas Del Protocolo Modelo TCP/IP

El modelo TCP/IP es el que actualmente se está implementando a nivel mundial, fue utilizado en primer lugar en ARPANET y es actualmente a nivel global en Internet y redes locales. Su nombre deriva de la unión de los nombres de los dos principales protocolos que lo conforman: TCP en la capa de transporte e IP en la capa de red, este protocolo se forma de cuatro capas que son: Enlace, Red, Transporte y Aplicación.

2.6.3 Internet

Internet es la implementación mejor conocida y la más grande de la interconexión de redes, es el enlace de miles de redes individuales de todo el mundo. Permite a sus usuarios, mediante una computadora o un terminal, conectarse hacia servidores localizados en instituciones educativas, proveedores comerciales y otras organizaciones para la obtención de información. Por otro lado internet no es una simple red de ordenadores, sino una red de redes, es decir, un conjunto de redes interconectadas a escala mundial con la particularidad de que cada una de ellas es independiente y autónoma.

Para poder enviar datos desde un dispositivo conectado a una LAN a otro dispositivo conectado a otra LAN se requiere de una vía de comunicación estándar, debido a esta necesidad se desarrolló un sistema de direcciones IP y protocolos basados en IP para comunicarse a través de Internet, que conforma un sistema global de redes informáticas interconectadas.

Las LAN también pueden utilizar direcciones y protocolos IP para comunicarse dentro de una red de área local, aunque el uso de las direcciones MAC es suficiente para la comunicación interna.

2.6.4 Direcciones IP

Las direcciones IP sirven para identificar a los dispositivos emisores y receptores. Actualmente existen dos versiones IP: IP versión 4 (IPv4) e IP versión 6 (IPv6). La principal diferencia entre las versiones es que la dirección IPv6 tiene una longitud mayor (128 bits), y una dirección IPv4 (32 bits de).

2.6.5 Dirección IPv4

Las direcciones IPv4 se agrupan en cuatro bloques, cada uno de los cuales se separa con un punto. Cada bloque representa un número entre 0 y 255, por ejemplo: 192.168.12.23.

En las direcciones IPv4 algunas se han reservado exclusivamente para uso privado. Estas direcciones IP privadas son 10.0.0.0 hasta 10.255.255.255, 172.16.0.0 hasta 172.31.255.255 y 192.168.0.0 hasta 192.168.255.255. Los dispositivos que quieran comunicarse a través de

Internet deben contar con su propia dirección IP pública, esta es una dirección asignada por un proveedor de servicios de Internet (ISP).

Un proveedor de servicio de internet puede asignar direcciones IP dinámicas, o direcciones estáticas. Para una cámara IP o codificador de video es necesaria la asignación de una dirección IP de manera automática con un DHCP (Protocolo de configuración dinámica de Host), o colocando de manera manual la IP estática que viene escrito en el producto.

El DHCP gestiona un conjunto de direcciones IP que puede asignar dinámicamente a un equipo de vídeo, se llama dirección IP dinámica porque puede cambiar de un día para otro.

2.6.6 Plataformas de Hardware para CCTV

Existen dos tipos de hardware para los sistema de gestión de video en red: una de servidor de PC formada por uno o más computadores que ejecuta un software de gestión para video y otro establecido en una grabadora de video en red (NVR), que es un hardware con software de gestión de video instalado.

2.6.7 Plataforma de servidor de PC

Este tipo de plataforma incluye servidores PC y unidades de almacenamiento que se pueden escoger directamente con la finalidad de obtener un rendimiento superior para el diseño específico del sistema. Una plataforma abierta con estas características facilita la opción de añadir funcionalidades al sistema, tales como almacenamiento incrementado o

externo, cortafuegos, protección contra virus y algoritmos de video inteligentes, en paralelo con un programa de software de gestión de video.

Además puede ampliarse, permitiendo añadir los productos de video en red sean necesarios. El hardware del sistema se puede ampliar o actualizar para satisfacer nuevas necesidades de rendimiento.

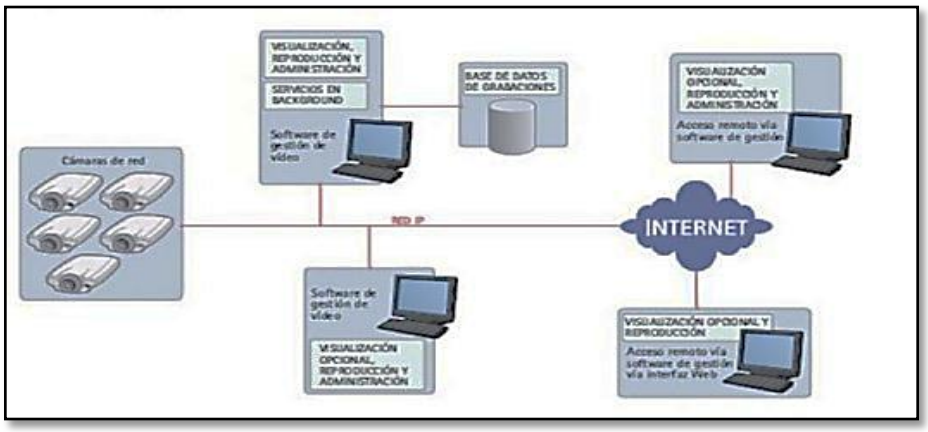

Figura 22: Arquitectura Centralizada de Video Basado en un Servidor

2.6.8 Plataforma NVR

Una plataforma NVR está diseñada para ofrecer un óptimo rendimiento para un conjunto de cámaras, esta plataforma es menos escalable que un sistema basado en servidor de PC, esta plataforma resulta más adecuada para sistemas más pequeños donde el número de cámaras se encuentra dentro de los límites de la capacidad de diseño de un NVR, un NVR es más fácil de instalar que un sistema basado plataforma de servidor de PC.

El hardware de NVR normalmente está diseñado específicamente para gestión de video (grabación, análisis y reproducción de video en

red) y generalmente no permite que ninguna otra aplicación se conecte a éste. El sistema operativo puede ser Windows, NIX/Linux o patentado.

Figura 23 Sistema De Cámara Con Plataforma NVR

2.6.9 Switch o Conmutador

Para conectar diversos dispositivos a una LAN se requiere un equipo de red, denominado conmutador de red o switch. Con un equipo de red se utiliza un cable de red convencional en vez de un cable cruzado.La función principal del switches es enviar los datos desde un dispositivo a otro en una misma red.

Este método es eficaz, puesto que los datos se pueden dirigir de un dispositivo al otro sin que ello afecte a otros dispositivos que utilicen la misma red.

Un conmutador de red registra las direcciones MAC (Media Access Control – Control de acceso al medio) de todos los dispositivos conectados. Cada dispositivo de red tiene una dirección MAC única, formada por una serie de números y letras implantada por el fabricante que se encuentra en la etiqueta del producto, cuando un conmutador recibe

datos, los remite sólo al puerto que está conectado a un dispositivo con la dirección MAC de destino adecuado.

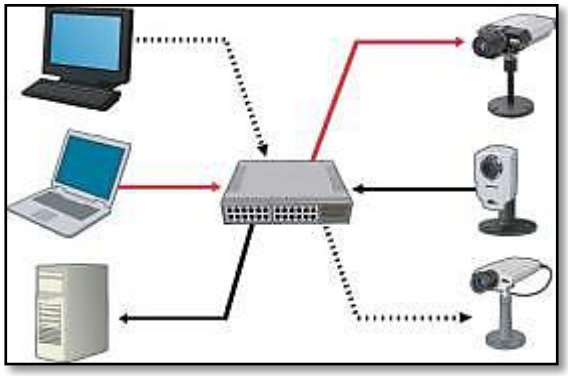

Figura 24 Sistema De Vigilancia Con Switch

2.6.10 Servidores o Codificadores de Video

Son dispositivos que permiten la integración de cámaras con tecnología análogas a un sistema con tecnología IP, es decir que permiten la migración de la tecnología coaxial de las cámaras análogas a la tecnología digital IP, permitiendo que el software de gestión de monitoreo pueda visualizar y controlar las cámaras análogas en un sistema digital IP.

Los servidores de video desempeñan un papel importante en los sistemas donde se deben mantener muchas cámaras análogas, ya que permite migrar de un sistema analógico a un sistema digital IP, de modo que los usuarios puedan beneficiarse de las ventajas de un sistema digital sin descartar los equipos analógicos existentes, como cámaras análogas y cable coaxial, estos se conecta a la cámara a través del cable coaxial y este convierte las señales analógicas en señales digitales que son enviadas a través de una red basada en IP, además el servidor permite transmitir eñales de control enviadas a las cámaras (movimientos, zoom, alarmas, etc.).

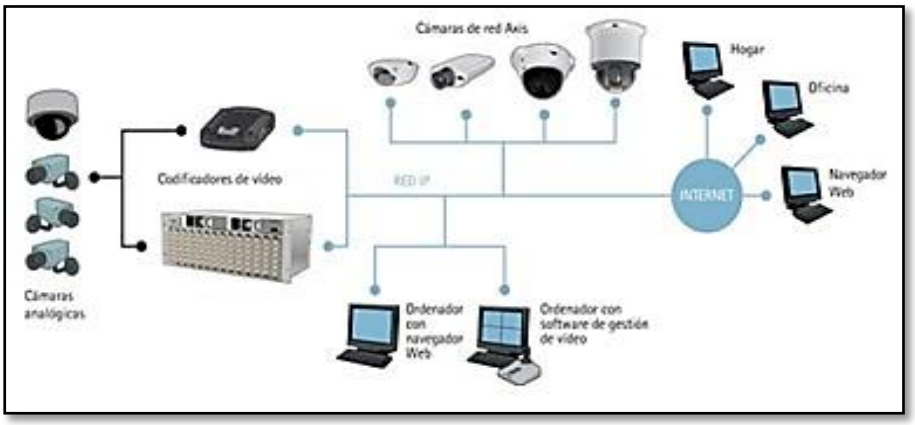

Figura 25 Sistema De Vigilancia Con Servidor De Video

Con los codificadores de vídeo se puede acceder desde otros lugares remotamente y controlar a través de una red IP cualquier cámara de vídeo analógica, como domos fijas, interiores o exteriores, cámaras con

movimiento horizontal, vertical y zoom, y cámaras especializadas de alta sensibilidad térmica o microscópicas.

2.6.11 Componentes y Consideraciones del Codificador de Vídeo

Los codificadores de vídeo ofrecen muchas de las funciones disponibles en las cámaras de red. A continuación se detalla los componentes principales de un codificado de video:

Entrada de vídeo análoga para conectar una cámara analógica mediante un cable coaxial.

Procesador para ejecutar el sistema operativo, las funciones de red y seguridad del codificador de vídeo para codificar el vídeo analógico

con varios formatos de compresión y para el análisis de vídeo. Estos disponen de detección automática para reconocimiento automático si una señal de vídeo analógica es NTSC o PAL estándar.

Memoria para almacenar el firmware (programa informático) utilizando memoria Flash, así como búfer de secuencias de vídeo (con memoria RAM).

Ethernet/puerto de Alimentación a través de Ethernet para conectar a una red IP y enviar y recibir datos, y para alimentar la unidad y la cámara conectada si ésta admite PoE

Puerto serie (RS-232/422/485) que se utiliza para controlar la función de movimiento horizontal/vertical y zoom de una cámara analógica PTZ.

Conectores de entrada/salida para dispositivos externos, tales como: sensores para detectar eventos de alarma y relés para activar, por ejemplo, luces como respuesta a un evento.

- Entrada de audio para conectar un micrófono o un equipo de entrada de línea y salida se audio para conectar altavoces.

Figura 26 Codificador De Video

De acuerdo a la configuración, cantidad de cámaras y tipo de cámara se pueden utilizar varios tipos de servidores de video:

2.6.12 Servidores de Video Montados en Rack.

Los codificadores de vídeo montados en rack son utilizados cuando existe un gran número de cámaras analógicas con cables coaxiales que van hasta una sala de control exclusiva, además permiten que muchas cámaras analógicas se controlen y gestionen desde un rack situado en una ubicación central.

Un rack permite montar distintos codificadores de vídeo en tarjeta y por eso se convierte en una solución flexible, ampliable y de alta densidad. Un codificador de vídeo en tarjeta admite una, cuatro o seis cámaras analógicas. La tarjeta es un codificador de vídeo pero sin carcasa, no funcionan por sí sola, sino que debe montarse en un rack.

Figura 27 Servidor de Video Montable en Rack

2.6.13 Codificadores de vídeo independientes

El tipo de codificadores de vídeo más habitual son los independiente, que ofrece una conexión o conexión multicanal (hasta cuatro puertos) a cámaras analógicas. Un servidor de vídeo multicanal es idóneo para las

situaciones en las que hay diversas cámaras analógicas ubicadas en una instalación bastante distancia de la sala central de supervisión, A través de este equipo las señales de vídeo de las cámaras pueden compartir el mismo cable de red, con lo que se reducen los costes del cableado.

Un codificador de vídeo produce imágenes digitales, de modo que no se reduce la calidad de imagen a causa de la distancia recorrida por la transmisión de vídeo digital.

Figura 28 Servidor De Video Independiente

2.7 Sistemas Inalámbricos De Transmisión

2.7.1 Transmisión inalámbrica.

Espectro electromagnético

Cuando los electrones se mueven crean ondas electromagnéticas que se pueden propagar en el espacio libre, aun en el vació.

La cantidad de oscilaciones por segundo de una onda electromagnética es su frecuencia, f, y se mide en Hz. La distancia entre dos máximos o

mínimos consecutivos se llama longitud de onda y se designa con la letra griega λ.

Al conectarse una antena apropiada a un circuito eléctrico, las ondas electromagnéticas se pueden difundir de manera eficiente y captarse por un receptor a cierta distancia. Toda la comunicación inalámbrica se basa en este principio.

En el vació todas las ondas electromagnéticas viajan a la misma velocidad, sin importar su frecuencia. Esta velocidad, usualmente llamada velocidad de la luz, c, es aproximadamente $3x10^8$ m/seg.

La figura 30, nos muestra el espectro electromagnético. Las porciones de radio, microondas, infrarrojo y luz visible del espectro pueden servir para transmitir información modulando la amplitud, la frecuencia o la fase de las ondas.

2.7.2 Radio Transmisión

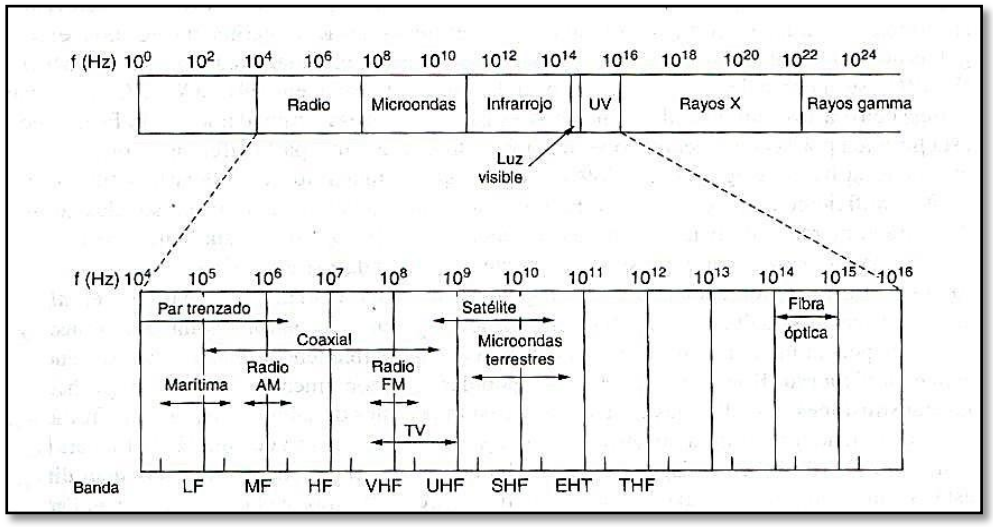

Figura 29 Espectro Electromagnético Para Comunicaciones

Las ondas de radio son fáciles de generar, pueden viajar distancias largas y penetrar edificios sin problemas, de modo que se utilizan mucho en la comunicación, tanto de interiores como de exteriores.

Las ondas de radio también son omnidireccionales, ósea viajan en todas las direcciones desde la fuente, por lo cual el transmisor y el receptor no tienen que alinearse.

Las propiedades de las ondas de radio dependen de la frecuencia. A bajas frecuencias, las ondas de radio cruzan bien los obstáculos, pero la potencia se reduce drásticamente con la distancia a la fuente. A frecuencias altas, las ondas de radio tienden a viajar en línea recta y a rebotar en los obstáculos. También son absorbidas por la lluvia. Todas las ondas de radio están sujetas a interferencia por los motores y equipos eléctricos.

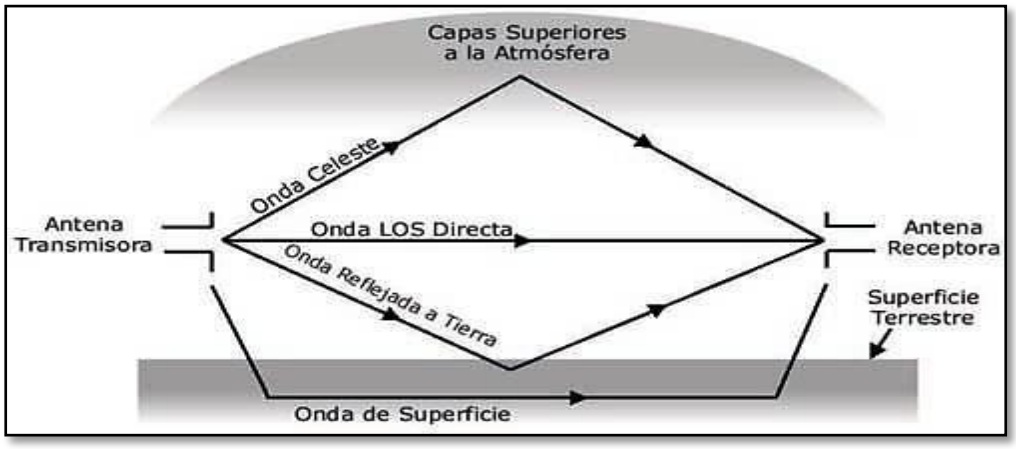

Figura 30 Componentes De Una Onda De Radio

Debido a la capacidad de viajar distancias largas y la interferencia entre usuarios, los gobiernos legislan el uso de radiotransmisores.

2.7.3 Transmisión por Microondas

Por encima de los 100MHZ las ondas viajan en línea recta y, por tanto se pueden enfocar en un haz estrecho. Concentrar toda la energía en haz pequeño con una antena parabólica produce una señal mucho más alta en relación con el ruido, pero las antenas transmisora y receptora se deben alinear entre sí.

2.7.4 Transmisión por Ondas Infrarrojas

Las ondas infrarrojas se usan mucho para la comunicación de corto alcance. Por ejemplo los controles remotos de los equipos utilizan comunicación infrarroja. Estos controles son direccionales, tienen el inconveniente de no atravesar los objetos sólidos.

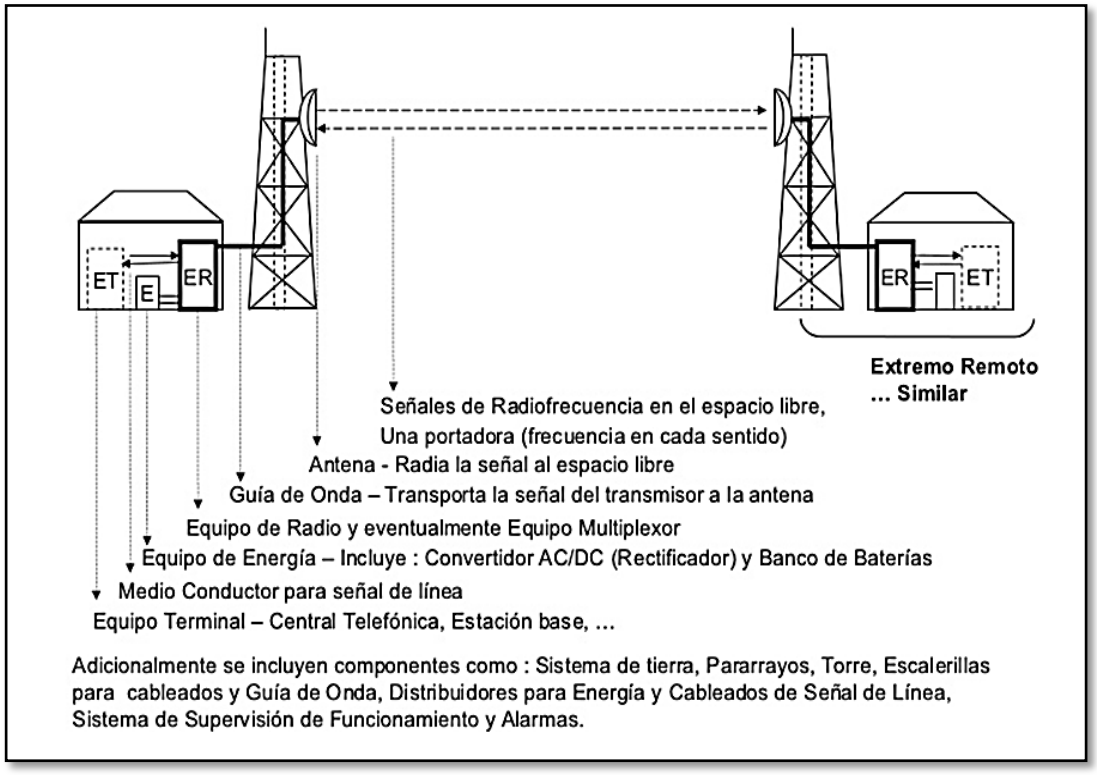

Figura 31 Componentes Enlace Microondas

El hecho de que las ondas infrarrojas no atraviesen los sólidos es una ventaja. Por lo que un sistema infrarrojo no interferirá un sistema similar en un lado adyacente. Además la seguridad de estos sistemas contra espionaje es mejor que la de los sistemas de radio.

Este sistema no necesita de licencia del gobierno para operar. Esta propiedad ha hecho del infrarrojo un candidato interesante para las LAN inalámbricas en interiores.

2.7.5 Transmisión por Ondas de Luz

Este tipo de transmisión se ha usado durante siglos. Una aplicación es conectar las LAN de dos edificios por medio de láseres montados en la parte más alta de los edificios, esta señalización óptica es unidireccional por lo que cada edificio necesita su propio láser y su propio foto detector. Este esquema ofrece un ancho de banda muy alto y un costo muy bajo. Fácil de instalar y no requiere de licencia.

Por ser un haz muy estrecho tiene ventajas pero también es una debilidad La desventaja es que los rayos láser no pueden penetrar la lluvia ni la niebla densa, funcionan bien en días soleados.

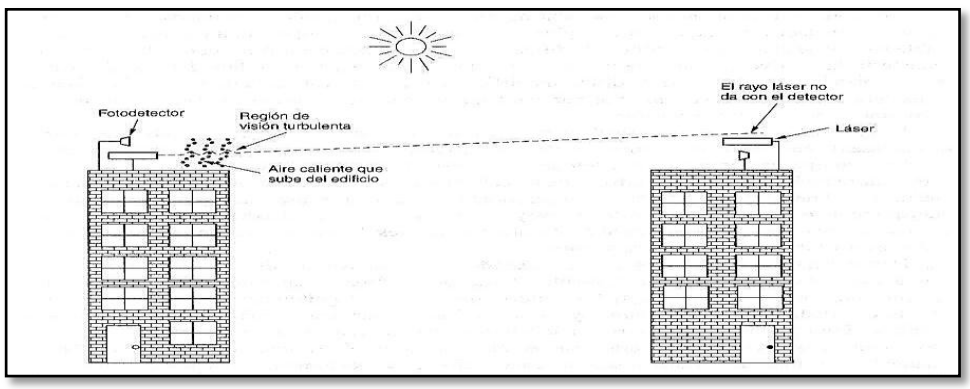

Figura 32 Transmisión Por Ondas De Luz

2.7.6 Redes Inalámbricas

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica.

La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada.

Las Redes Inalámbricas facilitan la operación en lugares donde los equipos no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos. No se espera que las redes

inalámbricas lleguen a remplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica.

Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps, las redes cableadas ofrecen velocidades de 10 Mbps y se espera que alcancen velocidades de hasta 100 Mbps. Los sistemas de Cable de Fibra Óptica logran velocidades aún mayores, y pensando futuristamente se espera que las redes inalámbricas alcancen velocidades de más de 10 Mbps.

Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, de esta manera generar una "Red Híbrida" y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina.

Existen dos amplias categorías de Redes Inalámbricas:

De Larga Distancia.- Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como Redes de Área Metropolitana MAN); sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps.

De Corta Distancia.- Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que

no se encuentran muy retirados entre sí, con velocidades del orden de 280 Kbps hasta los 2 Mbps.

Existen dos tipos de redes de larga distancia: Redes de Conmutación de Paquetes (públicas y privadas) y Redes Telefónicas Celulares. Estas últimas son un medio para transmitir información de alto precio. Debido a que los módems celulares actualmente son más caros y delicados que los convencionales, ya que requieren circuiteria especial, que permite mantener la pérdida de señal cuando el circuito se alterna entre una célula y otra. Esta pérdida de señal no es problema para la comunicación de voz debido a que el retraso en la conmutación dura unos cuantos cientos de milisegundos, lo cual no se nota, pero en la transmisión de información puede hacer estragos.

Redes Públicas de Radio.- Las ondas de radio pueden viajar a grandes distancias y penetrar los edificios sin problemas, razón por la cual se usan tanto en interiores como en exteriores. Las ondas de radio son

omnidireccionales ósea viajan en todas las direcciones por lo que el transmisor y receptor no tienen que alinearse. Las propiedades de la onda dependen de la frecuencia.

Abajas frecuencias las ondas de radio cruzan bien los obstáculos, pero la potencia disminuye drásticamente con la distancia de la fuente.

A frecuencias altas, las ondas tienden a viajar en línea recta y a rebotar por los obstáculos también son absorbidas por la lluvia. En todas las frecuencias, las ondas de radio están sujetas a interferencia por motores y otros equipos eléctricos. Esta es una de las razones por la cual, los gobiernos legislan el uso de los radiotransmisores.

Estas redes operan en un rango de 800 a 900 Mhz. Con una velocidad de transmisión de 4.8 Kbps. La red pública en Estados Unidos opera a 19.2 Kbps; y a 9.6 Kbps en Europa (debido a una banda de frecuencia más angosta).

Redes De Área Local (LAN).- Las redes inalámbricas se diferencian de las convencionales principalmente en la "Capa Física" y la "Capa de Enlace de Datos", según el modelo de referencia OSI. La capa física indica como son enviados los bits de una estación a otra. La capa de Enlace de Datos (denominada MAC), se encarga de describir como se empacan y verifican los bits de modo que no tengan errores. Las demás capas forman los protocolos o utilizan puentes, ruteadores o compuertas para conectarse. Los dos métodos para remplazar la capa física en una red inalámbrica son la transmisión de Radio Frecuencia y la Luz Infrarroja.

Redes Infrarrojas.- Las ondas infrarrojas se usan para comunicaciones de corto alcance no atraviesan los objetos sólidos lo cual ofrece una ventaja de no interferencia.

Además, la seguridad de los sistemas infrarrojos contra espionaje es mejor que la de los sistemas de radio, no es necesario obtener licencia del gobierno para operar un sistema infrarrojo.

Las redes de luz infrarroja están limitadas por el espacio y casi generalmente la utilizan redes en las que las estaciones se encuentran en un solo cuarto o piso, algunas compañías que tienen sus oficinas en varios edificios realizan la comunicación colocando los receptores/emisores en las ventanas de los edificios.

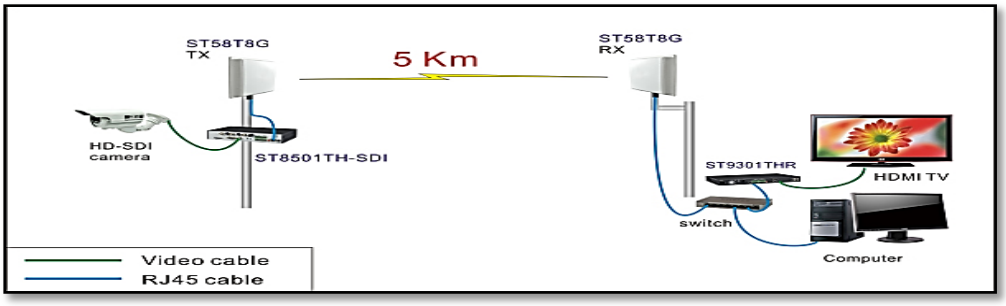

Figura 33 Red CCTV Infrarrojo

Las transmisiones de radio frecuencia tienen una desventaja: que los países están tratando de ponerse de acuerdo en cuanto a las bandas que cada uno puede utilizar, al momento de realizar este trabajo ya se han reunido varios países para tratar de organizarse en cuanto a que frecuencias pueden utilizar cada uno. La transmisión Infrarroja no tiene este

inconveniente por lo tanto es actualmente una alternativa para las Redes Inalámbricas.

El mismo principio se usa para la comunicación de Redes, se utiliza un "transceptor" que envía un haz de Luz Infrarroja, hacia otro que la recibe.

La transmisión de luz se codifica y decodifica en el envío y recepción en un protocolo de red existente. Se pueden instalar varias estaciones en una sola habitación utilizando un área pasiva para cada transceptor.

Redes de Radio Frecuencia.- Por el otro lado para las Redes Inalámbricas de Radio Frecuencia, la FCC permitió la operación sin licencia de dispositivos que utilizan 1 Watt de energía o menos, en tres bandas de frecuencia : 902 a 928 MHz, 2,400 a 2,483.5 MHz y 5,725 a 5,850 MHz. Esta bandas de frecuencia, llamadas bandas ISM, estaban anteriormente

limitadas a instrumentos científicos, médicos e industriales. Esta banda, a diferencia de la ARDIS y MOBITEX, está abierta para cualquiera.

Red Lan Ethernet Híbrida (Coaxial/Infrarrojo).- Las ventajas de las Redes de Área Local Inalámbricas (LAN´s) sobre las cableadas son: flexibilidad en la localización de la estación, fácil instalación y menores tiempos en la reconfiguración.

Las tecnologías para las LAN´s inalámbricas son dos: Infrarrojas y Radio Frecuencia. El grupo IEEE 802.11 está desarrollando normas para LAN´s inalámbricas.

Ellos planean introducir una nueva Subcapa de Control De Acceso al Medio (MAC) que tenga capacidad de accesar varios medios de transmisión y que tenga un rango aceptable para los requerimientos del usuario.

Así las LAN´s inalámbricas, únicamente son compatibles con las LAN´s cableadas existentes (incluyendo Ethernet) en la Subcapa de Control de Enlaces Lógicos (LLC).

Sin embargo por restricciones, el rango de aplicaciones de éstas requieren estaciones fijas y por reordenamiento, para la tecnología infrarroja, es posible rehusar cualquiera de las Subcapas MAC. Se propondrán algunas soluciones para la introducción de células infrarrojas dentro de redes Ethernet existentes (10Base5 ó se2).

Descripcion de Ethernet.- Ethernet es una topología de red que basa su operación en el protocolo MAC CSMA/CD. En una implementación "Ethernet CSMA/CD", una estación con un paquete listo para enviar, retarda la transmisión hasta que "sense" o verifique que el medio por el cual se va a

trasmitir, se encuentre libre o desocupado. Después de comenzar la transmisión existe un tiempo muy corto en el que una colisión puede ocurrir, este es el tiempo requerido por las estaciones de la red para "sensar" en el medio de transmisión el paquete enviado. En una colisión las estaciones dejan de transmitir, esperan un tiempo aleatorio y entonces vuelven a sensar el medio de transmisión para determinar si ya se encuentra desocupado.

Una correcta operación, requiere que las colisiones sean detectadas antes de que la transmisión sea detenida y también que la longitud de un

paquete colisionado no exceda la longitud del paquete. Estos requerimientos de coordinación son el factor limitante del espacio de la red. En un cableado Ethernet el medio coaxial es partido en segmentos, se permite un máximo de 5 segmentos entre 2 estaciones. De esos segmentos únicamente 3 pueden ser coaxiales, los otros 2 deben de tener un enlace punto-a-punto. Los segmentos coaxiales son conectados por medio de repetidores, un máximo de 4 repetidores pueden ser instalados entre 2 estaciones. La longitud máxima de cada segmento es:

1.- 500 mts para 10Base5

2.-185 mts para l0Base2.

La función del repetidor es regenerar y retransmitir las señales que viajen entre diferentes segmentos, y detectar colisiones.

Modos de Radiación Infrarrojos.- Las estaciones con tecnología infrarroja pueden usar tres modos diferentes de radiación para intercambiar la energía Óptica entre transmisores-receptores: punto-a-punto cuasi-difuso y difuso.

En el modo punto-a-punto los patrones de radiación del emisor y del receptor deben de estar lo más cerca posible, para que su alineación sea correcta. Como resultado, el modo punto-a-punto requiere una línea-de-vista entre las dos estaciones a comunicarse. Este modo es usado para la implementación de redes Inalámbricas Infrarrojas Token-Ring. El "Ring" físico es construido por el enlace inalámbrico individual punto-a-punto conectado a cada estación.

Configuracion de una red etherneth hibrida. Los nuevos componentes imponen restricciones a la máxima extensión física de la red, como se mencionó un Ethernet coaxial puede tener un máximo de 5 segmentos (3 coaxiales) y 4 repetidores entre 2 estaciones. La Ethernet híbrida debe de respetar estas reglas.

Ahora un MCU será como un repetidor coaxial al momento de la definición de la red, con funciones similares. Algunas restricciones resultan de este factor, dado que la transformación de un paquete entre dos estaciones inalámbricas de diferentes células, se transportará a través de dos MCUs, por ejemplo, si se requiere que 3 segmentos deban de soportar células infrarrojas (segmentos híbridos), entonces el enlace punto-a-punto no puede ser utilizado entre estos segmentos.

La extensión máxima de una red híbrida se obtiene cuando un segmento es híbrido.

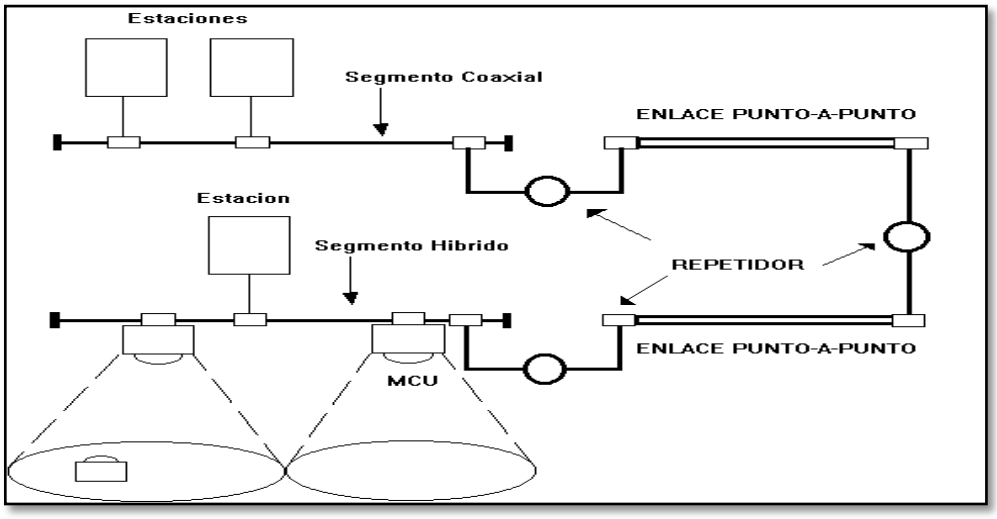

Figura 34 Red Ethernet Híbrida

Bluetooth.- Describe un método de conectividad móvil universal con el cual se pueden interconectar dispositivos como teléfonos móviles, Asistentes

Personales Digitales (PDA), ordenadores y muchos otros dispositivos, ya sea en el hogar, en la oficina o, incluso, en el automóvil, utilizando una conexión inalámbrica de corto alcance.

Es un estándar que describe la manera en la que una enorme variedad de dispositivos pueden conectarse entre sí, de una forma sencilla y sincronizada, con cualquier otro equipo que soporte dicha tecnología utilizando las ondas de radio como medio de transporte de la información.

Técnicamente, la implementación de esta novedosa tecnología no entraña ninguna complicación técnica especialmente problemática ni sofisticada. Tampoco supone que los nuevos dispositivos equipados con esta tecnología deban sufrir profundas revisiones o modificaciones, todo lo contrario.

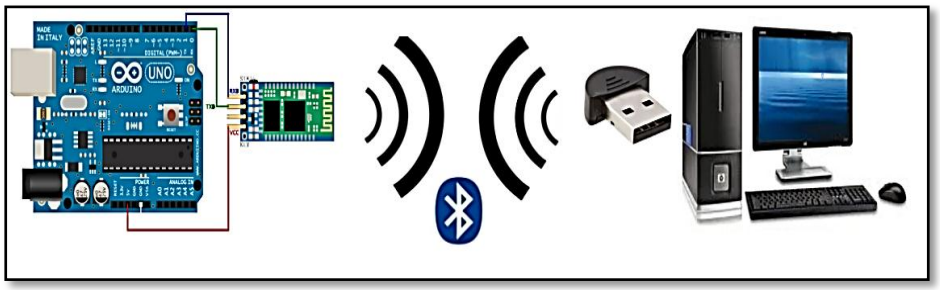

Figura 35 Comunicación Bluethooth

En sí, cada dispositivo deberá estar equipado con un pequeño chip que transmite y recibe información a una velocidad de 1 Mbps en la banda de frecuencias de 2,4 GHz que está disponible en todo el mundo, con ciertas particularidades según los diferentes países de aplicación, ya que es empleada con enorme profusión en numerosos dispositivos.

La tecnología HomeRF.- Con una finalidad muy similar, la tecnología HomeRF, basada en el protocolo de acceso compartido (Shared Wireless Access Protocol - SWAP), encamina sus pasos hacia la conectividad sin cables dentro del hogar.

Los principales valedores de estos sistemas, se agrupan en torno al Consorcio que lleva su mismo nombre HomeRF, teniendo a Proxim (una filial de Intel) como el miembro que más empeño está realizando en la implantación de dicho estándar.

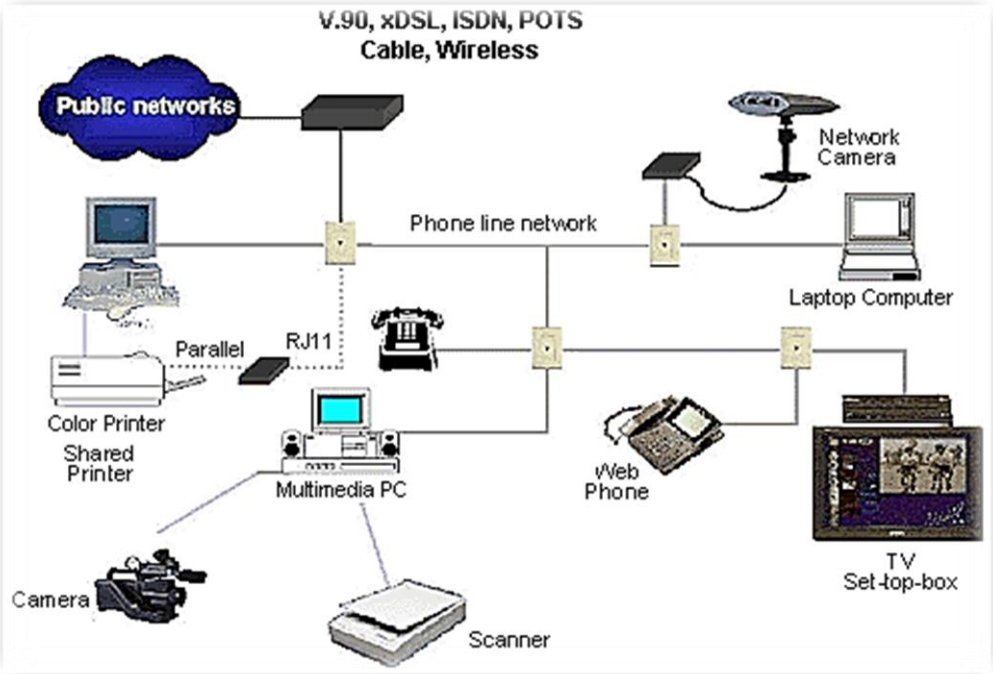

Figura 36 Comunicación HOMERF

Las redes inalámbricas pueden tener mucho auge en nuestro país debido a la necesidad de movimiento que se requiere en la industria. La tecnología óptica se puede considerar que es la más práctica y fácil de

implementar pues para la tecnología de radio se deben de pedir licencias de uso del espacio.

Como ya se dijo es relativamente fácil el crear una red híbrida, porque seguiríamos teniendo las ventajas de la velocidad que nos brinda la parte cableada y expandiríamos las posibilidades con la parte inalámbrica, la implementación de una red híbrida Ethernet con infrarrojos y coaxial, que se puede considerar una de las redes de más uso en el mundo.

Obviamente, no se espera que las redes inalámbricas lleguen a reemplazar a las redes cableadas, las prestaciones de unas y otras, a día de hoy, no pueden compararse.

Sin embargo, la pacífica convivencia de las redes cableadas y las inalámbricas , da lugar a una nueva generación de redes híbridas que

cubren por completo, según su configuración y diseño, las necesidades de conectividad tanto fija como móvil, que toda empresa moderna y competitiva requiere las redes inalámbricas (wireless) han venido ha revolucionar el mercado de las comunicaciones no solo de datos, ahora también para la voz y el video propiciando una integración total de medios para las empresas, las instituciones y el servicio público en general.

Velocidad de las redes inalámbricas.- Un nuevo estándar en la industria, el 802.11b, comúnmente conocido como Wi-Fi, puede transmitir datos a velocidades de hasta 11 megabits por segundo (Mbps) a través de enlaces inalámbricos. En comparación, las redes estándares de Ethernet ofrecen 10 Mbps. El Wi-Fi es más de cinco veces más rápido que las soluciones inalámbricas de la generación anterior, y su rendimiento es más que suficiente para la mayoría de las aplicaciones de negocios.

Wi-Fi.- Es una certificación de interoperabilidad para sistemas 802.11b, que otorga la Alianza de Compatibilidad de Ethernet Inalámbrico (Wireless Ethernet Compatibility Alliance - WECA). El sello Wi-Fi indica que algún aparato ha pasado pruebas independientes y que opera confiablemente con

otros equipos certificados en dicha certificación. Los clientes se benefician de este estándar ya que no están atados a la solución de un solo fabricante: pueden comprar puntos de acceso y PC cards, certificados con Wi-Fi, de diferentes fabricantes y confiar en que trabajarán conjuntamente.

Uso de las Redes Inalámbricas.- Algunos ejemplos de cuándo una red inalámbrica podría ser su solución ideal.

- Para oficinas temporales
- Cuando los cables no son prácticos ni posibles
- Soporte de usuarios móviles en localidades externas
- Expansión de una red de cables
- Redes temporales
- Oficinas en el hogar

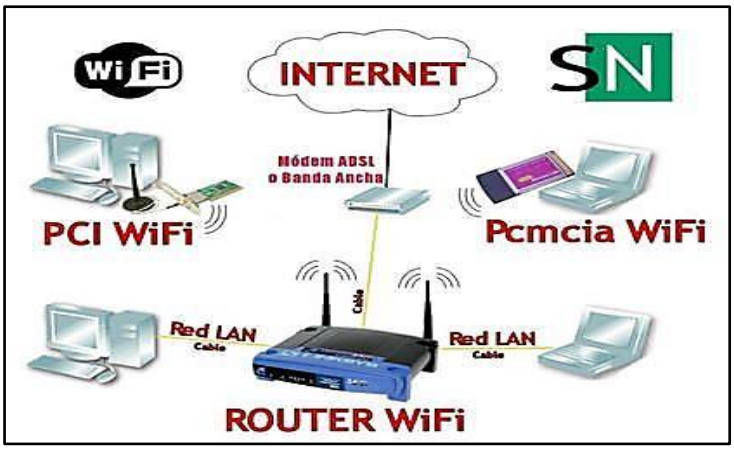

Figura 37 Comunicación WiFi

Seguridad y Privacidad en las Redes Inalámbricas.- Si se escoge una solución con sofisticadas tecnologías de seguridad, las comunicaciones inalámbricas serán muy seguras. Las soluciones líderes ofrecen encriptación de 128 bits y para los niveles más altos de seguridad, los sistemas más avanzados generarán automáticamente una nueva clave de 128 bits para cada sesión de red inalámbrica. Estos sistemas también ofrecerán autenticación de usuarios, requiriendo que cada usuario ingrese con una contraseña.

Elementos que constituyen una red inalámbrica.-

- Puntos de acceso
- PC Cards

Las redes inalámbricas están formadas por dos componentes: puntos de acceso y PC cards. Los componentes se comunican entre sí, a través de transmisiones de frecuencia de radio, que eliminan la necesidad de cables.

Puntos de acceso.- Una red inalámbrica se crea con uno o más puntos de acceso que actúan como hubs, enviando y recibiendo señales de radio desde o hacia computadoras personales equipadas con PC cards inalámbricas para clientes. El punto de acceso puede ser un aparato en sí que forma parte de la base de la red o la conecta por medio de cables a una red de área local (LAN) convencional. Los usuarios pueden enlazar múltiples puntos de acceso a una LAN, creando segmentos inalámbricos en todas sus instalaciones.

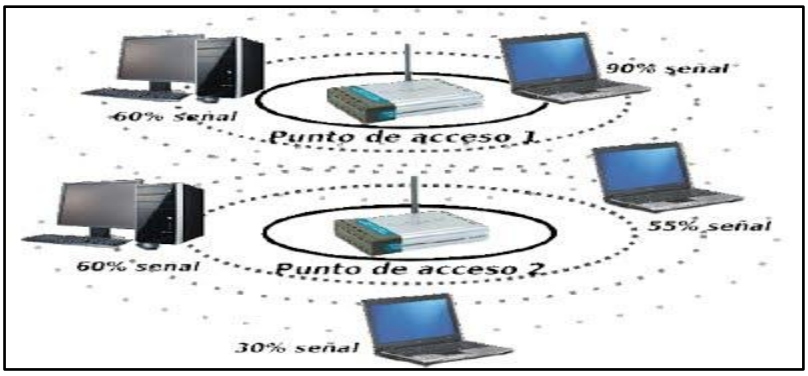

Figura 38 Puntos De Acceso Red Inalámbrica

PC Cards .- Para comunicarse con el punto de acceso, cada equipo portátil o de escritorio necesita una tarjeta especial para redes inalámbricas.

Al igual que las tarjetas de interfaz para redes (NICs) de las redes tradicionales, estas tarjetas permiten que los aparatos se comuniquen con el punto de acceso.. Además, un usuario puede conectar cualquier otro dispositivo que no tenga una ranura para Tarjetas PC o PCI a su red inalámbrica, al usar un Ethernet Client Bridge que funciona con cualquier dispositivo que cuente con Ethernet o puerto serial, impresoras, escáners, etc.

Una vez que se conecta el punto de acceso a una toma de poder y los aparatos en red están debidamente equipados con tarjetas inalámbricas, las conexiones de red se hacen automáticamente cuando estos aparatos se encuentren dentro del campo de alcance del hub. El campo de alcance de una red inalámbrica en ambientes estándares de oficinas puede ser de varios cientos de metros.

Las redes inalámbricas operan igual que las redes tradicionales y ofrecen los mismos beneficios y eficiencia en cuanto a productividad.

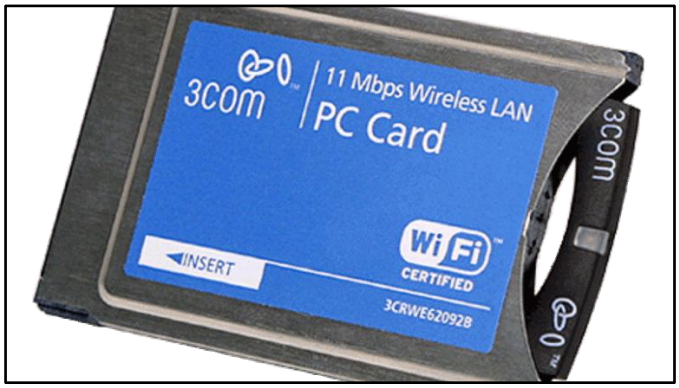

Figura 39 PC Card

Los usu

arios podrán compartir archivos, aplicaciones, periféricos y acceso al Internet.

2.7.7 Características de una red inalámbrica

- Estar basada en estándares y contar con certificación Wi-Fi
- Instalación simple
- Robusta y confiable
- Escalabilidad
- Facilidad de uso
- Servidor Web para una administración más fácil
- Seguridad
- Una aplicación que detecte localidades

Estar basada en estándares y contar con certificación Wi-Fi

La selección de una solución inalámbrica basada en estándares, que sea totalmente ínter operable con redes Ethernet y Fast Ethernet, le permitirá al usuario que su red inalámbrica trabaje sin interrupciones con su sistema existente de LAN tradicional.

Instalación simple

La solución inalámbrica debe ser del tipo plug and play; tomando solamente unos minutos para su instalación.

Al conectarla, los usuarios empezaran a gozar de inmediato de los servicios en red. Para obtener una instalación aún más fácil, su solución deberá soporta el protocolo denominado Dynamic Host Configuration Protocol (DHCP), el cual asignará automáticamente direcciones IP a los clientes inalámbricos.

En lugar de instalar un servidor DHCP en algún aparato independiente para obtener esta capacidad de ahorro de tiempo, losusuarios deben seleccionar hubs inalámbricos que ofrezcan servidores DHCP incorporados.

Robusta y confiable

Considere soluciones inalámbricas robustas que tengan alcances de por lo menos 100 metros. Estos sistemas le ofrecerán una considerable movilidad dentro sus instalaciones. Un usuario puede optar por un sistema superior que automáticamente detecte el ambiente, para seleccionar la mejor señal de frecuencia de radio disponible y obtener máximos niveles de comunicaciones entre el punto de acceso y las PC cards.

Escalabilidad

Un hub inalámbrico deberá soportar aproximadamente 60 usuarios simultáneos, permitiéndole expandir su red con efectividad de costos, con simplemente instalar tarjetas inalámbricas adicionales listas para ser conectadas a la red.

Facilidad uso

Si un usuario planea conectar múltiples hubs inalámbricos a una red existente de cables, considere una solución que ofrezca conexiones automáticas a la red. Cuando un usuario se desplace fuera de los límites de un hub al campo de otro, una capacidad automática de conexión a la red transferirá sus comunicaciones sin interrupciones al siguiente aparato, aún al cruzar límites de routers, sin siquiera tener que reconfigurar la dirección IP manualmente.

Servidor Web para una administración más fácil

Un usuario simplificará la administración de su red inalámbrica si selecciona un punto de acceso con un servidor Web incorporado. Esto le permitirá acceder y definir parámetros de configuración, monitorear el rendimiento y hacer diagnósticos desde un navegador Web.

Seguridad

Una solución segura también le ofrecerá una encriptación de por lo menos 40 bits de encriptación. Tanto para su facilidad de uso como para una protección más fuerte, una solución superior que automáticamente genere una clave nueva de 128 bits para cada sesión de red inalámbrica, sin tener que ingresar la clave manualmente. Además, el usuario debe considerar un

sistema que ofrezca autenticación del usuario, requiriendo que una contraseña antes de acceder la red.

2.8 Sistemas Alámbricos De Transmisión

En las instalaciones de circuito cerrado de televisión se utilizan cables coaxiales para transmitir la información entre las cámaras y el resto de los dispositivos de la instalación, pero gracias a los avances de la tecnología en lo que respecta a la electrónica y telecomunicaciones, han desarrollado otros medios de comunicación que ofrecen mejores ventajas al momento de realizar el montaje y configuración de un sistema de este tipo.

La señal de video que sale de la cámara debe llegar en las mejores condiciones posibles al monitor o monitores correspondientes, para lo cual se emplean las líneas de transmisión que debe ser capaz de transportar la señal de video. Usualmente el método de transmisión ha sido el cable

coaxial, antecesor del cable UTP, usando en las modernas redes de video vigilancia IP.

Dentro los principales medios de transmisión que se utiliza en las instalaciones de CCTV, son: Cableados e inalámbricos

Dentro de los medios de transmisión físicos (cableados), existen varios tipos de cables, pero los más comunes son:

- Cable Coaxial
- Doble par trenzado
- Fibra óptica
-

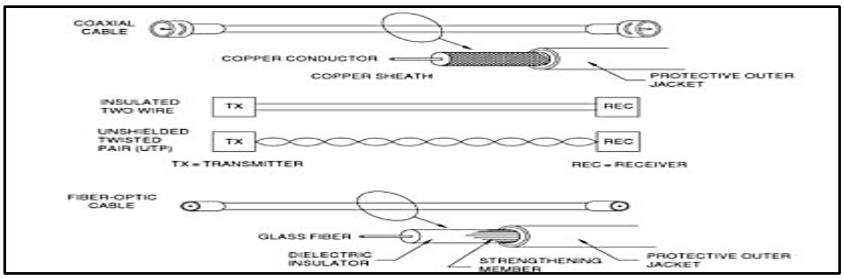

Figura 40 Medios De Transmisión Alámbrico

Cable coaxial

Medio de transmisión utilizado para la distribución de señales electromagnéticas de alta frecuencia, por lo que su uso resulta bastante idóneo en las instalaciones de CCTV, dada que su composición interna es muy resistente ante interferencias externas.

Figura 41 Cable Coaxial

Componentes del cable coaxial:

- La funda protege al cable del entorno externo. Generalmente está hecha fabricada en caucho (o, a veces, Cloruro de Polivinilo (PVC) o Teflón).
- La protección (cubierta de metal) que recubre los cables y protege los datos transmitidos en el medio para que no haya interferencias (o ruido) y los datos se puedan distorsionar.

- El aislante que rodea al núcleo central está fabricado en material dieléctrico que sirve para evitar cualquier contacto con la protección que pueda causar cortocircuitos.
- El núcleo es el que realiza la tarea de transportar los datos.

Consiste en un solo hilo de cobre, o en varias fibras trenzadas. Además tiene mejor blindaje que el cable de par trenzado, así que puede abarcar tramos muy largos a velocidades mayores".

Existen dos tipos de cables coaxiales:

- 10Base2 - cable coaxial delgado (denominado Thinnet o CheaperNet), es un cable delgado (6 mm. de diámetro) que por convención, es blanco (o grisáceo). Este cable es muy flexible y se puede utilizar en la mayoría de las redes, conectándolo directamente a la tarjeta de red. Es capaz de transportar una señal hasta unos 185 metros, sin que se pierda la señal.

- 10Base5 - cable coaxial grueso (Thicknet o Thick Ethernet también se denomina Cable Amarillo, ya que, por convención, es de color amarillo), es un cable protegido con un diámetro más grueso (12 mm.) y 50 ohm de impedancia, posee un núcleo con un diámetro más grueso y es capaz de transportar señales a través de grandes distancias: hasta 500 metros sin perder la señal.

Cable de par trenzado: Este es uno de los medio de transmisión más utilizados en las redes de área local. Está compuesto básicamente por 2 cables de cobre entrecruzados en forma de espiral recubiertos por un aislante, pero normalmente está formado por un grupo de cuatro pares trenzados, recubiertos en una envoltura protectora.

Existen varios tipos de cable de par trenzado, el mismo que se detalla a continuación:

Cable de Par trenzado No Protegido (UTP) Unshielded Twisted Pair

El cable UTP cumple con la especificación 10BaseT. Este es el tipo de cable de par trenzado más utilizado, fundamentalmente en redes locales. A continuación le mostraremos algunas de sus características:

- Longitud máxima de segmentación: 100 metros.

- Composición: 2 hilos de cobre recubiertos por un material aislante.

- Estándares UTP: determinan el número de vueltas por pie (33 cm.) del cable, según el uso que se le quiera dar.
- UTP: recopilado en la EIA/TIA (Electronic Industries Association / Telecommunication Industries Association (Asociación de Industrias

  Electrónicas / Asociación de Industrias de la Telecomunicación)) Commercial Building Wiring Standard 568. El estándar EIA/TIA568 utiliza UTP para crear estándares que se apliquen a todo tipo de espacios y situaciones de cableado, garantizando de esta manera productos homogéneos al público.

Categorías del cable UTP:

- Categoría 1: Cable de teléfono tradicional (transmisión de voz pero no de datos)
- Categoría 2: Transmisión de datos hasta un máximo de 4 Mb/s (RNIS). Este tipo de cable contiene 4 pares trenzados.

- Categoría 3: máximo de hasta 10 Mb/s. Este tipo de cable contiene 4 pares trenzados y 3 trenzas por pie

- Categoría 4: máximo de hasta 16 Mb/s. Este tipo de cable contiene 4 pares de hilos de cobre trenzados.
- Categoría 5: máximo de hasta 100 Mb/s. Este tipo de cable contiene 4 pares de hilos de cobre trenzados.
- Categoría 5e: máximo de hasta 1000 Mb/s. Este tipo de cable contiene 4 pares de hilos de cobre trenzados.
- Categoría 6: No está estandarizada aunque ya está utilizándose. Se definirán sus características para un ancho de banda de 250 MHz.
- Categoría 7: Definida y mucho menos estandarizada, para un ancho de banda de 600 MHz. El gran inconveniente de esta categoría es el tipo de conector que utiliza.

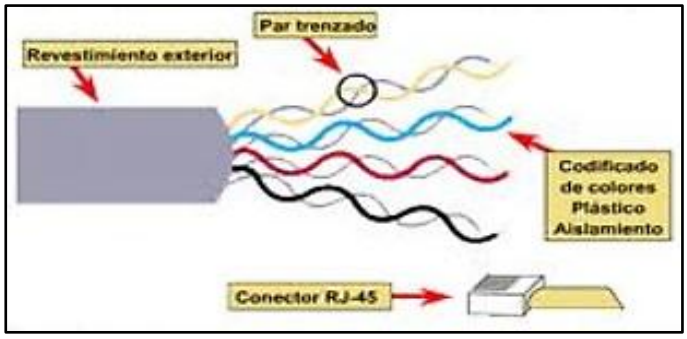

Figura 42 Cable UTP Par Trenzado Sin Blindaje

Cable de Par trenzado protegido (STP) ShieldedTwistedPair

Utiliza una funda de cobre que es de mejor calidad y protege más que la funda utilizada en el cable UTP, contiene una cubierta protectora entre los pares y alrededor de ellos.

En un cable STP, los hilos de cobre de un par están trenzados en sí mismos, lo que da como resultado un cable STP con excelente protección (en otras palabras, mejor protección contra interferencias). También permite una transmisión más rápida a través de distancias más largas.

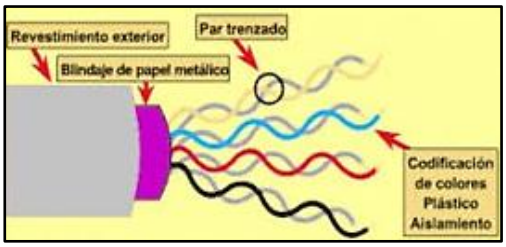

Figura 43 Cable Par Trenzado Blindado

Cable de Fibra óptica

La fibra óptica tiene una estructura cilíndrica, es decir un hilo transparente formado por dos zonas concéntricas llamadas núcleo y recubrimiento. Una vez que la onda ingresa en el núcleo, la diferencia de índices produce «reflexión total» en la frontera entre el núcleo y el recubrimiento, manteniendo la luz confinada en el núcleo y guiada dentro de los extremos de la fibra, lo que es más importante. Esto hace que este tipo de cable sea ideal en los entornos donde haya gran cantidad de interferencias electromagnéticas, además no le influye la humedad ni la exposición solar.

La fibra óptica está constituida por un núcleo de cristal de silicio por el que se envía un haza de naturaleza óptica que codifica la información.

La fibra óptica tiene un diámetro equivalente al grosor de un cabello y se fabrican con vidrio que es material muy barato, además son fáciles de instalar porque son pequeñas y porque alcanzan distancias de 100 Km, logrando reducir el mantenimiento de repetidoras. Estas fibras pueden llegar a conseguir mayores distancias que los cables coaxiales o los cables UTP.

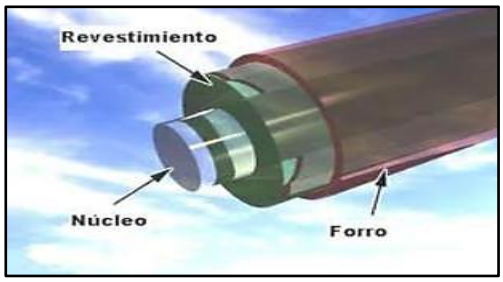

Figura 44 Cable Fibra Óptica

Tipos de Fibra Óptica.

Fibras Multimodo: El término multimodo indica que pueden ser guiados muchos modos o rayos luminosos, cada uno de los cuales sigue un camino diferente dentro de la fibra óptica. Este efecto hace que su ancho de banda sea inferior al de las fibras monomodo. Por el contrario los dispositivos utilizados con las multimodo tienen un coste inferior (LED). Este tipo de fibras son las preferidas para comunicaciones en pequeñas distancias, hasta 10 Km.

Figura 45 Luz En El Interior De La Fibra Óptica Multimodo

Fibras monomodo. El diámetro del núcleo de la fibra es muy pequeño y sólo permite la propagación de un único modo o rayo, el cual se propaga directamente sin reflexión, causando esto un ancho de banda muy elevado, por lo que se utiliza a distancias superiores a 10 Km, junto con dispositivos laser costosas.

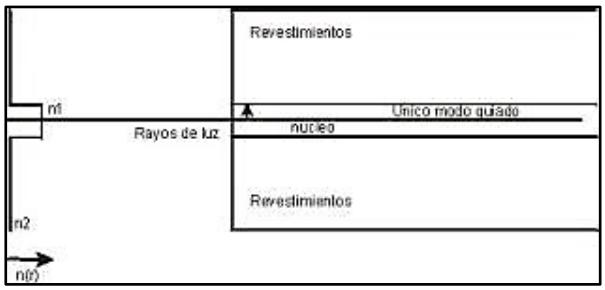

Figura 46 Luz En El Interior De La Fibra Óptica Monomodo

2.9 Sistemas Híbridos

En la terminología de redes, una red híbrida (también llamada topología de red híbrida) combina las mejores características de dos o más redes diferentes. De acuerdo con la Auditoría y Control de la Tecnología de la Información, las topologías híbridas son confiables y versátiles. Estas proporcionan un gran número de conexiones y caminos de transmisión de datos para los usuarios. Las redes más reales son las híbridas.

Los dos tipos principales de redes híbridas son el anillo de estrella y de bus de estrella por cable. Una red de anillo de estrella híbrido con cable combina el diseño físico de una red en estrella y la topología lógica (o el flujo de datos) de una red en anillo. La red de bus de estrella por cable utiliza la distribución física de una red en estrella y la transmisión de datos de una red de bus.

Los componentes de red híbridos comunes incluyen enrutadores, repetidores, concentradores, puentes, conmutadores, módems y cables.

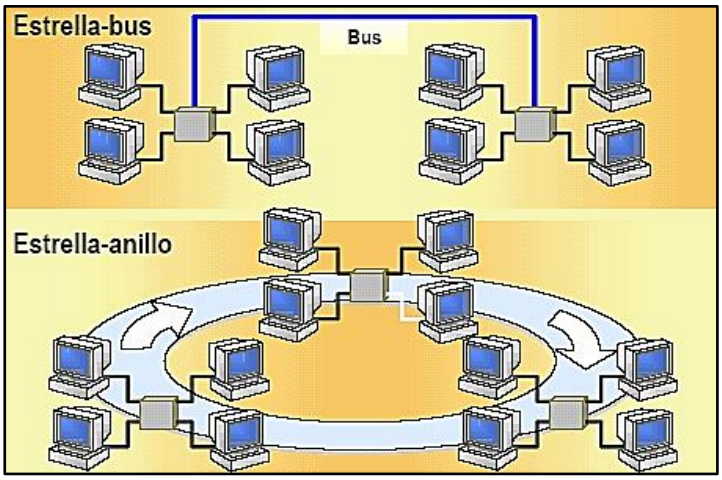

Figura 47 Sistemas Híbridos

Las redes híbridas ofrecen múltiples posibilidades para la transmisión de datos entre nodos de la red. El fallo de cualquier componente simple de hardware (tal como una impresora o un cable) no afecta al rendimiento de la red. En tal caso, la red híbrida evita el nodo/cable afectado y desplaza los datos a una ruta de transmisión alternativa. Las redes híbridas son versátiles y pueden adaptarse a una amplia variedad de requerimientos y tamaños de red.

Las redes híbridas son caras, difíciles de establecer, extender y resolver cuando se presentan problemas, requiere más cableado entre sus nodos que otros tipos de redes. Las inconsistencias y errores en los nodos individuales de una red híbrida son a menudo difíciles de aislar y reparar. Las redes híbridas eficientes requieren puntos o centros inteligentes de concentración. Los concentradores inteligentes están diseñados para proporcionar aislamiento de fallos y procesamiento automáticos.

Constantemente escanean la red, recogen información sobre todos los nodos, detectan errores, aíslan los nodos defectuosos y convierten el tráfico de red a rutas alternas. Los concentradores inteligentes, aunque eficientes, son más caros que los pasivos y los activos. Las redes híbridas de gran tamaño comúnmente requieren varios concentradores inteligentes.

CAPITULO 3

ESTUDIO Y SITUACIÓN ACTUAL DE LA ESPE

3.1 Descripción Física le las Instalaciones del Campus Politécnico (ESPE - Sangolquí).

La Escuela Politécnica del Ejército ESPE se encuentra ubicada geográficamente en la ciudad de Sangolquí, Valle de los Chillos, a una distancia de 22 kilómetros al Sur - Este de Quito, capital de la República del Ecuador, con una altitud de 2.510 metros sobre el nivel del mar, posee un clima andino privilegiado, con temperaturas que oscilan alrededor de los 20°C.

La ESPE limita: al Norte con las instalaciones del centro de recreación de Petro Ecuador, al Sur la fábrica de artículos militares FAME, al Este la Av. El progreso, urbanización La Colina y al Oeste colinda con la nueva vía Boulevard de Santa Clara y propiedades privadas de Sangolquí.

Figura 48 Ubicación Geográfica De La ESPE- Sangolquí

La red organizacional con que cuenta la universidad, permite administrar todo el sistema que conlleva el manejo de personal, recursos e instalaciones que cuenta este instituto de educación superior en sus diferentes niveles.

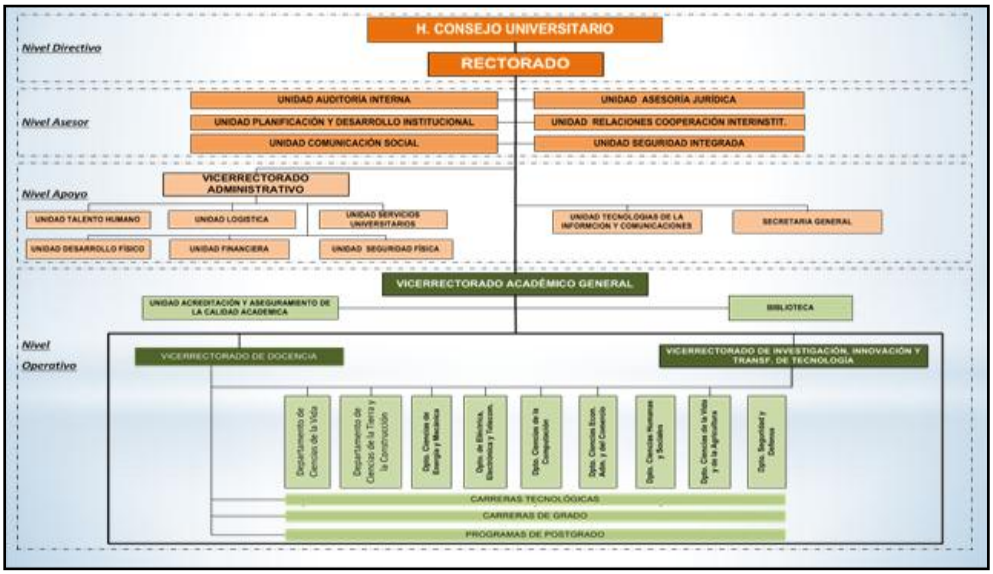

Figura 49 Red Organizacional De La ESPE- Sangolquí

La Escuela Politécnica del Ejército ESPE, tiene 26 edificios/bloques, los mismos que son utilizados para aulas, oficinas, laboratorios, biblioteca, residencia, bodegas, SIS y coliseo.

Figura 50 Edificios/Bloques ESPE- Sangolquí

Los edificios/bloques son de fácil acceso, se puede trasladar a pie o en vehículo, utilizando el anillo vial de aproximadamente 1,8 Km que circunvala todo el campus universitario, con acceso a 8 parqueaderos distribuidos acorde a las necesidades de nivel de gestión educativa.

Para el desarrollo de este proyecto se ha considerado inicialmente en forma macro al Campus Politécnico, el cual consta de dos sitios de acceso vehicular y peatonal.

1.- Acceso Principal - Este (Av. Gral. Rumiñahui).
2.- Acceso Secundario – Oeste (Boulevard de Santa Clara).

Para el control mediante el sistema de ojos de águila, se ha dividido el área del Campus Politécnico en 4 zonas.

Zona 1: Salida e ingreso peatonal y vehicular, por el sector ESTE del Campus.

Zona 2: Parqueadero ubicado en el sector este, centro de investigaciones tecnológicas, centro médico, ingreso a la biblioteca, laboratorios de electrónica, postgrados y perímetro en la parte noroste

Zona 3: Laboratorios de mecánica, geográfica, gasolinera y perímetro en la parte noroste, parqueadero ubicado en el bar, ingreso y salida oste, estadio.

Zona 4: Talleres, auto centro, estadio y perímetro por la parte sureste, coliseo, canchas de vóley, tennis, residencia, comedor, parqueaderos por la parte este y material bélico.

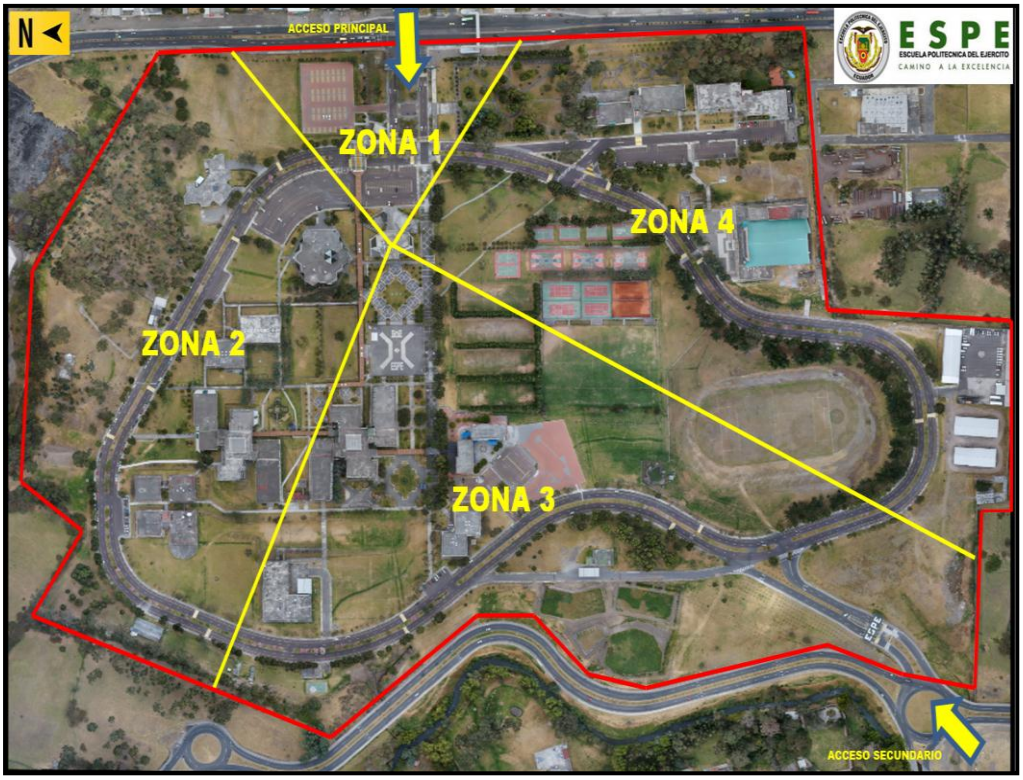

Figura 51 Zonificación ESPE- Sangolquí

La ESPE, por ser un centro educativo posee con recursos tanto el humanos como material de cuantiosa valía económica y por estar ubicada en un sitio central de la ciudad, donde se genera el movimiento económico e industrial de Sangolquí, por lo que tiene muchas falencias en lo que respecta a seguridad en las actividades que se suscitan tanto en el día como en la noche, y que dichas debilidades se incrementan por la falta de cultura de seguridad de la comunidad politécnica y escasas medidas para precautelar su integridad.

Por lo expuesto, es urgente el estudio y adopción de medidas de seguridad que permitan detectar y eliminar las actividades irregulares en el Campus Politécnico de la ESPE-Sangolquí.

La implementación del sistema de video vigilancia inalámbrica y control de accesos, cumplirá la función de supervisar a través de las cámaras de video el sector perimetral de la ESPE, parqueaderos y las entradas principales de este centro educativo, con tecnología de punta, con lo que se dispondrá de información adecuada para coadyuvar la seguridad integral y que deberá ser complementada con respuesta humana.

Los accesos y zonas para desplazamiento peatonal, están cubiertas, señalizadas y bien definidas proporcionando una adecuada circulación y seguridad de las personas que transitan por las diferentes instalaciones de la universidad.

El estacionamiento de la ESPE está compuesto por varios parqueaderos en los diferentes bloques que la componen, con un total de 600 plazas de parqueo habilitadas, distribuidos en franjas laterales campus.

Se dispone de estacionamientos para áreas restringidas de uso exclusivo, áreas de contratos con terceros y de uso para clientes o visitantes de la ESPE.

La nueva zonificación de la figura 3.4, permitirá una mejor distribución del estacionamiento y administración del mismo en las horas de mayor afluencia de estudiantes y servidores públicos que es a las 07:00, 13:00 y 18:00

El horario establecido para el uso de los parqueadero es:

Lunes a Viernes de 06:00 hasta las 22:00
Sábados y Domingos de 06:00 hasta las 20:00

La capacidad de los estacionamientos para vehículos se satura únicamente en el sector para visitantes, en las horas pico de 07:00 a 13:00.

Las vías de ingreso y el perímetro de circulación vehicular que tiene el campus, constan de dos carriles bidireccionales, para un mayor flujo de los automotores.

Existen siete diferentes tipos de usuarios de parqueadero:

1. Estudiantes regulares (pregrado)
2. Estudiantes irregulares (postgrados, cursos, seminarios, charlas)
3. Docentes
4. Administrativos
5. Visitantes
6. Proveedores
7. Servidores públicos

En el campus de la ESPE Sangolquí el movimiento de personas está conformada en su totalidad por:

- Personal Militar: 250 personas.
- Personal Administrativo: 480 personas.
- Personal Docente: 600 personas
- Alumnos diurnos y nocturnos: 7000 personas.
- Posgrados: 400 alumnos.
- Estudiantes a distancia: 2000.

3.2 Descripción De Los Sistemas Disponibles.

La Escuela Politécnica del Ejército ESPE, actualmente no dispone de un sistema de seguridad integrada, en vista que el personal militar es quien

realiza físicamente el control de las instalaciones y de las personas que ellos laboran o estudian, resultado de lo cual no se tiene una respuesta rápida y efectiva a los acontecimientos emergentes, por la falta de personal que realiza la guardia para cubrir todas las edificaciones que dispone la universidad, a pesar de que el edificio administrativo cuenta con sistemas electrónicos de control, no se dispone de un centro de control y monitoreo centralizado.

Figura 52 Distribución De Edificaciones Espe- Sangolquí

Por no disponer la ESPE de un Sistema Integrado de Seguridad se han detectado varios inconvenientes y necesidades tales como:

- La ESPE no contribuye eficazmente al desarrollo del valle de los chillos, por los varios accidentes que se han suscitado en la comunidad politécnica, basado en la deficiente educación en valores y por la falta de atención a las necesidades integrales de la comunidad universitaria.

- Reducida integración de la ESPE con los gobiernos seccionales del cantón Rumiñahui, debido a la escasa confianza en la institución por

la débil seguridad y control, ya que no existe un sistema de circulación y aparcamientos para vehículos de forma adecuada.

- No existe un control de registro e identificación vehicular tanto en el ingreso como a la salida y en el interior del perímetro del campus politécnico.

- Utilización indiscriminada de los parqueaderos, ya que los controles que se realizan son obsoletos, limitada vigilancia física y no se dispone de un lugar para el acceso de vehículos para visitas.

- El ingreso de vehículos es el mismo para todos, en vista de que se tiene un insuficiente control y seguridad en el ingreso y salida de personal de la ESPE y particulares

- No existe control de ingreso y registro e identificación de las personas.

- No existen pasos cubiertos para ingreso de personal desde la autopista

- No existe sistema de control de ingreso de armas o explosivos

- Ausencia de control y seguridad en las áreas administrativas y académicas

- Presencia de ventas informales en interior de áreas académicas, administrativas y junto a la prevención.

- Áreas de atención a estudiantes y particulares vulnera la seguridad

- No existen normas de seguridad, planes de evacuación antes desastre naturales y contraincendios en áreas académicas y administrativas

- No existen normas de uso de las instalaciones administrativas y académicas.

- Los servicios universitarios no satisfacen las aspiraciones de la comunidad politécnica tales como: papelería, librería, farmacia, etc.

- Servicios de bar sin normas de salubridad

- Proceso de recolección de basura no se cumple

- Reducido apoyo de las autoridades del cantón Rumiñahui para optimizar la seguridad y control en la ESPE, ya que se ha detectado venta de licor en negocios ubicados frente a la ESPE, lo que ha ocasionado accidentes al cruzar la autopista

- No se dispone de un sistema de seguridad politécnico modernizado.

- No existe un organismo donde se centralice la seguridad y control de la ESPE

- No existe un circuito cerrado de televisión para monitoreo y control.

- Sistema de iluminación no está integrado con la seguridad de la ESPE

- Normas de seguridad industrial y salud ocupacional no han sido implementadas

3.3 Análisis De Los Servicios Y Necesidades De Las Instalaciones

La Universidad de Fuerzas Armadas-ESPE es una institución de educación superior, con personería jurídica, autonomía administrativa y patrimonio propio, de derecho público, con domicilio en la ciudad de Quito, y sede principal en la ciudad de Sangolquí; se rige por la Constitución de la República, la Ley de Educación Superior, su Ley Constitutiva Decreto Nº.

2029, publicado en el Registro Oficial Nº 487 del 20 de diciembre de 1977, otras leyes conexas, el estatuto, los reglamentos internos expedidos de

acuerdo con la ley y por normas emitidas por sus órganos de administración y autoridades.

En la Universidad de Fuerzas Armadas-ESPE, los estudiantes y usuarios son las personas más importantes a quien servir y satisfacer, cumpliendo con lo que se ofrecen y en los plazos establecidos, mejorando permanentemente todos los procesos académicos y administrativos.

La exigencia académica, el bienestar y la seguridad de todos quienes conforman la comunidad universitaria, el respeto al medio ambiente son prioridades, para que dentro de un marco de principios y valores, desarrollar una Cultura de Calidad Institucional.

La Universidad de Fuerzas Armadas-ESPE, es un sistema con áreas de gestión estratégicas de conformidad con los preceptos establecidos en la Constitución Política de la República, la Ley de Educación Superior, su

Reglamento y el Estatuto vigente, los cuales se integran para cumplir con la misión de la Universidad Ecuatoriana y con el Plan Estratégico.

Dentro de estas áreas de gestión tenemos la de GESTIÓN DE SEGURIDAD INTEGRAL, cuya finalidad es la de implementar una serie de medidas preventivas para proteger a las personas y los bienes de la comunidad politécnica, ante posibles riesgos laborables, patrimoniales o riesgos medioambientales.

Es importante considerar los campos de acción de la seguridad integral, los mismos que se orientan a:

- Seguridad Física.
- Seguridad de Documentos.
- Seguridad de Personal.
- Seguridad de Transportes.
- Seguridad Computacional.

- Salud Ocupacional.
- Prevención de Accidentes

Para mantener la seguridad de los diferentes campos de acción, es necesario contratar los servicios de una empresa que proporcione el equipamiento, requerimientos técnicos y operacionales necesarios para implementar, administrar, operar, gestionar, mantener y actualizar un sistema electrónico integrado de control de accesos y CCTV para el campus Sangolquí, el mismo que permita prevenir acciones delincuenciales que atenten a la seguridad de las personas y bienes de la comunidad politécnica.

Figura 53 Acceso Principal ESPE- Sangolquí

El conjunto de acciones que proponga la Universidad de Fuerzas Armadas-ESPE debe permitir cumplir adecuadamente con los procesos planteados para la implementación y ejecución exitosa del sistema electrónico de control de accesos de acuerdo a la normativa legal vigente.

Los servicios y sistemas que deben ponerse en funcionamiento, así como las conexiones y actividades administrativas, que se encargará de desarrolla la Oficina de Seguridad de la ESPE, se enmarcará en normas y estándares técnicos (ISO 9000, 27000) así como en el Reglamento de Contratación Pública establecido por el Instituto Nacional de Contratación Pública INCOP.

Un sistema Integral de seguridad, tiene como objetivo brindar una seguridad total de las instalaciones, reducción del tiempo de respuesta ante un evento, reducción del costo y la minimización de los errores en el mismo.

SEGURIDAD TOTAL.- Debido a que se contará con Circuito cerrado de Televisión (CCTV), control de Accesos, Alarmas de Intrusión y Rondas de

Guardia; en cada una de las instalaciones que conforman el Campus Politécnico.

REDUCCIÓN DEL TIEMPO DE RESPUESTA ANTE UN EVENTO.- Un sistema de seguridad electrónico al no tener necesidades biológicas y fisiológicas como comer, dormir, descansar etc., elimina por completo la pérdida de tiempo al estar funcionando sin descanso alguno.

REDUCCIÓN DEL COSTO.- Gracias a que un sistema Integral de Seguridad para edificios brinda un control centralizada de los equipos que conforman el sistema de seguridad de todas las instalaciones del edificio, se necesita contratar un menor número de personas para el manejo del mismo y por consiguiente una reducción del costo sistema de seguridad.

MINIMIZACIÓN DE ERRORES.- Al implementar los equipos electrónicos que conforma el Sistema Integral de Seguridad, se prescindirá de una menor intervención por parte del hombre, lo que conlleva a que se minimicen en forma considerable los errores que se producen con la sola acción humana.

Figura 54 Mejora De Procesos

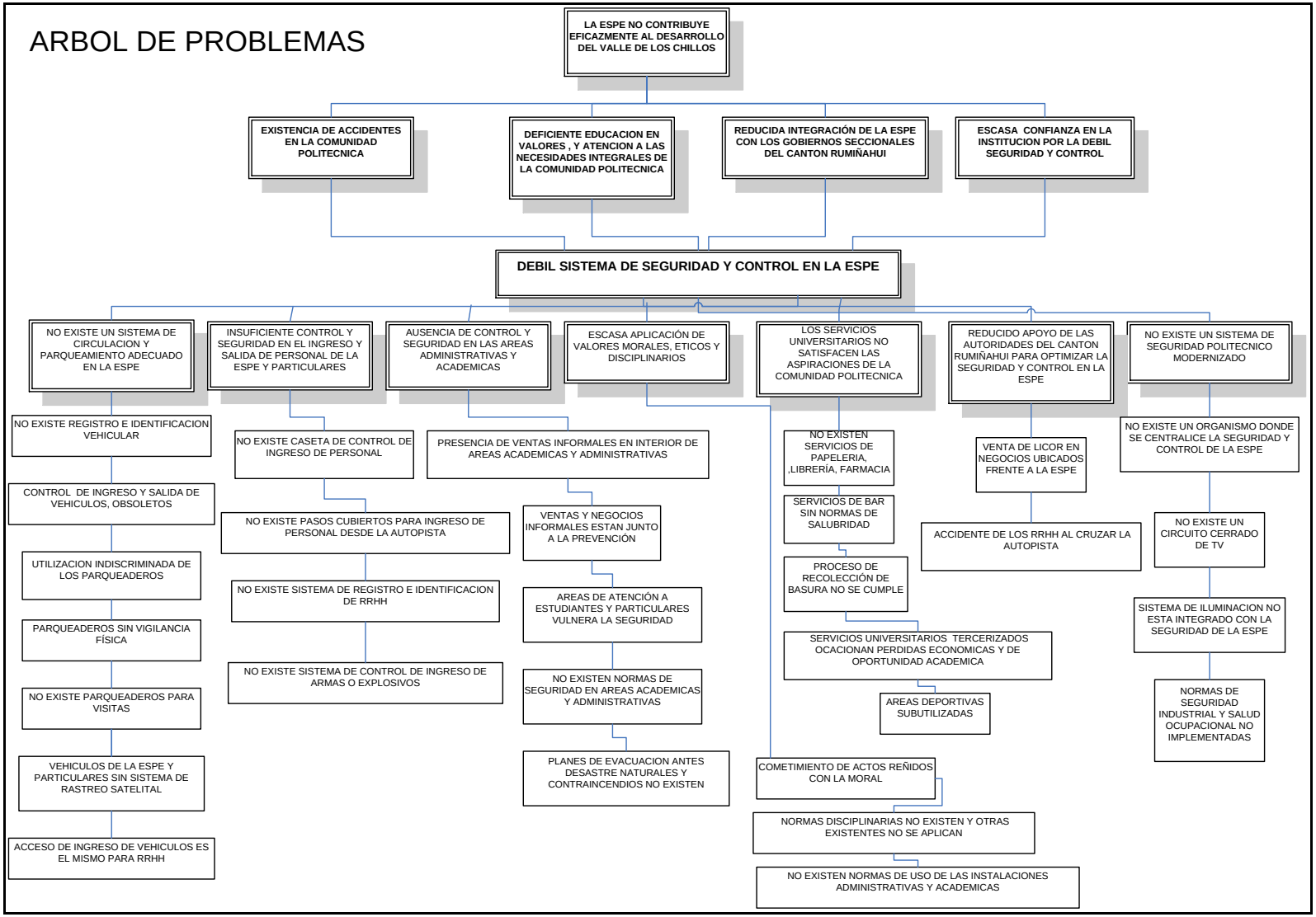

Figura 55 Árbol De Problemas ESPE-Sangolquí

Mediante el análisis del árbol de problemas que actualmente tiene la ESPE, al no contar con un Sistema Integrado de Seguridad se desprende que se debe:

Disponer de la más alta tecnología de CCTV Inalámbrico, para tener la información en tiempo real de las actividades rutinarias que se efectúan las 24 horas del día en la ESPE.

Contar con una herramienta de apoyo para la seguridad y disponer de información antes, durante y después de cualquier evento que pueda suscitarse al interior de la institución.

Para cubrir esta necesidad se torna sumamente necesaria la adquisición del hardware y software adecuado para implementar el CCTV Inalámbrico en el Campus Politécnico de la ESPE-Sangolquí.

Promover la conciencia de seguridad en la comunidad Politécnica, integrando la tecnología inalámbrica de CCTV de monitoreo y la respuesta humana a las actividades desarrolladas en el campus de la ESPE.

El impacto que se espera es permitir que la ESPE, como centro de educación de élite, esté a la vanguardia en la seguridad, salvaguardando los recursos humanos y materiales que conforman el Campus Politécnico de la ESPE-Sangolquí lo que permita un mejor desarrollo del estudiante y de la institución.

En la actualidad existen diferentes mecanismos de seguridad que se han ido implementando según las necesidades de cada persona, empresa e institución, teniendo una evolución muy significativa en la actualidad, de tal manera que la tecnología permite automatizar la gran mayoría de procesos

que requerían del cuidado y supervisión de una persona "llamada Guardia", el mismo que debe cuidar y precautelar la

integridad de la Institución. Hoy en día la ingeniería ha proporcionado herramientas útiles de seguridad electrónica que ayudan a mantener el orden y la integridad de la empresa.

Entre los diferentes elementos de seguridad utilizados por las empresas son los de video vigilancia y monitoreo satelital.

Optimizar el uso de los espacios físicos disponibles del parqueadero, para lograr una mejor circulación vehicular y peatonal, cumpliendo con las normas técnicas de manejo de parqueaderos de tal forma que exista:

- Parqueadero para visitas.
- Parqueadero para docentes
- Parqueadero para servidores públicos.
- Parqueadero para personal directivo
- Parqueadero para estudiantes.

Figura 56 Parqueaderos Frontales Espe-Sangolquí

Para de esta forma brindar un excelente servicio a los usuarios (personal administrativo, docentes, residentes, estudiantes, proveedores y demás visitantes) de los parqueaderos con personal calificado.

Administrar los vehículos que ingresan a los parqueaderos, mejorando la infraestructura instalada, con tecnología actual, mediante la implementación de un software para el control de vehículos y personas, ocupando eficientemente las diferentes áreas del Campus.

Proporcionar seguridad a los vehículos parqueados y facilitar un seguro contra todo riesgo para los mismos, mientras se encuentren dentro de la ESPE.

Integrar el sistema de accesos vehicular con el sistema de seguridad a instalarse en la Universidad de Fuerzas Armadas-ESPE, mejorando los estándares de calidad, nivel de servicio que vayan en concordancia con la imagen corporativa de la universidad.

Entregar a los usuarios del servicio, una constancia física del tiempo y valor cobrado por el servicio prestado, a la salida del parqueadero de visitas.

Auto sustentarse mediante el tarifado por la ocupación del espacio en el parqueadero de visitas, mediante un sistema de control, que permita el cobro justo de la hora o fracción, para satisfacer las necesidades de los diferentes usuarios, brindando un servicio de excelencia a un precio justo.

Operación eficiente del sistema de parqueo mediante equipos computarizados, que permitan activar un mecanismo de control al servicio del personal administrativo, directivo, militar, docentes y estudiantes.

Implementación de tarjetas inteligentes para las personas que ocupen el parqueadero de visitas, mediante la emisión de tickets con la información de fecha, hora, tiempo transcurrido: además se debe contar con la asistencia personal de así requerirlo, lo que permitirá usar eficientemente los espacios y controlar los vehículos en forma técnica.

Contra automatizado de entrada y salida de los vehículos mediante el uso de tarjetas inteligentes y tickets según sea el caso, logrando seguridad y ahorro de tiempo para el usuario en la manipulación automática de las barras.

Mantener registros estadísticos del flujo vehicular y del personal que ingresa/sale del campus universitario, mediante un sistema computarizado de control de parqueadero, acorde a la necesidad de información generada mediante archivos de los movimientos, los mismos que estarán disponibles para consulta o impresión y que deberán ser proporcionados por el departamento de seguridad de la institución para su supervisión y auditora de forma mensual.

Figura 57 Parqueadero Edificio Administrativo Espe-Sangolquí

Mantener y operar el servicio de parqueadero, con equipos de última tecnología y de marca reconocida a nivel mundial y nacional.

Mantener una señalización de las vías internas del Campus, tanto horizontal como vertical, cumpliendo con normas técnicas y los estándares de calidad.

El avance de la tecnología exige que la institución cuente con un sistema avanzado en comunicación, monitoreo y vigilancia, más aun siendo uno de los centros de educación superior más importantes del Ecuador.Por la ubicación geográfica del Campus Politécnico de la ESPE-Sangolquí, las vulnerabilidades y amenazas a su seguridad aumentan considerablemente.

En el Campus Politécnico de la ESPE-Sangolquí, existe recursos humanos y materiales muy valiosos, por lo que se cree indispensable precautelar la integridad, tranquilidad y seguridad, tanto de: autoridades, estudiantes, público en general. Por otra parte, en sus instalaciones, bodegas, aulas, auditorios, coliseo y los diversos equipos que existe en los laboratorios, estructurados en el sistema educativo de la ESPE, mismos que son indispensables para su funcionamiento del centro de educación superior.

Por lo que es indispensable implementar este proyecto de "SEGURIDAD INTEGRAL", que comprende la instalación de un sistema de seguridad inalámbrica, con tecnología de punta, acorde a la moderna arquitectura de control del circuito cerrado de televisión (CCTV-inalámbrica).

CAPITULO 4

ESTUDIO Y DISEÑO DEL SISTEMA DE COMUNICACIONES DEL CIRCUITO CERRADO DE TELEVISIÓN Y CONTROL DE ACCESOS DEL CAMPUS ESPE-SANGOLQUI

4.1 Arquitectura Del Sistema

Para el diseño de seguridad electrónica en la ESPE se lo realizó mediante el estudio de factibilidad para implementar un circuito cerrado de televisión IP, aprovechando la red de datos y para ello se consideró los puntos más vulnerables de accesos a la Institución (accesos frontal y posterior).

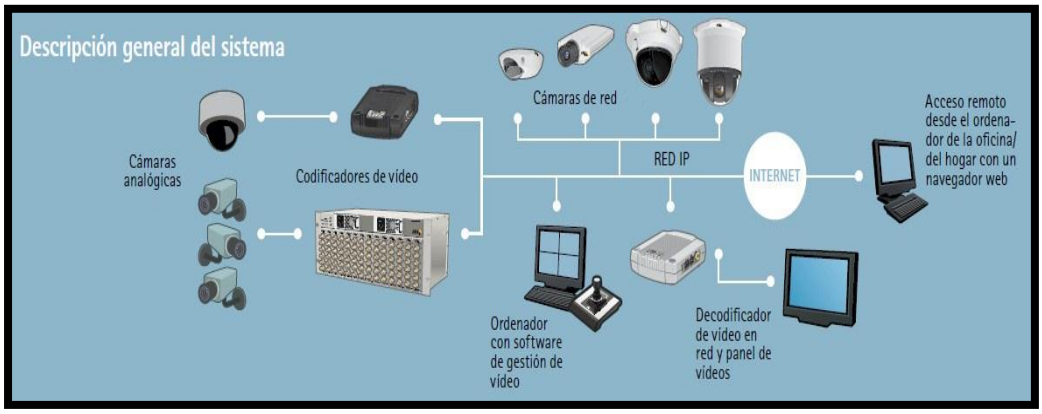

Figura 58 Descripción General Sistema Cctv

Cualquier evento producido en las áreas de influencia será captado por una cámara de video tipo domo PTZ (movimiento horizontal de 360º y vertical desde +2º hasta -90º y acercamiento) que serán consideradas para

el área perimetral, y los accesos, al igual que los parqueaderos de vehículos con cámaras fijas de tecnología IP.

Figura 59 Áreas De Influencia De La Espe Para El Cctv

Las cámaras PTZ serán del tipo analógicas, cuya señal de video y datos serán conectados a un interfaz que convertirá la señal analógica de video y la señal de control, a una señal digital (IP).

La señal digital de cada cámara será transmitida de forma inalámbrica hacía un equipo receptor de señales digitales ubicado en la terraza del edificio administrativo en una torre de 10 metros de altura. Luego esta señal digital IP será dirigida a un switch de red y de aquí al servidor de grabación de video, la visualización será en las estaciones o monitores.

El centro de control o monitoreo de este sistema estará ubicado en el mezanine del edificio administrativo.

Figura 60 Centro De Control Cctv - Espe

El sistema contempla el uso de equipos con función de servidor de grabación dedicada al almacenamiento de las señales de video IP, así como de matriz virtual. El proyecto contempla 19 cámaras de las cuales 11 son del tipo PTZ y 8 son fijas, 17 dispondrán de encoders inalámbricos, y se ha establecido 4 celdas para la cobertura en todo el campus dispuestas de acuerdo a la tabla 46

Tabla 1

Distribución Cámaras Por Sectores En El Campus ESPE

Celda 1	Celda 2	Celda 3	Celda 4
Cámara 6	Cámara 12	Cámara 16	Cámara 3
Cámara 7	Cámara 13	Cámara 17	Cámara 4
Cámara 8	Cámara 14	Cámara 1	Cámara 5
Cámara 9	Cámara 15	Cámara 2	
Cámara 10			

La distribución de las cámaras y las zonas**,** se muestra en la Figura 4.1, las cámaras 18 y 19 serán instaladas por medio de cable, dada la cercanía hacia el centro de control.

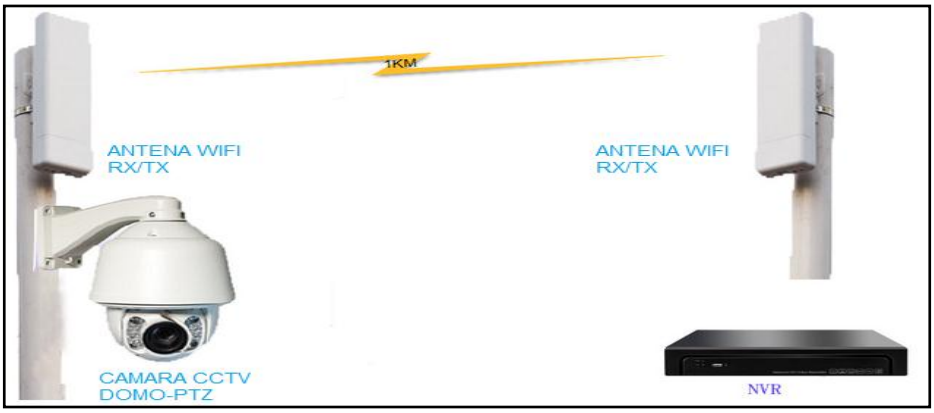

Figura 61 Cámara CCTV Inalámbrica

ANTENA RECEPTORA: Será un arreglo de antenas sectoriales Wifi de 120° cada una, que permitirá captar la señal de las diferentes cámaras y se encontrará ubicada en la torre metálica ubicada en la terraza del edificio administrativo.

Figura 62 Arreglo Antenas Sectoriales Wifi

C1.- Es del tipo fija, permitirá la visualización del ingreso vehicular, hacia el centro educativo, por la parte ESTE del Campus de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

C2.- Es del tipo fija, permitirá la visualización del ingreso al parqueadero ubicado en la parte ESTE del Campus Politécnico de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

C3.- Es del tipo fija, permitirá la visualización del parqueadero ubicado en la parte ESTE del Campus de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

C4.- Es del tipo PTZ, permitirá la visualización del Centro de Investigaciones Tecnológicas, Centro Medico, Ingreso a la Biblioteca, y perímetro en la parte NorEste del Campus de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

C5.- Es del tipo PTZ, permitirá la visualización de los laboratorios de Electrónica, Postgrados y perímetro en la parte NorOste del Campus Politécnico de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

C6.- Es del tipo PTZ, permitirá la visualización de los laboratorios de Mecánica, Geográfica, Gasolinera y perímetro en la parte NorOste del Campus Politécnico de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

C7.- Es del tipo PTZ, permitirá la visualización del parqueadero ubicado en el Bar del Campus Politécnico de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

C8.- Es del tipo PTZ, permitirá la visualización del ingreso por la parte Oste y estadio del Campus Politécnico de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

C9.- Es del tipo fija, permitirá la visualización del ingreso vehicular, hacia el centro educativo, por la parte OSTE del Campus de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

C10.- Es del tipo fija, permitirá la visualización de la salida vehicular, del centro educativo, por la parte SurOste del Campus de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

C11.- Es del tipo PTZ, permitirá la visualización del ingreso a los talleres, estadio y perimetro por la parte SurEste del Campus de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

C12.- Es del tipo PTZ, permitirá la visualización de los talleres y autocentro, por la parte Sur del Campus de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

C13.- Es del tipo PTZ, permitirá la visualización del Coliseo, canchas de voley y tennis, por la parte SurEste del Campus de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

C14.- Es del tipo PTZ, permitirá la visualización de la residencia, comedor, coliseo y parqueaderos, por la parte Este del Campus de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

C15.- Es del tipo PTZ, permitirá la visualización del Material Belico, por la parte Sur del Campus de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

C16.- Es del tipo fija, permitirá la visualización de la salida vehicular, del centro educativo, por la parte Este del Campus de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

C17.- Es del tipo fija, permitirá la visualización del ingreso peatonal, hacia el centro educativo, por la parte ESTE del Campus de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

C18.- Es del tipo PTZ, permitirá la visualización del sector ESTE del Campus de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

C19.- Es del tipo PTZ, permitirá la visualización del sector ESTE del Campus de la Escuela Politécnica del Ejercito (ESPE-Sangolquí).

La ubicación de cada una de las cámaras ha sido concebida y diseñada en función de las actividades que se desarrollan en el Campus de la Escuela Politécnica del Ejercito (ESPE-Sangolquí), estarán colocadas en los postes de alumbrado eléctrico de sector perimetral, en los accesos principales mediante brazos y en los parqueaderos en postes de sujeción.

Para este proyecto se utilizarán cámaras de video analógicas PTZ y cámaras fijas de tecnología IP.

Las cámaras de video fijas IP, tipo profesional tendrán un rango dinámico mayor a 100dB, a color, con lente auto iris varifocales, para cubrir un área específica y las cámaras tipo domo análogas, a color, con la función PTZ,(Pan/Tilt/Zoom), para cubrir un área específica. Además se utilizará un controlador, para el manejo y configuración de las funciones PTZ. Los dos tipos de cámaras deben tener la función día/noche, con características para ser ubicadas en el exterior y deben cumplir las normas nema 4X o IP67.

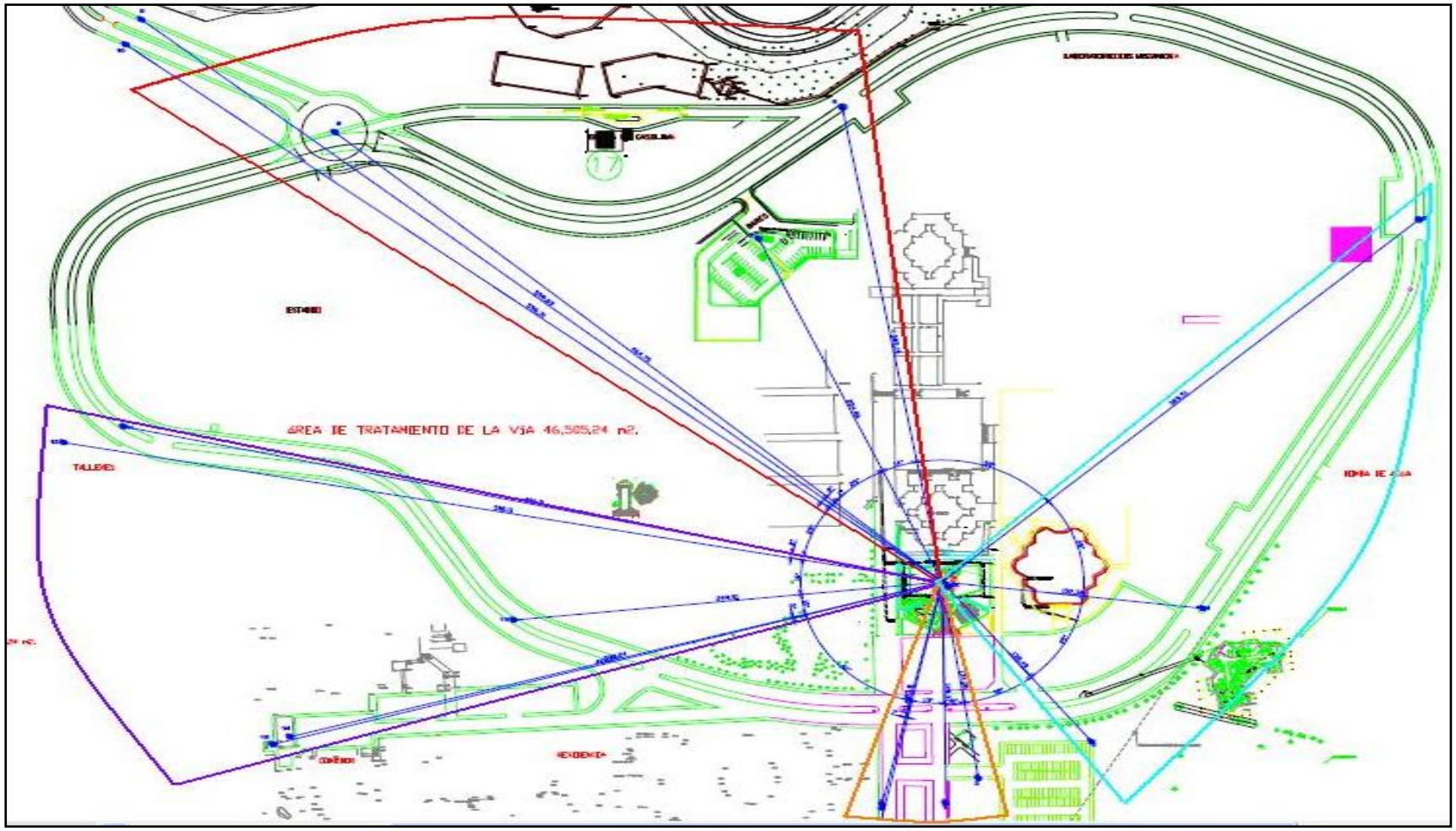

Figura 63 Distribución Cámaras Por Sectores En El Campus ESPE

Figura 64 Cámara IP CCTV

Sistema De Transmisión De La Señal De Video

Se ha considerado que la transmisión de las señales de video y datos de las cámaras PTZ, se lo realice de forma inalámbrica, utilizando enlaces de radio diseñados para transmisión de señales de video IP, dentro de los estándares 802.11a y 802.11g, que utilizan las bandas de frecuencia de 5 GHz y 2.4 GHz.

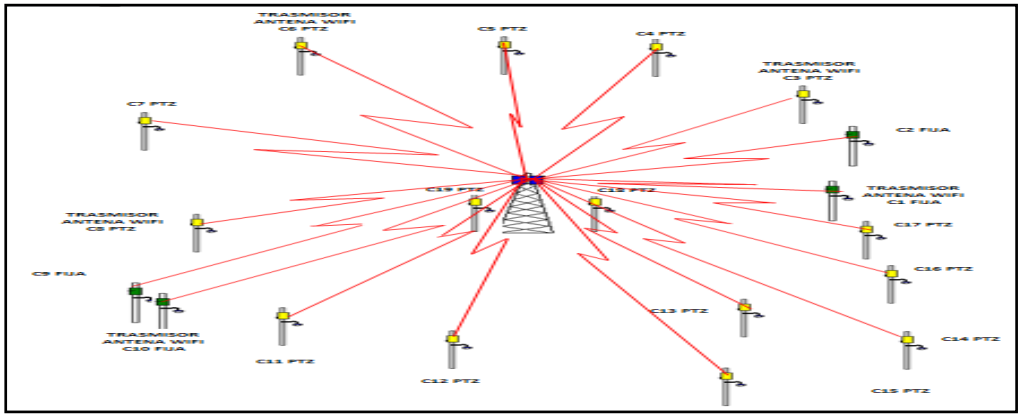

Figura 65 Enlaces Wifi Cámaras Por Sectores En El Campus Espe

4.2.1 Equipo Utilizado Para La Transmisión De Video

Para integrar la señal de video, proveniente de la cámara de video analógica a la Red TCP/IP, se utiliza un equipo denominado VIDEO SERVER, el mismo que cumple las funciones de digitalizar la señal de video, la comprime y luego la adapta a la Red, para su respectiva transmisión a través de esta red.

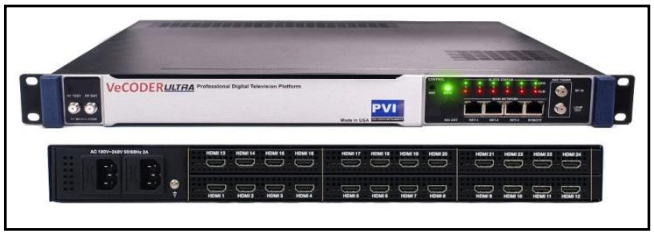

Figura 66 Iptv Encoder De 24 Canales

El Video Server además, de transmitir la señal de video por la red TCP/IP transmite datos y con opción de tener señales de alarma. La transmisión de datos se utiliza para controlar remotamente las cámaras PTZ (Pan /Tilt/ Zoom), para lo cual disponen de un puerto serial RS-232/RS-485; y las señales de alarma, para realizar una conexión automática con la estación remota cuando exista alguna emergencia.

De preferencia, en los sistemas de transmisión inalámbricos de video seguridad, se puede disponer de equipos integrados en una sola unidad el video server y el transmisor.

El sistema de recepción inalámbrico será basado en AP Access Point, que podrán configurarse punto a punto o multipunto. Los equipos deben estar equipados con calidad de servicio, por especificación directa del fabricante.

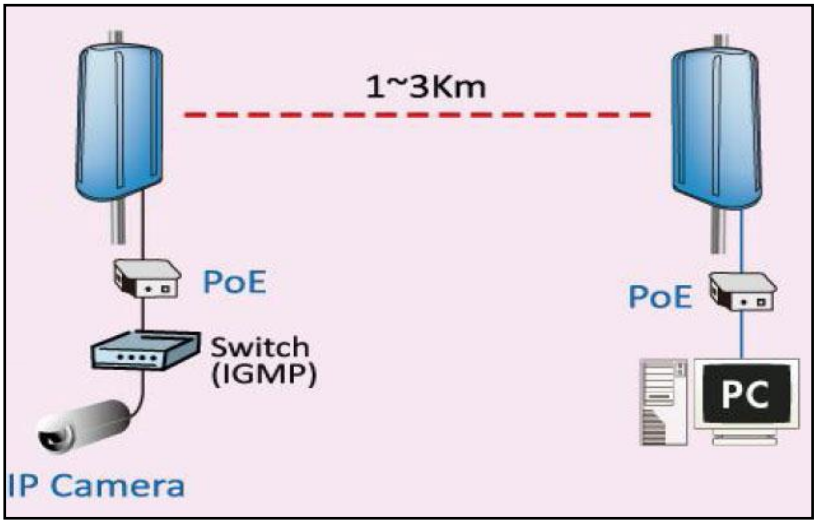

Figura 67 Acces Point CCTV

Las señales de video IP digital son conducidas al Sistema de Grabación de Video Digital IP, para su almacenamiento y visualización. Estas señales serán observadas en monitores dedicados para este fin.

4.2.2. Sistema De Transmisión De Las Señales De Video Y Datos

Las cámaras de video que se utilizarán en este proyecto, serán cámaras analógicas para las PTZ y de tecnología IP para las fijas. En el caso de las cámaras PTZ, sus señales de video y datos deberán ser convertidas a señales IP, para poder transmitirlas. En el lado de recepción de las señales (Estación Base), estas señales serán recolectadas por Access Points de Uso Exterior.

Para transmitir las señales de video y datos de las cámaras de video tipo Domo PTZ, se ha determinado realizarlo de forma inalámbrica.

Se utilizará un sistema de enlaces punto-multipunto para todas las cámaras tipo Domo PTZ, con lo cual se tendrá mayor disponibilidad de ancho de banda para la transmisión de las señales de video y datos. De acuerdo con el cuadro anterior de la celdas de video.

Se debe utilizar equipos de radio multibanda, optimizados para transmisión que trabajen en la banda de frecuencia de 2.4 GHz y 5,8 GHz, estándar 802.11 a y 802.11g, lo que flexibiliza la configuración para escapar de posibles fuentes de interferencias externas, que afecten el funcionamiento del sistema de CCTV proyectado.

Los enlaces inalámbricos serán instalados desde cada una las posiciones de ubicación de las cámaras de video, hacia una estación base, en donde se instalarán los equipos de recepción de las señales.

Se debe considerar que las antenas que se utilizarán para realizar los respectivos enlaces, cuya instalación debe cumplir con los márgenes de seguridad en la transmisión mantener libre la zona de Fresnel, cumpliendo de esta manera con la línea de vista, garantizando el funcionamiento del enlace.

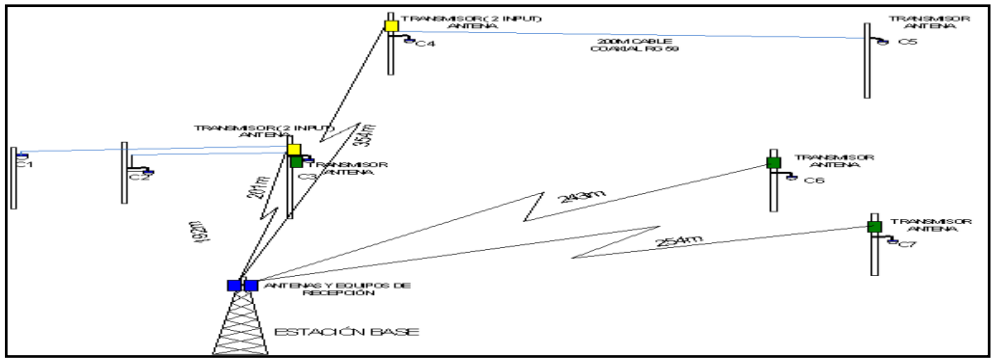

Figura 68 Enlaces Inalámbricos Con Margen De Seguridad

Para el montaje de los equipos de transmisión y de las cámaras de video, se utilizará los postes ya existentes en el sector perimetral del Campus, esto a una altura de 10 metros para obtener enlaces con línea de vista hacia el acces point colocado en la torre del edificio administrativo.

Los equipos de recepción (Estación Base), serán montados sobre la terraza del centro de monitoreo (edificio de administración).

Las señales de red IP obtenidas en la Estación Base, serán conducidas por medio de los cables correspondientes, por el interior del edificio administrativo, a través de tubería EMT y por los ductos dispuestos para las instalaciones eléctricas, existentes en el Centro de Monitoreo, de la misma forma se debe canalizar los cables de acometida eléctrica que utilizarán los equipos de recepción.

Las unidades podrán tener sus respectivas antenas integradas, con la posibilidad de conexión a diferentes tipos de antenas, según los requerimientos de cada enlace.

Para disminuir la posibilidad de interferencia entre canales, se recomienda configurar los enlaces con canales no adyacentes en las bandas de frecuencias de 2,4 ó 5,8 GHz.

A continuación se presenta un ejemplo de configuración de los canales a utilizarse en los enlaces inalámbricos. Además, de las 11 cámaras tipo Domo PTZ, se ha considerado la instalación de 8 cámaras fijas IP, que serán montadas con soportes de acuerdo con la FIGURA 57

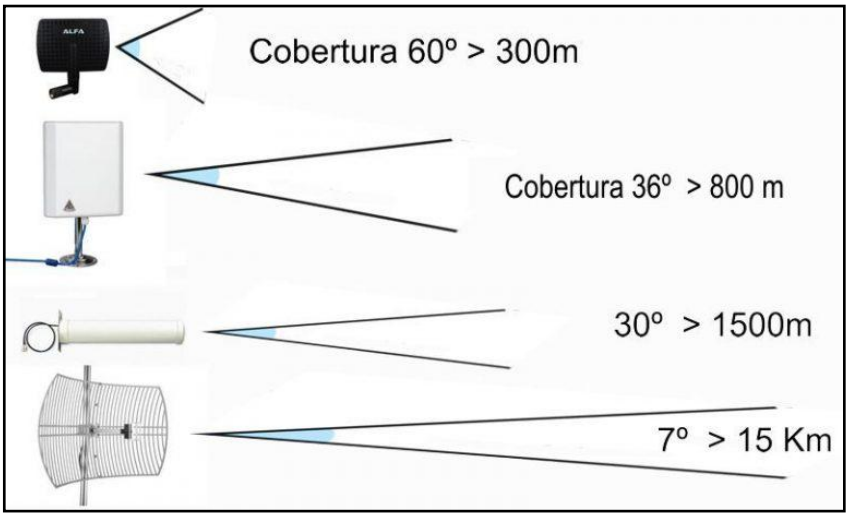

Figura 69 Antenas Wifi

4.2 Diseño Y Cobertura Del Sistema

El estudio y diseño del proyecto se realizó tomando en cuenta las diferentes problemáticas existentes en el Campus de la ESPE en Sangolquí, al no tener implementado un sistema integrado de seguridad y en vista que el crecimiento de este establecimiento educativo ha sido vertiginoso, lo que conlleva a que en cada período de clases se incremente la oferta académica y por ende las carreras, estudiantes, profesores, servidores públicos, laboratorios, equipos y en fin todo lo que engloba un sistema educativo de categoría A.

Partiendo de estas premisas, se ha considerado para el desarrollo del diseño del sistema de CCTV y acceso perimetral de la ESPE,

como punto inicial de partida, los sitios de ingresos y salidas de vehículos y personas, siendo estos los siguientes:

Acceso/salida Principal – Sector Este – Av. General Rumiñahui

Este acceso contará con dos carriles para ingreso/salida de vehículos para personal administrativo, servidores públicos y estudiantes presenciales, así como también de dos carriles para ingreso/salida al parqueadero de visitas, estos ingresos y parqueo de visitas serán monitoreados con cámaras fijas y controlados por vallas de gestión vehicular.

Figura 70 Acceso/Salida Principal Vehicular ESPE

El ingreso/salida de peatones se controlará mediante molinetes (torniquetes), los mismos que serán accionados mediante el carnet o identificación acreditada por la universidad y monitoreados por una cámara fija.

Figura 71 Acceso/Salida Peatonal ESPE

Acceso/salida Secundario – Sector Oeste – Paseo San Luis

Este acceso contará con dos carriles tanto para ingreso como para salida de vehículos para personal administrativo, servidores públicos y estudiantes presenciales, por este sector no se autoriza el ingreso de visitas ni vehicular ni peatonal, será monitoreado con cámaras fijas y controlados por vallas de gestión vehicular.

Las cámaras a utilizarse serán tipo DOMO, de grabación continua mediante activación interna y externa, serán comandadas mediante el software adecuado, conectadas a un servidor de video ya sea a través de cable coaxial o fibra óptica, dependiendo de las distancias donde se encuentren instaladas cada una de ellas, la señal de video analógica será inyectara a la red Ethernet en forma de paquetes IP, las secuencias de video serán almacenadas en los grabadores de video en red (NVR).

Con capacidad de almacenar todos los acontecimientos ocurridos durante las 24 horas del día y por el tiempo determinado por los administradores del sistema, los servidores estarán instalados en el mezzanine del edificio administrativo.

4.3.1 Especificaciones Generales.

El sistema CCTV estará conformado principalmente por cámaras IP, servidor o grabador de video en red (NVR), estaciones de trabajo y pantallas de monitoreo.

El sistema de CCTV estará compuesto por las siguientes cámaras:

- Cinco (5) cámaras PTZ IP resolución 1280 X 960 pixeles, compresión H.264 y MPEG -4, preparadas para exteriores (IP66) y zoom de 18 X.

- Tres (3) cámaras PTZ IP resolución de 768 x 496 pixeles, compresión H.264 y MPEG -4, preparadas para exteriores (IP66) y zoom de 23 X.

- Una (3) cámara PTZ IP resolución de 768 x 496 pixeles, compresión H.264 y MPEG -4, preparadas para exteriores (IP66) y zoom de 35 X.

- Dos (2) cámaras fijas infrarrojas resolución 976 x 494 pixeles, lente varifocal de 6 – 50 mm, preparadas para exteriores IP66. Iluminación IR por los menos de 40 m

- Dos (2) cámaras fijas infrarrojas resolución 976 x 494 pixeles, lente varifocal de 4 – 12 mm, preparadas para exteriores IP66. Iluminación IR por los menos de 20 m

- Cuatro (4) cámaras fijas día /noche con resolución 800 x 600 pixeles, lente varifocal de 2.8-12 mm, preparadas para exteriores IP 66. Iluminación mínima 0,05 lux (monocromático).

Todas las señales de video y control de las cámaras serán enviadas a través de una red TCP/IP hacia los servidores de video, por tal motivo si se presenta una cámara análoga se deberá considerar codificadores de video. Las señales deberán ser direccionadas al servidor o NVR ubicado una en el EDIFICIO ADMINISTRATIVO el mismo que se encargará de administrar toda la data del sistema CCTV, incluyendo el manejo de las grabaciones de video, por lo que éste deberá contar con características específicas para esta función, con una capacidad de almacenamiento de por lo menos 4TB:

Cámaras PTZ deberán grabar a su mayor resolución a 15 imágenes por segundo durante 16 horas (6 am- 10 pm), en la noche se deberá programarlas para que se activen mediante movimiento, manteniéndose las condiciones de grabación continua.

Las Cámaras Fijas Infrarrojas deberán realizar laa grabación continua durante las 24 horas del día a su máxima resolución a 15 imágenes por segundo.

4.3 Control De Accesos Al Campus Espe – Sangolquí

El sistema de control de accesos tiene como finalidad registrar, monitorear y controlar el ingreso y salida de personas; también considera el monitoreo y registro de intrusión no deseada.

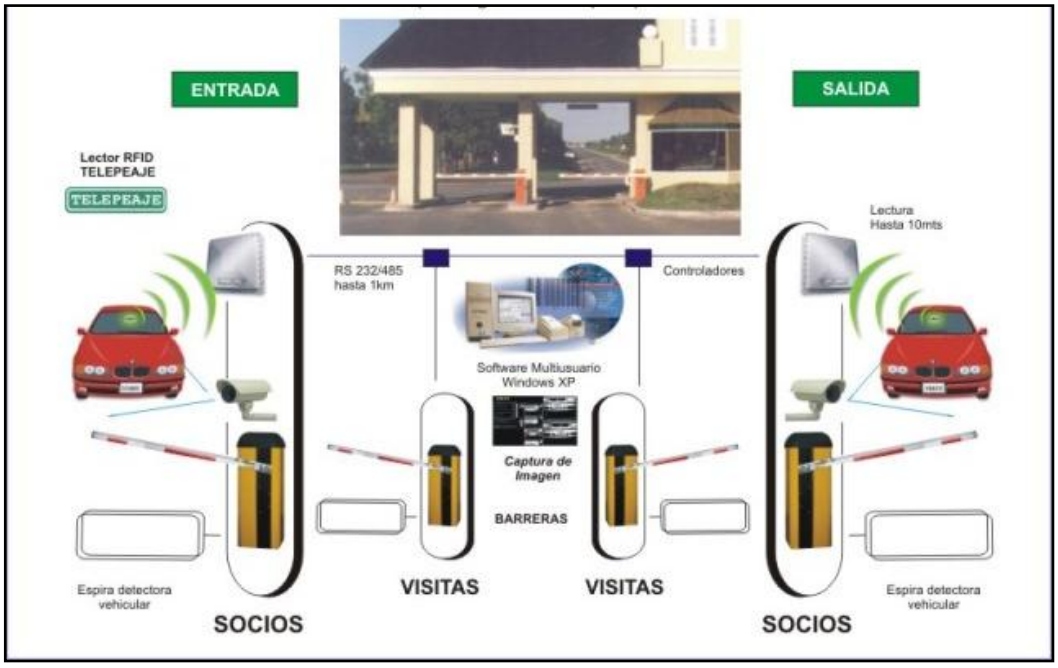

Figura 72 Configuración Control De Acceso Vehicular

El sistema de control de accesos estará conformado por tarjetas de acceso, lectores de tarjetas en combinación con molinetes (torniquetes) para el control de ingreso/salida de personas, controladores y un servidor/estación de control dedicado para este sistema.

Las tarjetas de acceso serán entregados a todo el personal autorizado de la universidad, mediante lectores se debe enviar la información a los controladores para permitir o denegar el acceso a la institución. Los datos se enviarán y almacenarán en un servidor a través de un protocolo TCP/IP u otro protocolo estándar.

El servidor dedicado al sistema de control de accesos debe mantener toda la información configurada en una base de datos, el cual se ubicara en el edificio administrativo, MEZANINE.

La Base de datos del sistema de control de accesos deberá exportarse desde bases existentes en la ESPE, por lo tanto deben estar constituidas mediante estándares abiertos y la posibilidad de conexión a través de ODBC.

Con la finalidad de un correcta administración y monitoreo de los sistemas de control de accesos y circuito cerrado de televisión, deben integrarse en una plataforma, la cual este concebida con estándares abiertos como XML, HTML, MODBUS, BACnet, etc.

El software de integración debe partir del sistema de control de accesos, es decir el hardware debe ser de la misma marca del sistema de control de accesos y CCTV deben ser compatibles con el sistema de integración.

CONTROL DE ACCESOS: El sistema de control de accesos estará enfocado principalmente a cubrir los accesos peatonales, para lo cual se requiere la instalación de molinetes/torniquetes en las garita principal y prevención, el sistema deberá permitir el acceso o salida de usuarios de la universidad a través de tarjetas inteligentes.

Como complemento del sistema de control de accesos se deberá instalar un sistema de CCTV que permita la vigilancia de ingresos y salidas tanto de personas como vehículos.

Figura 73 Acceso Peatonal ESPE

GARITA PRINCIPAL: se deberá realizar la instalación de 4 torniquetes /molinetes para personas sin discapacidad y 1 carril para personas con discapacidad, además se deberá incluir dos cámaras para la vigilancia de estas áreas. También se deberá incluir 1 cámara de vigilancia por carril vehicular que permita tener una visón de la parte frontal del vehículo tanto para entradas como para salidas, es decir 4 cámaras.

Figura 74 Acceso Vehicular Y Peatonal ESPE

PREVENCIÓN: se deberá realizar la instalación de torniquetes/molinetes 3 para la mayor cantidad de personas y 1 carril para personas con capacidades diferentes, además se deberá incluir dos cámaras para la vigilancia en estas áreas.

También se deberá incluir 1 cámara de vigilancia por carril vehicular lo que permita tener una visión de la parte frontal del vehículo tanto para entradas como para salidas, es decir 6 cámaras, ya que en esta área existen dos carriles bi-direccionales.

Se deberá considerar que la ESPE dispondrá de hilos de fibra óptica en la garita principal y prevención para lo cual se deberá instalar switch de la

misma marca de equipos que al momento posee la ESPE. La comunicación de las cámaras perimetrales se deberá realizar mediante una comunicación inalámbrica, para lo cual la ESPE proveerá de puertos disponibles en los switchs ubicados en: EDIFICIO CENTRAL, EDIFICIOS DE POSTGRADOS, RESIDENCIA POLITECNICA. Además para las cámaras FIJAS IR se tendrá puertos disponibles en MATERIAL BELICO y AUTOCENTRO. Se deberá proveer los switchs necesarios de acuerdo al diseño, la cantidad de puertos necesarios sobrepasa a los existentes.

Se considerará los puntos eléctricos necesarios para el correcto funcionamiento de los equipos de control de accesos y CCTV, para lo cual la ESPE permitirá la interconexión a la red eléctrica interna mediante los tableros de distribución más cercanos a estos sitios y /o la disponibilidad de puntos eléctricos en edificios.

4.4.1 Detalle Del Equipamiento Básico Para El Control De Los Parqueadero

La implementación de un sistema automatizado de parqueadero (Tag o llave en mano) que brinde seguridad, servicio y organice las áreas de parqueo con tecnología de punta debe cumplir con los siguientes parámetros:

Equipos, infraestructura eléctrica y de comunicación necesaria para el sistema de automatización de parqueaderos de visitas y personal de comunidad universitaria

Operación eficiente del sistema de parqueo mediante un sistema computarizado instalado, activados con un mecanismo de control que será: para el personal administrativo, directivo, militar, docentes y estudiantes,

tarjetas inteligentes, para las personas que ocupen el parqueadero de visitas mediante, la emisión de tickets con la información de fecha, hora, tiempo transcurrido además se debe contar con la ayuda de personal de logístico, lo que permitirá usar eficientemente los espacios y dejar los vehículos en forma organizada.

Control automatizado de entrada y salida de los vehículos mediante el uso de tarjetas inteligentes y tickets según sea el caso logrando segundad en la manipulación automática de las barras.

Mantener registros estadísticos del flujo vehicular mediante un sistema computarizado de control de parqueadero de acuerdo a la necesidad de información de los eventos que se susciten, donde los archivos de consulta o impresión deberán ser proporcionados a la institución para su control y auditoría.

Mantener y operar el servicio de parqueadero con equipos de última tecnología, con marcas reconocidas a nivel mundial y nacional.

Mantener una señalización de las vías internas del Campus, tanto horizontal como vertical, cumpliendo con normas técnicas y considerando los estándares de calidad, en concordancia con el manual de imagen corporativa de la universidad, para ello el proveedor presentará los diseños que se someterán a su aprobación por parte del administrador, previo a su instalación.

El Horarios de movimiento vehicular y peatonal en el interior del Campus universitario es: Lunes a viernes 06h00 hasta 22h00 y sábados, domingos y feriados 06h00 a 20h00.

El contratista debe proporcionar seguridad física, personal y contra terceros a través de una póliza de seguros contra todo riesgo. El oferente debe asumir todos los costos directos e indirectos; los costos fijos, incluidos impuestos referentes a la actividad, retenciones de ley e imprevistos y utilidades.Para la correcta administración del estacionamiento se deberá mantener un número de personal mínimo de 13 personas.

ACCESO DE VISTAS.- El usuario ocasional que llega al Campus Politécnico de la Escuela Politécnica del Ejercito (ESPE-Sangolquí), oprime el botón, toma el ticket e ingresa en el parking. El usuario abonado ingresa acercando la tarjeta transponder al lector de proximidad.

FORMA DE PAGO: El usuario entrega el ticket en la caja manual deslocalizada. El sistema calcula el costo por hora de parqueo, y el operador devuelve el ticket timbrado.

SALIDA DEL PARQUEO VEHICULAR PARA VISITAS: El usuario ocasional acerca el ticket timbrado en el lector óptico de la estación de salida y la valla se activa permitiendo la salida del vehículo. El usuario abonado sale acercando la tarjeta transponder al lector de proximidad.

SISTEMA S-04: Configuración adaptada a la gestión de parking con pago a través de una caja manual con operador, parking con múltiples entradas y salida.

Figura 75 Punto Pago Parqueadero

4.3.2 Configuracion Del Sitema S-04

El sistema debe poseer los siguientes elementos para su normal funcionamiento:

- Estación MOOVI 30 S
- Easy park ET plus
- Estación de entrada
- Botón para el ticket
- Impresora y emisor del ticket
- Detector Espira magnética Bi-canal
- Lector de proximidad
- Pantalla y síntesis vocal
- Citófono
- Espiras magnéticas
- Easy park scanner
- Estación de salida
- Lector óptico del ticket
- Detector espira bi-canal
- Lector di proximidad
- Pantalla y síntesis vocal
- Citófono
- Easy cash top
- Caja manual
- Computadora personal
- Lector óptico de mesa
- Impresora recibos
- Pantalla de cortesía
- Citófono (opcional)

4.3.3 Ingreso Vehicular Mediante Telepass De Largo Alcance

Una alternativa para descongestionar y permitir el acceso/salida al Campus Universitario de los vehículos hacia los diferentes parqueaderos alrededor del perímetro, es el telepeaje de largo alcance el mismo que debe constar de un telepass y un transponder

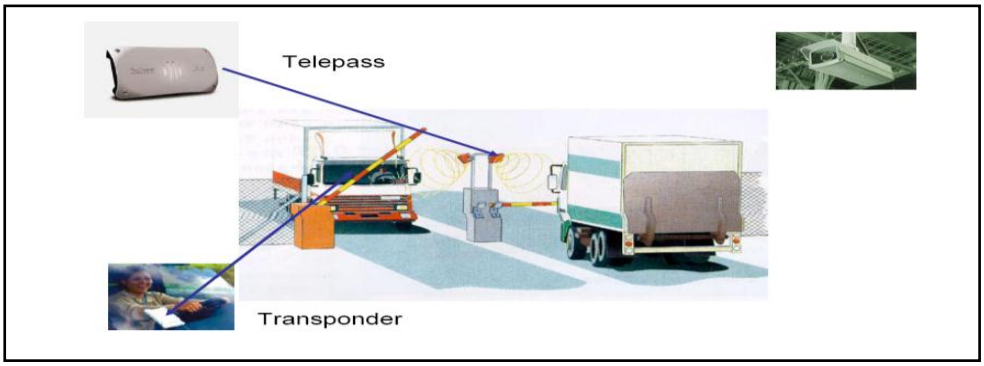

Figura 76 Esquema Telepeaje Acceso Vehicular

4.4.2 Reconocimiento De Matriculas Para Control De Acceso Vehicular.

Es una tecnología de reconocimiento visual que permite detectar, localizar e identificar el vehículo por el número de matrícula, complementándose con lectores de proximidad mediante tarjetas RFID para controlar y restringir el acceso, en función de días de la semana, franjas horarias, etc.

Figura 77 Software Reconocimiento De Matricula Vehicular

DESCRIPCIÓN DEL SISTEMA: Debe poseer los siguientes componentes para su normal funcionamiento:

UNIDA DE LECTURA CAMARA REF. CCD-PK: carcasa óptica y soporte, proporciona imágenes de las matrículas de los vehículos mediante la unidad de identificación IM-PK para su proceso.

UNIDA DE IDENTIFICACION IM-PK: Ordenador integrado donde se procesa las imágenes recibidas de la unidad de lectura, extrae los caracteres alfanuméricos de la matrícula y los transmite a través de la unidad de control de gestión y cobro del parking al sistema emisor de tickets.

Está conformada por:

- Unidad de control CA-PK controlador CA4-K.
- Lector de proximidad telepass

Cuando el lazo inductivo detecta la presencia de un vehículo se activa el sistema de reconocimiento de matrícula.

La entrada de imágenes al sistema de reconocimiento de matrícula se realiza normalmente mediante una señal de vídeo estándar por una cámara CCD. Las imágenes son transmitidas a la unidad de control CA-PK, normalmente una señal de vídeo estándar (PAL/NTSC). Esta señal de vídeo es recibida y digitalizada por un dispositivo de captura de vídeo, que está instalado en la unidad de control CA-PK

En esta unidad CA-PK, el software de reconocimiento de imágenes procesará las imágenes digitalizadas. El proceso de reconocimiento de la matrícula de la imagen que se ha capturado es el siguiente:

– Se localiza la matrícula dentro de la imagen

- Se extrae el número de la matrícula localizada y se transforma en una imagen de tamaño uniforme. En un proceso de segmentación, se identifican los carácter es alfanuméricos.

– Los caracteres identificados son interpretados mediante un sistema de Reconocimiento Óptico de Caracteres

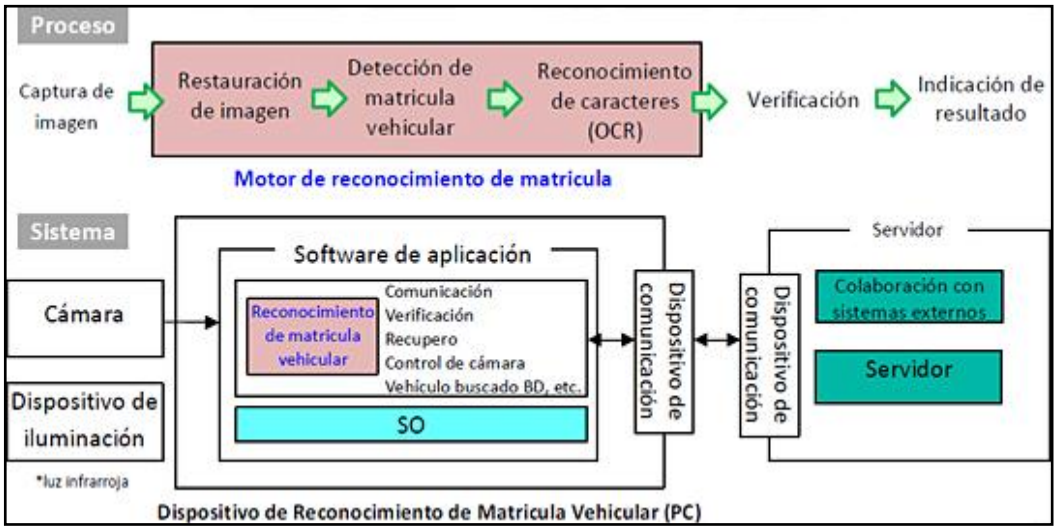

Figura 78 Reconocimiento De Matrícula Vehicular En Pc

El resultado de reconocimiento se transmite al controlador CA4 -K. Si al mismo tiempo que se detecta la presencia del vehículo, el usuario del mismo activa el lector de proximidad CI RPROX mediante el dispositivo que este posea (tarjeta o llavero proximidad), el lector enviará al controlador CA4-K un código correspondiente al usuario. Las dos tecnologías utilizadas al mismo tiempo, permiten opciones adecuadas a cada aplicación, como accesos permitidos o denegados por :

- Reconocimiento de matrícula o usuario

- Reconocimiento de matrícula y usuario

4.4 Red De Integración Del Sistema Del Cctv Y Control De Accesos En La Espe -Sangolquí.

Figura 79 Integración CCTV y Acceso Vehicular/Peatonal.

CENTRO DE MONITOREO: deberá ser implementado en el sitio construido para este fin, que estará ubicado en el mezanine del edificio administrativo.

Las señales de video digital IP obtenidas desde la Estación Base y de las cámaras fijas IP, ingresarán vía Ethernet IP 10/100 al switch de red. Así mismo se tendrá un Workstation para visualización con funciones de Servidor de grabación, la cual se conectara al switch de red vía Ethernet 1000 o Gigabit Ethernet.

Para la transmisión y recepción de datos de las funciones Pan/Tilt/Zoom de las cámaras tipo Domo, se utilizará un controlador que

utilice el Protocolo RS-485 y que disponga de un joystick, para controlar las funciones PTZ. En el Centro de Monitoreo deberá estar instalado las protecciones contra sobrevoltajes o interferencias que puedan ingresar a través de los diferentes cables.

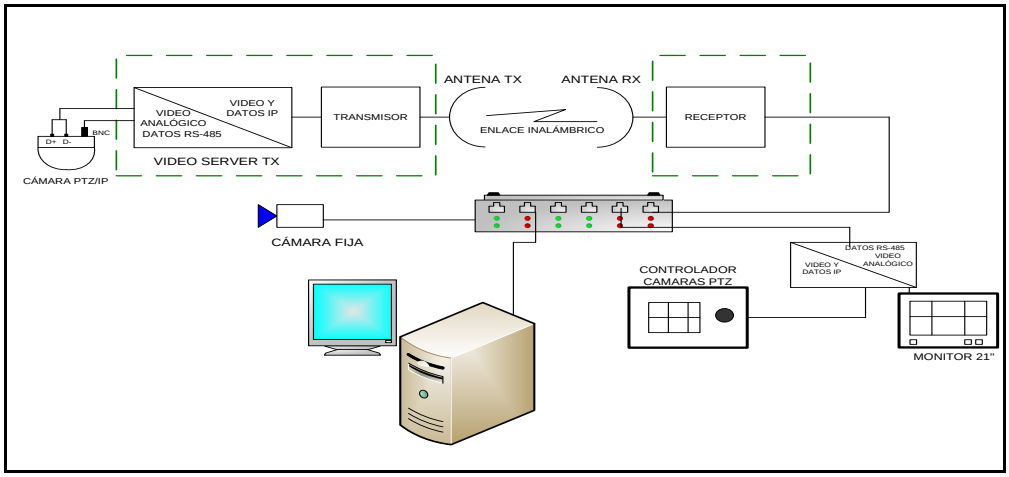

Figura 80 Integración De Sistemas CCTV

DESCRIPCIÓN DE LA RED: Los elementos de la conexión activa y pasiva con que cuenta la red de datos de la ESPE son los siguientes:

Un rack principal del cuarto de control, con todos sus elementos activos y pasivos distribuidos acorde al diseño de toda la red.

Figura 81 Rack Principal

RACK PRINCIPAL- CUARTO DE CONTROL: En la figura, elementos de rack principal, muestra como está organizado el sistema de comunicaciones con su respectivo switch, path panel, marca y número de puertos, con sus elementos:

- Distribución de Enlaces en Swich A- Swich B
- Puerto 45 en Switch B enlace cascada con Swich A.
- Convertidor de fibra servicio de Internet-Puerto 46 Swich B.
- Puerto 47 Swich B- Enlace cascada con puerto 9 SDF Administración.

RACK SECUNDARIO- CUARTO DE CONTROL.: En la figura el Gabinete - SDF se muestra la distribución de cada elemento que conforma la conexión y distribución en la sección primaria del Gabinete de Comunicaciones.

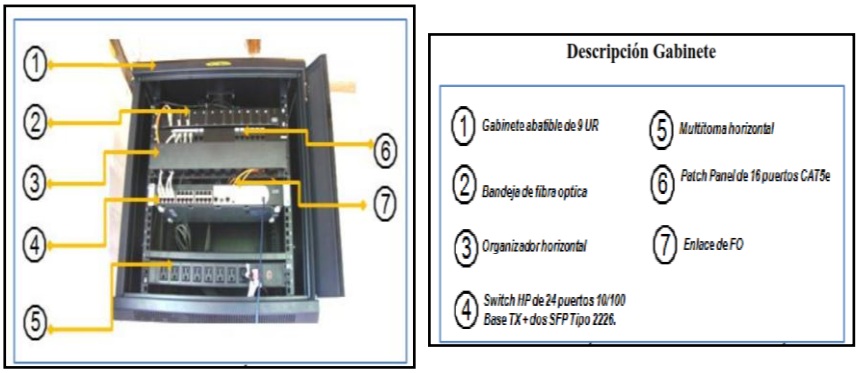

Figura 82 Rack Principal

Gabinete abatible de 9 U, la bandeja de fibra óptica el organizador horizontal, Switch HP de 24 puertos 10/100 base TX + dos SFP tipo 2226,

multitoma Horizontal, Path Panel de 16 Puertos Cat 5e. Enlace de fibra como se especifica en las normas de cableado estructurado norma ANSI/TIA/EIA 568-B.

A este rack se conectarán todas las cámaras del sistema CCTV y los equipos de control de acceso de la ESPE ya sea por fibra óptica o por cable UTP.

SISTEMA DE ALIMENTACIÓN DE 120 VAC Y PROTECCIONES ELÉCTRICAS : El Centro de monitoreo deberá contar con un sistema de energía ininterrumpida (UPS), regulada para la protección de los equipos del centro de monitoreo, las cámaras fijas y a los equipos de recepción instalados en la estación base.

Se deberá implementar un sistema de puesta a tierra, en el centro de monitoreo, para la protección de los equipos mencionados anteriormente.

Las acometidas eléctricas de 120 VAC para las fuentes de energía de las cámaras tipo Domo PTZ y los equipos de transmisión, serán proporcionadas por la administración de la Escuela Politécnica del Ejercito (ESPE-Sangolquí), en todos los sitios de instalación de las cámaras tipo Domo PTZ y en el centro de Monitoreo.

Se deberá contar en cada sitio de instalación de las cámaras PTZ y equipos de Transmisión de un UPS, el mismo que proporcione energía eléctrica a los equipos correspondientes. Además, en cada uno de estos sitios, se deberá instalar un sistema de puesta a tierra y las protecciones contra descargas atmosféricas, sobre voltajes, el mismo que permitirá tener una protección adecuada para las cámaras de video y equipos de transmisión.

Los UPS y fuentes de energía que utilicen las cámaras PTZ y equipos de transmisión/recepción, deberán ser instalados en cajas normalizadas para exteriores que cumplan con las especificaciones IP66.

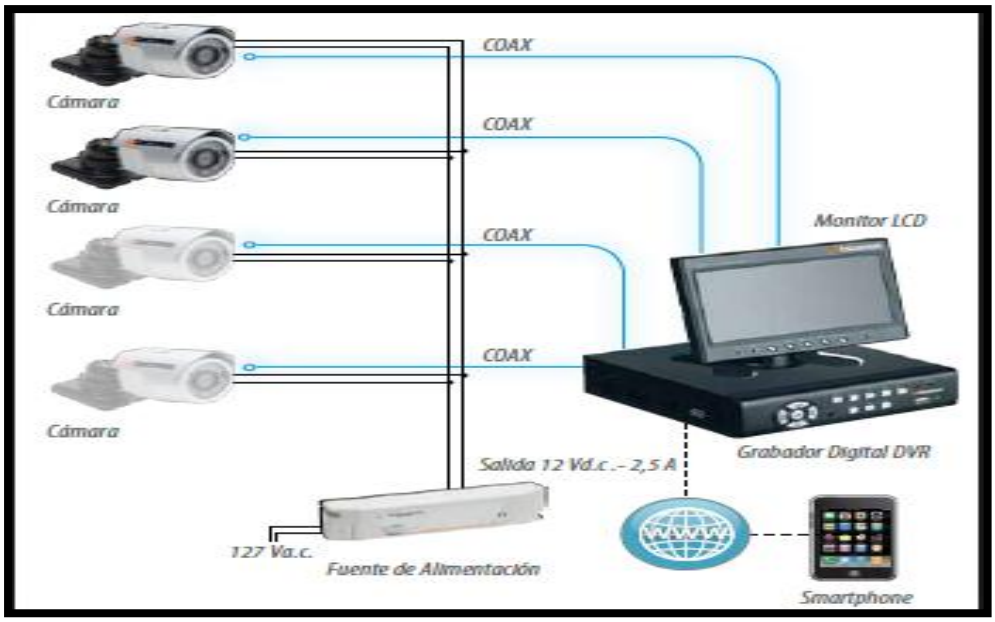

Figura 83 Respaldo De Energía Ups Para Cctv

CAPITULO 5

COSTOS DEL SISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN Y CONTROL DE ACCESOS

5.1 Bases Técnicas.

5.1.1 Generalidades

Los equipos y materiales utilizados deben ser componentes estandarizados, fabricados regularmente y de uso regular en el proceso de manufactura.

Los equipos y componentes ofrecidos deben tener cumplir normas RoHS.

La garantía de los equipos cubrirá la reparación o reemplazo de las unidades defectuosas por defectos de fabricación, por un periodo mínimo de dos años desde la fecha de despacho de la fábrica.

Especificaciones Del Sistema

El sistema de transmisión de video estará formado por unidades transmisoras y codificadoras de video inalámbrico y por unidades Puntos de Acceso.

Las unidades transmisoras y codificadoras de video inalámbrico deberá estar formado por una sola unidad:

Un transmisor inalámbrico, codificador de video con opción de análisis de video embebido, en un solo dispositivo. No se aceptaran soluciones formadas por dispositivos independientes que requieran el uso de cajas intemperie o de diferentes fabricantes.

Las unidades de Punto de Acceso tendrán la función de recibir una o múltiples unidades transmisoras y codificadoras de video inalámbrico, pasando las tramas de video a la red LAN, para que puedan ser recibidas por un sistema de administración de video IP o una unidad decodificadora de Video.

El sistema de transmisión de video, compuesto por unidades transmisoras y codificadoras de video inalámbrico y las unidades de punto de acceso, deberá permitir la transmisión de video, en tiempo real, sin retardo perceptible al ojo humano.

Deberá presentarse el plano con el diseño físico del sistema incluyendo ganancia de las antenas y ángulo de cobertura tanto en transmisores como receptores para su evaluación técnica.

5.1.2 Especificaciones Funcionales

El sistema transmisor deberá estar formado por una solución completa, incluyendo un transmisor inalámbrico y codificador de video como un solo dispositivo, con capacidad de transmitir audio, video, datos PTZ y alarmas, incluyendo el hardware necesario para estas funciones, como parte de la unidad. El retardo o latencia en el control PTZ no deberá ser superior a los 150ms.

Las unidades transmisoras y codificadoras de Video inalámbrico podrán ser instaladas en configuraciones Punto a Punto (PTP) o Punto Multipunto (PTM), y tener la capacidad de transportar sobre la misma portadora de microondas video, datos PTZ, audio y alarmas.

Las unidades transmisoras y codificadoras de Video inalámbrico deberá tener capacidad de operación multibanda, en las bandas de uso libre de 2.4 y 5GHz así como en la banda de seguridad ciudadana de 4.9GHz.

Las unidades transmisoras y codificadoras de Video inalámbrico deberán incluir protecciones internas contra transciendes eléctricos en todas las entradas y salidas de señales de video, datos PTZ, audio y alarmas.

Las unidades transmisoras y codificadoras de Video inalámbrico deberán incluir como opción, análisis de video embebido, con capacidad de detección de modificación de Imagen (Camera Tampering). El análisis del video debe efectuarse en el dispositivo, de modo que se utilice más eficientemente la red y los dispositivos de almacenamiento. Dentro de la funcionalidad de tampering el sistema deberá estar en capacidad de detectar Escenas fuera de Foco.

Las unidades transmisoras y codificadoras de Video inalámbrico deberán manejar el estándar de codificación de Video MPEG-4 y/o un protocolo basado en MPEG-4, con capacidad de manejar flujos de imágenes con resolución de 4CIF/30Fps ante todas las condiciones de movimiento de la imagen.

Adicionalmente, las unidades transmisoras y codificadoras de Video inalámbrico deberán tener la capacidad de manejar MJPEG a una resolución

mínima de 4CIF/15fps bajo todas las condiciones de movimiento de la imagen.

Las unidades transmisoras y codificadoras de Video inalámbrico deben permitir la selección de la resolución de video desde formato (352 x

240 pixels para NTSC, 352 x 288 pixels para PAL) hasta 4CIF (704 x 480 pixels para NTSC, 704 x 576 pixels para PAL).

Las unidades deben ser compatibles tanto para cámaras en formato PAL como NTSC.

El firmware de las unidades, incluyendo el codificador de video (Video Codec), deberá poder ser actualizado con una conexión local o remota, por medio de un programa de emulación de terminal, utilizando interface de comandos, o por medio de un programa con interfaz de usuario grafica. El firmware deberá permitir la configuración remota de todas las funciones de la unidad (Video, comunicación inalámbrica, puertos de comunicación, etc).

Las unidades deberán poder ser configuradas y accesadas vía Internet Explorer 5.0, Internet Explorer 6.0 o un navegador de características similares. El video en las unidades transmisoras y codificadoras de video Inalámbrico podrá también ser visualizado por este medio.

Las unidades deberán poseer una interface CLI para configuración adicional a la del literal anterior.

5.1.3 Especificaciones Del Radio

Las unidades del sistema inalámbrico deberán soportar el estándar 802.11a y 802.11g, con un protocolo de capa física que garantice enlaces de video confiables y proporcione solución al problema de nodo oculto, con modulación OFDM.

Las unidades transmisoras y codificadoras de Video inalámbrico deberán soportar un segundo modo opcional que soporte el estándar WiFi

IEEE 802.11a y 802.11g con WEP/WPA2, de modo que provea interoperabilidad con nodos WiFi.

Las unidades transmisoras y codificadoras de video inalámbrico deberán soportar un ancho de banda efectivo (Throughput) de hasta 28 Mbps. La Unidad de punto de Acceso deberá permitir una conexión de hasta 24 unidades.

Las unidades transmisoras y codificadoras de video inalámbrico deberán incluir una antena tri-banda embebida, que permita la operación en las bandas no licenciadas de 2.4 y 5GHz, así como en la banda seguridad publica de 4.9 GHz, sin necesidad de cambios de Hardware. La selección de la banda de operación deberá efectuarse en el software de configuración del dispositivo.

Adicional a la antena embebida, tanto las unidades transmisoras y codificadoras de video inalámbrico como las unidades de punto de acceso, deberán tener un puerto RF que permita la conexión de una antena externa de diferente ganancia, que permita flexibilizar el diseño e instalación.

Las unidades transmisoras y codificadoras de video inalámbrico y las Unidades de Punto de Acceso deberán soportar encriptación utilizando estándares AES 128-bit, con rotación automática de clave (Auto-key Rotation), WPA2 y WEP.

5.1.4 Especificaciones Físicas

Las unidades transmisoras y codificadoras de video inalámbrico y las Unidades de Punto de Acceso deberán estar diseñadas como una sola unidad resistente a la intemperie, que cumpla la norma NEMA 4X/IP66

Las conexiones de Video, datos, alarma, potencia, audio y Puerto de Red (Ethernet) en la unidades transmisoras y codificadoras de video inalámbrico y las Unidades de Punto de Acceso deberán poseer protección intemperie NEMA 4X/IP 66 mediante conectores industriales que cumplan esta normatividad.

Las unidades del sistema inalámbrico deberán incluir un sistema de sujeción estandarizado, que permita sujeción de los dispositivos en mástiles de diferentes diámetros, así como la fijación en poste o en pared, cambiando la configuración del mismo herraje de sujeción.

Las unidades no deberán requerir el uso de sistemas de calefacción o refrigeración externos, tales como calentadores o ventiladores, ni el uso de cajas intemperie de ningún tipo para la ubicación de los equipos.

5.2 Especificaciones De Los Dispositivos De Captura Video

5.2.1 Especificaciones Del Sistema

El sistema de captura de video estará formado por cámaras fijas y cámaras móviles (no del tipo domo), mismas que deberán permitir una visualización nocturna en sitios que carecen de iluminación o poseen una iluminación muy tenue.

5.2.3 Especificaciones Fisicas Y Funcionales

Las unidades deben permitir la visualización o grabación de vídeo en la noche en blanco y negro y el día a color, deberán permitir visualizar a una iluminación 0 luxes por lo que es indispensable tengan un sistema infrarrojo de iluminación embebido ya sea en la cámara o su chasis.

Las cámaras fijas y móviles deberán poseer tanto desempañador como limpiador y tener una certificación NEMA / IP66.

Las cámaras PTZ deberán permitir un giro de 360 grados a alta velocidad y un acercamiento de mínimo 100 mts, deben permitir la creación de mascaras de privacidad mediante el menú propio de la cámara y la grabación de mínimo 128 posiciones.

Tanto las cámaras fijas como móviles deben tener una garantía mínima de 1 año y poseer todos los dispositivos para montaje tanto en pared como en poste.

Se debe considerar un teclado para el manejo de las cámaras mismo que será conectado a la matriz virtual mediante un codificador de red.

5.2.4 Especificaciones De Sistema De Respaldo De Energía

El sistema de respaldo de energía será compuesto por un UPS en cada una de las cámaras que nos ofrezca tanto respaldo como regulación del voltaje.

5.2.5 Especificaciones Físicas Y Funcionales

El ups que se coloca en cada una de las cámaras debe ser de 1 KVA en línea, con respaldo de 7 minutos con el 100% de la carga, adicional su montaje deberá ser realizado en el posteo en cajas metálicas totalmente selladas para no permitir el paso de agua y deben poseer soporte para montaje en poste.

5.1 **REQUISITOS PARA LAS EMPRESAS A LICITAR**

a) Acreditar mediantes certificados otorgados por clientes una experiencia mínima de 10 años en Seguridad Electrónica.

b) Certificado de representación directa de fábrica de los equipos cotizados, no serán validos certificados de reventa.

c) Poseer al menos un técnico certificado por fábrica para La instalación y montaje de los equipos cotizados.

d) Poseer al menos un técnico certificado en switchs sean estos 3COM ò CISCO.

5.3 Especificaciones Tecnicas De Productos

CAMARA DE VIDEO TIPO DOMO PTZ

- Formato de TV: NTSC
- Luxes: 0
- Dispositivo de Imagen: 1/4 Sony CCD
- Capacidad: Día/ Noche / Infrarroja
- Pixeles efectivos: 752(H) X 582(V)
- Frecuencia de barrido: 15.73 KHz (H) y 59.94 KHz
- Sincronización: interna/externa
- Salida de video: 1.0 p-p/75 ohmios
- Relación señal/ruido: más de 48 dB (AGC desactivado).
- Resolución horizontal: 480 líneas de TV. (Color) y 570 (B&W)
- Distancia focal: 3.9 – 85.8 mm (zoom óptico 35X mínimo)
- Backligth Compensation
- Zoom Óptico: 18X
- Zoom Digital: 12X (total zoom 220X)
- Velocidad Focal máxima: gran angular 1: 1.6 Teleobjetivo1: 3.7
- Ángulo de cobertura: f=3.9 mm 51.26º (H) x 39.03º (V) F=85.8mm 2.39º (H) x 1.80º (V).
- Distancia mínima de enfoque: 1.0 metros (teleobjetivo) – 0.01 m (gran angular).
- Distancia máxima de enfoque: 200 metros
- Ángulo de rotación panorámica: 360º continuo
- Rotación panorámica: manual/programable.
- Velocidad panorámica: 0.5º por segundo a 125º por segundo.
- Ángulo de rotación de inclinación: de 0º a 90º
- Posición preconfigurada: 128 puntos
- Temperatura de funcionamiento: de -45ºC - 50ºC

- Humedad de funcionamiento: 20% - 95% (sin condensación).
- Protocolo: Propietario, Pelco P, Pelco D
- Marcara de Privacidad programable hasta 8 zonas
- Fuente de alimentación: 24 VAC + 10%
- Consumo de energía: 8 vatios en espera, 13 vatios en funcionamiento.

HOUSING PARA CÁMARA PTZ

- A prueba de agua: IP66
- Disponga de calentador y ventilador.
- Cubierta del domo: polycarbonato.
- Rango de temperatura de operación: -20º C a 50ºC.
- Humedad relativa: de 0 a 90%.
- Compatible con soportes para pared y poste.

CÁMARA DE VIDEO A COLOR TIPO PROFESIONAL

- Formato de TV: NTSC estándar.
- Dispositivo de Imagen: 1/3 Sony Super HAD CCD
- Capacidad: Día/Noche
- Resolución Horizontal: 540 líneas TVL
- Método de Control: OSD
- Número de Pixeles: 768(H) x 494(V).
- Escaneo de Imagen : 2:1
- Relación Señal/Ruido: mayor de 48 dB.
- Tipos de lentes: Lente de DC Auto-Iris, Vari focal, Infrarrojo
- Compresión de Video: MPEG-4, MPEG-4 ISO 14496-2, MJPEG
- Salida de Video: Video compuesto 1Vpp 75 Ohms. Conector BNC.
- Alimentación: 12 VDC
- Consumo de Energía: 5 W aproximadamente.

- Temperatura de Operación: -10ºC a 50ºC.
- Humedad de operación: 95% no condensada a 50 C

LENTE PARA CÁMARA DE VIDEO

- Lente Auto Iris
- Formato: 1/3”
- Tipo: Vari focal
- Longitud Focal: 2.9 a 8 mm
- AUTO IRIS DC
- Rango de temperatura de operación: -10ºC a 50ºC.

HOUSING PARA CÁMARA FIJA

- A prueba de agua: IP66.
- Inluminador Infrarojo embebido
- Heather a Blow
- Rango de temperatura de operación: -20º C a 50ºC.
- Humedad relativa: de 0 a 90%.
- Compatible con soportes para pared y poste.

EQUIPO DE RADIO FRECUENCIA

- El equipo de Radio Frecuencia debe ser considerado para trabajo en áreas exteriores, debe cumplir las siguientes especificaciones:

EQUIPO DE RECEPCION AP RF

- Bandas: Multibanda 2.4 GHz, 5.x GHz

- Frecuencia: 2.4 – 2.4835 GHz, 5.250 – 5.825 GHz.
- Estándares 802.11a/802.11g con MAC propietaria
- Modulación: OFDM.
- Distribuciòn: Stream Server a Doble Stream
- Alcance: 3.4 KM a 10 KM, con línea de vista.
- LED Indicadores: Estado, Actividad en Wireless y en LAN
- Seguridad: Encriptación AES 128 bits, SSL AUTENTIFICACION
- Celdas: Agrupación y protección por Clave
- Upgrade Firmaré: Vía Red
- Configuración: CLI, HTTP
- Resolución: 4 CIF a 30 FPS
- Protocolos: RTP/IP, UDP/IP, TCP/IP o Multicast IP
- Tipo de alimentación: POE (Power Over Ethernet)
- Salida Ethernet: RJ45 de Intemperie 10/100 BaseT
- Gabinete: NEMA 4X/IP66. OUTDOOR

EQUIPO DE TRANSMISION RF

- Bandas: Multibanda 2.4 GHz, 5.x GHz
- Frecuencia: 2.4 – 2.4835 GHz, 5.250 – 5.825 GHz.
- Estándares: 802.11a / 802.11g con MAC propietario
- Modulación: OFDM.
- Distribuciòn: Stream Server a Doble Stream

- Alcance: 3.4 KM a 10 KM, con línea de vista.
- Seguridad: Encriptaciòn AES 128 bits , SSL Autentificacion
- Celdas: Agrupación y protección por Clave
- Upgrade Firmaré: Vía Red

- Configuración: CLI, http
- Resolución: 4 CIF a 30 FPS
- Protocolos: RTP/IP, UDP/IP, TCP/IP o Multicast IP
- Puerto : RS485/RS422
- Voltaje de alimentación: DC Y AC
- Salida Ethernet: RJ45 de Intemperie 10/100 BaseT
- Gabinete: NEMA 4X/IP66.

PLATAFORMA de GRABACION DIGITAL IP

SERVIDOR

- Arquitectura Servidor
- Interface de Red: 10/ 100 /1000
- No debe estar basado en tarjetas capturadoras de video para PC
- Capacidad de administrar video streaming wired y wireless
- Capacidad de integración con productos de otras fabricas
- Disponible para plataforma Windows y Base de Datos MSDE y SQL 2005
- Formato de Compresion: MJPEG4 Propietario
- Modos de Grabación: Continua, por calendario, por evento (Movimiento, markup), por alarma (Analitica, entrada externa)
- Disco duro: 1.5 TByte
- Capacidad de expansión interna o externa RAID5
- Soporte de cámaras PTZ de diversos fabricantes
- Soporte de teclados de CCTV de diversos fabricantes

- Operación Simultánea: permita grabar video, ver video en vivo, ver video grabado, recibir notificaciones de alarmas, recibir notificaciones de alarma con imágenes y videos
- Capacidad de Matriz Virtual
- Web Server embebido
- Velocidad de grabación configurable cámara por cámara hasta 30 FPS.
- Salida de Video DVI
- Deteccion de Tampering de Camara

CLIENTE

- Multipantalla: 1, 4, 6, 9 y 16 canales.
- Permita obtener respaldo de grabación.
- Capacidad de funciones de búsqueda de imágenes por cámara, hora y fecha.
- Disponga de certificado digital para firmar los videos que son exportados.

ESPECIFICACIONES MINIMAS ESTACION de TRABAJO

- Sistema Operativo Windows XP SP2 Ingles o Windows Server 2003 R2
- Hardware
- CPU • Core 2 Duo/Quad @ 1.86 GHz or faster
- 2GB RAM
- 1 x 80GB boot drive
- Almacenamiento de Video
- x 500GB 7.2k HP SATA HDD storage drives
- DVD-ROM drive
- Embedded gigabit NIC

- Tarjeta de Video: High-end con 128 MB RAM, resolucion 1024 x 768 @ 32 bits color
- Incluye monitor de 21" o 22"

CONTROLADOR DE CÁMARAS PTZ

- Baud Rate (bps): Max 38400 bps.
-
- Control de PTZ: joystick (3 ejes).
- Auto supervisión: tour, grupo, swing, preset.
- Control remoto: RS-485/ RS422.
- Entrada de voltaje: 12 VDC.
- Consumo de energía: máx. 700 mA.
- Temperatura de operación: de 0º a 40º.
- Humedad relativa: 10% al 75%.
- Protocolo de Transimision: Pelco ASCII
- Método de transmisión: HALF DUPLEX/FULL DUPLEX.

VIDEO DECODER

- Compresión: MPEG-4.
- FPS: 1 – 30 fps programable
- Resolución: Escalable hasta 4CIF
- Formato de TV: NTSC.
- Salida: 1 entrada de video compuesto, 1 Vpp, 75 ohmios (NTSC).
- Puerto Serial: Auto-sensing RS-422/485, para conexión de teclados CCTV.
- Disponga de Alarmas de Entrada/salida .

SISTEMA DE ENERGÍA ININTERRUMPIDA (UPS) PARA CENTRO DE MONITOREO

- Voltaje: 120VAC
- Frecuencia: 50/60 Hz compatible.
- Capacidad mínima de salida en VA: 3000 VA

- Salida nominal de voltaje: 120V AC
- Salida de onda senoidal dentro de un 2% de 120V.
- Menos del 5% de distorsión armónica total.
- Promedio de vida de la batería típica: 3-6 años dependiendo del uso.
- Velocidad de recarga de la batería: 2-4 horas al 90%.
- Acondicionamiento de la línea de doble conversión en línea, que mantenga la salida dentro del 2% de 120 volts todo el tiempo.
- Corrección de sobrevoltaje: Mantenga una salida de 120V +/-2%, sin consumir la energía de la batería durante sobrevoltaje hasta 138V AC.
- Corrección a caídas de tensión: Mantenga una salida de 120V +/-2% durante bajas del voltaje a 85V AC.
- Corrección a caídas de tensión severas: A niveles de carga menores al 70%, el UPS mantenga una salida de 120V +/- 2% durante bajas de voltaje a 60V AC.
- LEDs indicadores: información del estado, energía de la línea, derivación, batería encendida, sobrecarga, batería baja, información del nivel de CARGA/ BATERIA (100%, 75%, 50%,25%).
- Alarmas: Alarma audible multi función que avise el arranque del UPS, operación de respaldo, advertencia de batería baja, sobrecarga, falla del UPS y apagado remoto.

SISTEMA DE ENERGÍA ININTERRUMPIDA (UPS) PARA SITIOS REMOTOS

- Capacidad minima: 600 VA.
- Regulación Automática de voltaje.
- Control por microprocesador.
- Digitalizado.
- Encendido en frío.
- Protección en corto circuitos y descargas.
- Autosensor de frecuencia 50/60 Hz.
- Almacenamiento de energía (UPS modo sleep) .
- Mínimo 4 tomas de salidas protegidas.

SWITCH

CONNECTORES

- Switch 24 puertos capa 3
- auto-negotiating 10BASE-T/
- 100BASE-TX ports configured as auto
- MDI/MDIX
- Soporte IGMP y Trafico Multicast
- Posibilidad de detección de Looping en los puertos.

PERFORMANCE

- Wirespeed performance across all ports
- Store-and-forward switching

5.4 Costos De Los Equipos.

Tabla 2
Subcontratos Y Servicios

ACTIVIDAD	COSTO
Obra Civil	USD. 3.000,00
Instalación tomas de 110 Vac. En postes	USD. 3.000,00
TOTAL:	**USD. 6.000,00**

Tabla 3
Equipos Instalación Y Configuración

ITEM	DESCRIPCIÓN	VALOR
01	CCTV Wireless para protección perimetral Radio/Grabación /Matriz	USD. 118.917,00
02	CCTV Wireless para protección perimetral Cámaras	USD. 60.990,00
03	Torre Autosoportada de 12 mtrs.- Centro de Control	USD. 5.400.00
04	UPS de respaldo para cámaras	USD. 22.315.00
	TOTAL:	**USD. 207.622,00**

Incluye: Materiales, Instalación, Calibración y Programación

Tabla 4
Inversión de Equipos de Parking ESPE

CANT.	DETALLE	COSTO
1	Emisor de tickets rotación. Código de Barras, mod. PGL 3076	
1	Tratamiento de pensionados	
1	Tratamiento de abonos temporales en tiempo o dinero	
1	Barrera electromecánica para vehículos, modeo AS 30	
1	Brazo Recto rectangular de aluminio bicolor amarillo/negro longitud 2.45 mts.	11.555.29
	SALDA ESTACIONAMIENTO VISITAS PAGADO	
1	Validador de tickets de rotación. Código de Barras, mod. PL3GB	
1	Tratamiento de pensionados	
1	Tratamiento da abonos temporales en tiempo o dnero	
1	Barrera electromecánica para vehículos, modelo AS 30	
1	| Brazo Recto rectangular de aluminio bicolor amarílo/negro longitud 2.45 mts.	10.804,54
4	Poste de abonados, mod. PGL 30/8	
4	Tratamiento de pensionados	
4	Tratamiento de abonos temporales en tiempo o dinero	
4	Barrera electromecánica para vehículos, modelo AS 30	
4	Brazo iluminado 2. 5 metros esta Incluido y articulado	38.538,50
8	Poste de abonaos, mod. PGL 30/8	
8	Tratamiento de pensionados	
8	Tratamiento de abonos temporales en tiempo o dinero	

8	Barrera electromecánica para vehículos, modelo AS 30	
8	Brazo iluminado 2. 5 metros esta incluido y articulado	77.077,00
	CAMARAS LECTORES DE PLACAS	
8	Smary LPR camera	
8	iInterface Standard LPR	
8	Fixing kit pole	
8	Freight ES-D	
1	Software LPR	
1	image captura	
1	ICP configuration	
1	interface SW license	48.611,06
	SERVIDOR / PUNTO DE PAGO MANUAL	
1	Servidor de Gestión, mod. ZR30	
1	Cajero automático	
2	Caía de Cobro Manual, mod. POS30R B	63.175,30 1
	CAMARAS PERIMETRALES	
6	Cámaras perímetrales solo entradas	
3	Capturador de imágenes para procesamiento de un máximo de 4 cámaras	
3	Converso' IP "quatro" para un máximo de 4 cámaras	
1	Software integrado en el propio Centro de Control S&B Entervo.B24	18.234,72 1
	INTERFONIA IP OPCIONAL	
1	CENTRAL INTERFONIA IPECS MFIM50B (50 PUERTOS)	

2	SOPORTE PARA PARED IPECS	
1	SSADO0008001 Alimentador para teléfonos IP	
1	TERMINAL IP LIP 8024D (STANDAR)	
14	LICENCIA PARA 1 TERMINAL SlP (LIK-SIPE)	
14	Panel IP Solo placa	
1	CENTRAL INTERFÓNIA IPECS LGCM 4 1íeas analógicas	
1	MODULO DETECTOR DE 12 KHZ e Inversión pol	
1	LIK 300 ALIMENTADOR PARA MODULO	14.521,200
	CONFIGURACION DEL SISTEMA	
1	Configuración del sistema	22.022,00
	MONTAJE	
1	Montaje. Puesta en Marcha y Formación	10.894,68
	CCTV |	
7	Cámaras IP para vigilancia parqueadero ZONA DE ROTACION	
14	Camaías IP para vigilancia parqueadero ZONAS RESERVADAS	
6	Cámaras IP para vigilancia parqueadero ENTRADAS Y SALIDAS DEL ANILLO	
4	Cámaras IP para vigilanca parqueadero CAJAS MANUALES Y MONITOREO	
1	NAS de grabación 8 teras de respaldo	
		38.149,80

OBRAS CIVILES ELÉCTRICAS Y DATOS (ANILLO DE FIBRA)

14	Red de datos (anillo de fibra óptica)	
1	Red eléctrica	30.516,38
1	Señalización vertical	10.580,00
1	Señalización horizontal mantenimiento pnmera *vez*	25.000,00
	TOTAL INVERSION	**420.806,61**

El oferente presentará con su oferta lo siguiente:

- El Oferente deberá incluir en su propuesta un plan de implementación en detalle cuyo plazo de ejecución no será mayor a 100 días calendario a partir de la entrega del anticipo.

- El Oferente deberá incluir en su propuesta los lineamientos generales de la capacitación y transferencia tecnológica a realizarse para la ESPE o quien ésta designe.

- El oferente deberá presentar un cronograma de un mantenimiento anual.

- El oferente deberá entregar junto a la oferta el certificado de la visita técnica realizada al campus universitario.

5.5 Análisis Costo Beneficio

El análisis y estudio de factibilidad para la implementación de un sistema de “ojos de águila”, para el campus Politécnico y un sistema de “control de accesos” perimetral de la Escuela Politécnica del Ejército

(E.S.P.E.-SANGOLQUI), se lo realizó sin fines de lucro para la Universidad, motivo por el cual no se realizará un análisis netamente económico de costo-beneficio, por lo que el trabajo de investigación se enfocó específicamente analizar las necesidades técnicas, con la finalidad de que sean empresas externas las que brinden el servicio de seguridad integral en el Campus Universitario.

La contratación de un proveedor externo para la implementación del sistema de CCTV y control de accesos en la ESPE, permitirá al personal de la ESPE (servidores públicos, profesores y alumnos) que se enfoquen en sus "actividades centrales", generando las siguientes ventajas y desventajas.

Ventajas:

- Da tiempo para enfocarse en las actividades vitales para el agregado de valor del personal de la ESPE (servidores públicos, profesores y alumnos).

- Permite encontrar ayuda experta, de forma temporaria y sin compromisos a largo plazo.

- Para las empresas contratantes, el aporte de pequeñas empresas diversas resulta en mayor versatilidad y nuevas ideas que pueden faltarle internamente.

- Permite sumar esfuerzos, apoyándose en quienes ya realizan y tienen experiencia en este tipo de actividades.

- Permite ocupar menos espacio de trabajo, optimizando los lugares específicos que se asigne a la empresa que proporcionara el servicio.

Desventajas

- Para un funcionamiento sin fricciones exige entornos más cooperativos que la típica relación de proveedor-cliente.

- Puede afectar la confidencialidad.

- Puede llevar tiempo llegar a acuerdos claros sobre obligaciones y responsabilidades de cada parte.

- Puede perderse el control sobre el producto final y verse afectada la calidad.

- Puede requerir capacitación y actividades de integración regulares para mantener el trabajo en equipo

- Requiere de un análisis costo-beneficio para evitar costos ocultos.

- El implementar a la ESPE el sistema de seguridad integral con recursos propios, le es muy complicado por la baja asignación anual, lo que acarrearía demora en el tiempo en la activación.

- Se requiere de personal especializado para la implementación y manejo de los sistemas, actividades que no las pueden desarrollar el personal de la ESPE, en vista que sus actividades principales son las netamente académicas.

CAPITULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones.

- En el presente trabajo se realizó el análisis y estudio de factibilidad para la implementación de un sistema ”Ojos de Águila” para el Campus Politécnico y un sistema de “Control de accesos” perimetral de la Escuela Politécnica del Ejército (E.S.P.E. - Sangolquí), el mismo que nos permitió lo siguiente:

- Mediante el análisis del flujo vehicular y peatonal en el Campus Politécnico, se logró determinó las necesidades primordiales para el convivir en el Campus universitario, para implementar la seguridad física perimetral en el Campus Politécnico.

- A través del levantamiento de información actual de la infraestructura eléctrica, electrónica y de telecomunicaciones del campus ESPE, permitió también el levantamiento del informe técnico relativo a la ubicación de las cámaras y el sistema de control de accesos en la ESPE.

- Mediante la información recopilada tanto de sistemas de seguridad en CCTV, se analizaron alternativas de diseño de sistema Ojos de Águila y Control de Accesos, factibles de aplicar en la ESPE.

- Se diseñó el sistema Ojos de Águila y Control de Accesos, acorde a los requerimientos de seguridad electrónica del Campus de la ESPE-Sangolquí, el mismo que cuenta con un Sistema de Comunicación capaz de integrar a otros, mediante el establecimiento de las características técnicas mínimas pero óptimas, para que los equipos que lo constituyen, sean de tecnología de punta.

- Mediante el presupuesto referencial analizado en cuanto al costo que conforma los sistemas y equipos de Ojos de Águila y Control de Accesos, permitirá a las empresas ofertantes acceder a participar en la prestación de los servicios electrónicos de seguridad integral para beneficio del Campus de la ESPE-Sangolquí como son: El control de las áreas vulnerables, control de vehículos y personas que ingresan y salen, monitoreo perimetral de parqueaderos y laboratorios, también se dispondrá de un sistema de identificación para el tránsito de particulares en las diferentes áreas de la ESPE (Tarjetas).

6.2 Recomendaciones.

- Complementar la seguridad electrónica del CCTV y Control de accesos con seguridad humana privada, mediante rondas motorizadas diurnas y nocturnas.

- Capacitar e informar a toda la comunidad universitaria sobre los cambios que se implementan sobre seguridad, mediante la implementación de campañas de valores, comportamiento y convivir ciudadano.

- Implementar instructivos y normas para el buen uso de los sistemas de seguridad electrónica.

- Coordinar un plan de trabajo de seguridad corporativo con la participación de la Policía Nacional y autoridades del GAD del cantón Rumiñahui, específicamente de Sangolquí.

- Se debe realizar una redistribución de las zonas de parqueo vehicular, las mismas que deben acoplarse a las áreas de trabajo y estudio, con la finalidad de evitar el ingreso de alumnos y particulares a lugares no autorizados.

- Emprender campañas permanentes de difusión del sistema de seguridad integral que posee el Campus Universitario, con la finalidad de que toda la comunidad tenga conocimientos de las normas y procedimientos a seguir cuando se desplace dentro de la ESPE ya sea a pie o en vehículo.

BIBLIOGRAFÍA

Amaya, J. (2009). Sistemas de información gerenciales: Hardware, software redes

Bernal. (2006). Metodología de la Investigación. pág. 78, 79, 80

Huidobro, J. Millán, R. (2010). Manual de domótica. España. Creaciones Copyright. Pag: 72

Dordoigne, J. (2013). Recursos Informáticos Redes informáticas Nociones fundamentales. Barcelona – España. Ediciones ENI 4ta Edición. Pág.: 33, 37

García, F. (2010). Video vigilancia: CCTV usando vídeos IP. Málaga-España. Editorial Vértice. Pag: 12, 13

Gil, P. Pomares, J. Candelas, F. (2010). Redes y transmisión de datos. Alicante-España. Publicaciones Universidad de Alicante-Textos Docentes. Pag: 28, 88

Herrera, E. (1998). Introducción a las telecomunicaciones modernas. Balderas – México, Editores Limusa Grupo Noriega. Pag: 64, 166, 217

Herrera, E. (2003). Tecnologías y redes de transmisión de datos. Balderas – Mexico, Editorial Llimusa. Edición 1ra – 2003. Pág. 41.

Martín, J. (2009), Instalaciones de telecomunicaciones. Madrid-España. Editorial: Editex. Pág.: 49

Rodil, I. Camino, P. (2010). Operaciones auxiliares con tecnologías de la información y la comunicación. Madrid – España, Ediciones Paraninfo Edición 1ra. Pag: 100

Eggelin, T. Frater, H. (2003). Ampliar, reparar y configurar su PC. Barcelona- España. Editorial marcombo. Boexareu. Pág.: 212

Tanenbaum, A. (2003). Redes de computadoras México. Edición 4ta. Editora. Pearson Educación. Pág.16, 37, 41 92

Rodríguez, A. (2007). Iniciación a la red Internet: Concepto, funcionamiento, servicios y aplicaciones de Internet. España. Editorial: Ideas propias. Edición 1ra. Pag: 2

Rodríguez, J. (2013). Circuito cerrado de televisión y seguridad electrónica. Ecuador. 1ra edición. pág. 110, 166, 173, 180

REFERENCIAS BIBLIOGRÁFICAS

- http://www.invdes.com.mx/anteriores/Octubre1999/htm/edificio.html
- http://www.dei.uc.edu.py/tai2004-2/2/Edificios_Inteligentes.htm
- http://docsetools.com/articulos-noticias-consejos/article_130946.html
- http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/lezama_l_a/capitulo1.pdf.
- Municipalidad de Cuenca. El Cuencano. www.cuenca.gov.ec.[En línea] [Citado el: 24 de Feb de 2010.]
- http://www.cuenca.gov.ec/elcuencano/publicaciones/010/elcuencano0110.pdf.
- Wikipedia. Corporación para la Seguridad Ciudadana de Guayaquil. [En línea] 21 de feb de 2010. [Citado el: 25 de Feb de 2010.]
- http://es.wikipedia.org/wiki/Corporaci%C3%B3n_para_la_Seguridad_Ciudadana_de_Guayaquil.
- Ojo: le estamos filmando. Carrión M., Fernando. 2008, Ciudad Segura, Programa Estudios de la Ciudad (FLACSO-Ecuador), pág. 1.
- Juan Carlos I, rey de España. Ley Orgánica 4/1997, de 4 de Agosto, por la que se Regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en Lugares Públicos. Palma de Mallorca : s.n., 1997.
- La video vigilancia: uns sistema de seguridad que requiere de control y regulación. Betancourt, Andrea. 2008. Ciudad Segura (FLACSO-ECUADOR).
- La video Vigilancia: Un sistema en Construcción. Betancourt, Andrea. 2008, Ciudad Segura, Programa Estudios de la Ciudad FLACSO-ECUADOR . Entrevista al Teniente Eduardo Ron, Central Metropolitana de Atención Ciudadana – CMAC.
- Ojos de Águila: una primera aproximación al sistema de video vigilancia en Quito. Löfberg, Sara. 25, Quito : Ciudad Segura, Programa estudios de la Ciudad. FLACSO-Ecuador, 2008.
- http://www.rnds.com.ar/articulos/045/RNDS_152W.pdf
- http://www.mslatam.net/index.php/aplicaciones/control-de-acceso-vehicular
- http://www.monografias.com/trabajos12/reina/reina.shtml#ixzz3WWLYD0GA