UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y COMUNICACIONES

Tema:

"CONTROL DE ACCESO PARA LA DOTACIÓN DE SEGURIDAD EN DORMITORIOS Y ÁREAS RESTRINGIDAS EN EL HOTEL DESTINY"

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

AUTOR: Santiana Navas Jairo Paúl

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

Ambato - Ecuador

Noviembre 2012

APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Investigación sobre el tema: "**CONTROL DE ACCESO PARA LA DOTACIÓN DE SEGURIDAD EN DORMITORIOS Y ÁREAS RESTRINGIDAS EN EL HOTEL DESTINY**", realizado por el Sr. Jairo Paul Santiana Navas, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, Universidad Técnica de Ambato, considero que dicho informe investigativo reúne los requisitos y méritos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato, Noviembre del 2012

EL TUTOR

_____

Ing. M.Sc. Mario García

AUTORÍA

El presente trabajo de investigación titulado: **"CONTROL DE ACCESO PARA LA DOTACIÓN DE SEGURIDAD EN DORMITORIOS Y ÁREAS RESTRINGIDAS EN EL HOTEL DESTINY"**. Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Noviembre del 2012

Jairo Paul Santiana Navas

CC: 1803863099

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Edwin Morales, Mg. e Ing. Giovanny Brito, Mg. , revisó y aprobó el Informe Final del trabajo de graduación titulado **"CONTROL DE ACCESO PARA LA DOTACIÓN DE SEGURIDAD EN DORMITORIOS Y ÁREAS RESTRINGIDAS EN EL HOTEL DESTINY"**, presentado por el señor Jairo Paúl Santiana Navas de acuerdo al Art. 17 del Reglamento de Graduación para obtener el título Terminal de tercer nivel de la Universidad Técnica de Ambato.

_____

Ing. Oswaldo E. Paredes O., M.Sc.

PRESIDENTE DEL TRIBUNAL

_____ _____

Ing. Edwin R. Morales P., Mg. Ing. Giovanni D. Brito M., Mg.

DOCENTE CALIFICADOR DOCENTE CALIFICADOR

DEDICATORIA

A dios, por darme la capacidad necesaria para afrontar los grandes retos de la vida, llenándome de conocimientos paz y amor al prójimo.

A mi madre, que desde pequeño afronto el papel de padre y madre, fundamentando que el conocimiento me llevara muy lejos y en cada caída está presente para levantarme y darme las fuerzas necesarias para continuar llenándome de bendiciones

A mi familia, mi esposa compañera incondicional en buenos y malos momentos de mi vida, mi hija luz de mi vida, aire de mis pulmones, es difícil describir sentimientos hacia mi pequeña que es la razón principal que me lleva a continuar y fomentarle los valores que se necesitan en el camino del hacia el éxito.

A todas las personas que me extendieron la mano en las más grandes necesidades que presentan la vida y los duros momentos que la acompañan.

Jairo Paúl Santiana Navas

AGRADECIMIENTO

Es difícil en un párrafo tan pequeño nombrar a todas las personas que contribuyeron en cada paso que me permito el desarrollo personal y profesional, las palabras no quedan en el viento solo esperan el momento indicado para sembrar un presente sobre la vida y sus largas enseñanzas.

A mi madre que vio las maneras necesarias para apoyarme en mis estudios hasta su culminación, sabiendo sembrar la semilla del agradecimiento ante todas las personas que nos extienden la mano para apoyarnos.

A mi esposa Fabiola Cofre, que supo entender que el amor que nos acoge es permanente y solido en busca siempre de un futuro mejor.

A la Facultad de Ingeniería en Sistemas, Electrónica e Industrial por abrirme las puertas y compartir su conocimiento, permitiendo participar esos momentos de felicidad y tristeza que solo son enseñanzas para afrontar mejor las cosas de un presente y futuro.

A los Docentes que supieron transmitir los mejores de sus conocimientos y al mismo tiempo como amigos enseñarnos que la responsabilidad nos abrirá las puertas necesarias para cumplir los objetivos de nuestras vidas.

Jairo Paúl Santiana Navas

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

En el primer capítulo se realizó una presentación de la base del problema que llevo a plantear interrogantes que ayudaron a la resolución del mismo, se planteó el tema de investigación del proyecto en base a varios parámetros establecidos en el capítulo siguiente, a esto se plantearon objetivos y se realizó un breve análisis que ayudo al planteamiento del problema en el Hotel Destiny que se encuentra en construcción en la ciudad de Baños.

En el segundo capítulo una vez planteadas las interrogantes se fundamenta las variables con teoría sobre el control de acceso y video vigilancia, los cuales llevan sus características principales, tecnología, tipos, entre otros, que buscan satisfacer las necesidades de seguridad en el Hotel, además del señalamiento de variables se plantea la hipótesis del proyecto.

En el capítulo tres se describen los métodos de investigación, recolección de información, operacionalización de las variables para el planteo de preguntas de las encuestas y los métodos de análisis e interpretación de la información.

En el cuarto capítulo se analiza la situación actual del hotel y su infraestructura física, se plantean preguntas sobre la posible implementación del proyecto mediante entrevistas y encuestas dirigidas a los encargados y hoteles de la ciudad.

En el quinto capítulo se exponen las conclusiones y recomendaciones de las encuestas y entrevistas realizadas en cuanto a la seguridad que necesita el hotel.

En el sexto capítulo se justificó, planteo, analizó, los objetivos y la factibilidad del trabajo, en el transcurso de la propuesta se investigó y analizó equipos, además se procede con el diseño en el hotel gracias al apoyo presupuestario de los propietarios, en donde se demuestra que el control de accesos cumple todos los requerimientos que se plantean en las consideraciones previas al diseño.

INTRODUCCIÓN

El hotel Destiny en búsqueda de cumplir con los más altos estándares de atención al cliente, contempla la seguridad tanto de la persona como sus pertenencias, toma como punto importante la instalación de un sistema de control de accesos el cual fue puesto en manos de mi persona que realiza la presentación de este documento en donde se puede revisar el transcurso que llevo a cabo el mismo.

Gracias a la tecnología actual y el desarrollo que se da día a día a través de investigaciones que realizan grandes empresas, en busca de satisfacer las demandas actuales en seguridad y todos los campos que la complementan, el proyecto de investigación que se muestra a continuación cuenta con un sin número de posibles soluciones al control de acceso que puede necesitar cualquier tipo de empresa, gracias a la información encontrada en internet y después de varias visitas técnicas se plantearon varios puntos relevantes que ayudaron a tomar una decisión en la elección de equipos, donde varias empresas distribuidoras presentaron las mejores opciones en cuanto a control de accesos se puede hablar en el país y a nivel internacional.

Una vez que se contó con el apoyo presupuestario se realizó un análisis que ayudo a determinar cuál cumple con los requerimientos necesarios y se procedió con el diseño de distribución de equipos, en donde se comprenden habitaciones y áreas restringidas.

Con todo listo se realizó el diseño y configuración de equipos los cuales serán puestos en funcionamiento aproximadamente en el mes de noviembre, para satisfacer la demanda hotelera que presenta el cantón de Baños.

CAPITULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1 Tema de Investigación

"CONTROL DE ACCESO PARA LA DOTACIÓN DE SEGURIDAD EN DORMITORIOS Y ÁREAS RESTRINGIDAS EN EL HOTEL DESTINY"

1.2 Planteamiento del Problema

1.2.1 Contextualización

En épocas, no muy lejanas, los controles de acceso eran simples puertas, que luego fueron reforzadas por guardias de seguridad. Estos sistemas de seguridad fueron efectivos, durante un tiempo, pero comenzaron a ser víctimas de personas inescrupulosas, que hacían lo posible para ingresar a lugares, a los que no habían sido autorizados con fines delictivos.

El control de acceso es una solución de seguridad para grandes empresas con ingreso de empleados y personal externo. El sistema permite convenientemente consentir la entrada y salida a ciertas zonas de la empresa libres o restringidas, en la mayoría de veces utilizan una tarjeta de identificación personal con una banda magnética, la cual tiene la información codificada, o a su vez se utilizan códigos en teclados numéricos, escáneres de huellas digitales, identificación de rostro, etc.

A nivel mundial los sistemas de control de acceso nacieron en la década de los 70, gracias a los avances de la tecnología de la época, se pudieron lograr diseños que ofrecían mayores niveles de seguridad y que representaban un completo desafío para los intrusos. Con la adopción de esta tecnología se puede establecer un

control de acceso, que resultaba, no sólo más efectivo, sino también más cómodo y rápido, el sistema está presente en Bancos Internacionales, hoteles de lujo, centros de investigación, incluso en apartamentos y dormitorios de colegio.

Es difícil saber con exactitud el porcentaje de uso de los distintos sistemas de seguridad en la actualidad. En pleno inicio del siglo XXI los más utilizados fueron tarjetas con banda magnética y teclados numéricos, según el avance tecnológico se han ido desarrollando nuevos y avanzados sistemas de identificación como las tarjetas de proximidad, el identificador biométrico de huellas, rostro, iris, voz, los cuales ganaron terreno en sitios con mayor control de alta prioridad de seguridad como en cajas fuertes de bancos, centros de investigación científica, desarrollo de armas, etc.

En el Ecuador una variedad de pequeñas y grandes empresas han optado por la implementación de sistemas de control de acceso y seguridad en áreas que se necesita un registro de entrada y salida. El mayor porcentaje se da en la mayoría de entidades financieras tal es el Banco del Pichincha, Guayaquil, Pacifico entre otros, Hotel Hilton Colon, Municipios, Garajes, sitúan este servicio como una regla de seguridad. Empresas como Promatco S.A., a Tiempo, ID. Consultants, presentan distintas soluciones de seguridad con un stock amplio de equipos de última tecnología y respaldo técnico a nivel nacional.

En Tungurahua así como a nivel nacional existe un gran porcentaje de empresas que tienen instalados sistemas de control de acceso, lo cual hace que el aporte tecnológico y respaldo técnico esté presente en la provincia, SIDEPRO, ICONO SISTEMAS, TELET con sede en Ambato presentan una alta gama de productos de control de acceso, el único inconveniente se da en los costos ya que al no contar directamente con los productos las importaciones incrementan el precio de los mismos, por este motivo la mayoría de instalaciones la realizan empresas de fuera de la provincia.

El Hotel Destiny en su diseño físico y tecnológico, presenta un deficiente control de acceso a dormitorios y áreas restringidas, al tratar de brindar un servicio de alta calidad los encargados de la construcción no tomaron en cuenta varios parámetros

que ayuden a proteger la integridad física y económica de los huéspedes y trabajadores, creando un ambiente vulnerable para la delincuencia que se hace presente en días festivos y de gran acogida, permitiendo que el proyecto de control de acceso sea el pilar fundamental para el prestigio y seguridad del Hotel.

1.2.2 Análisis critico

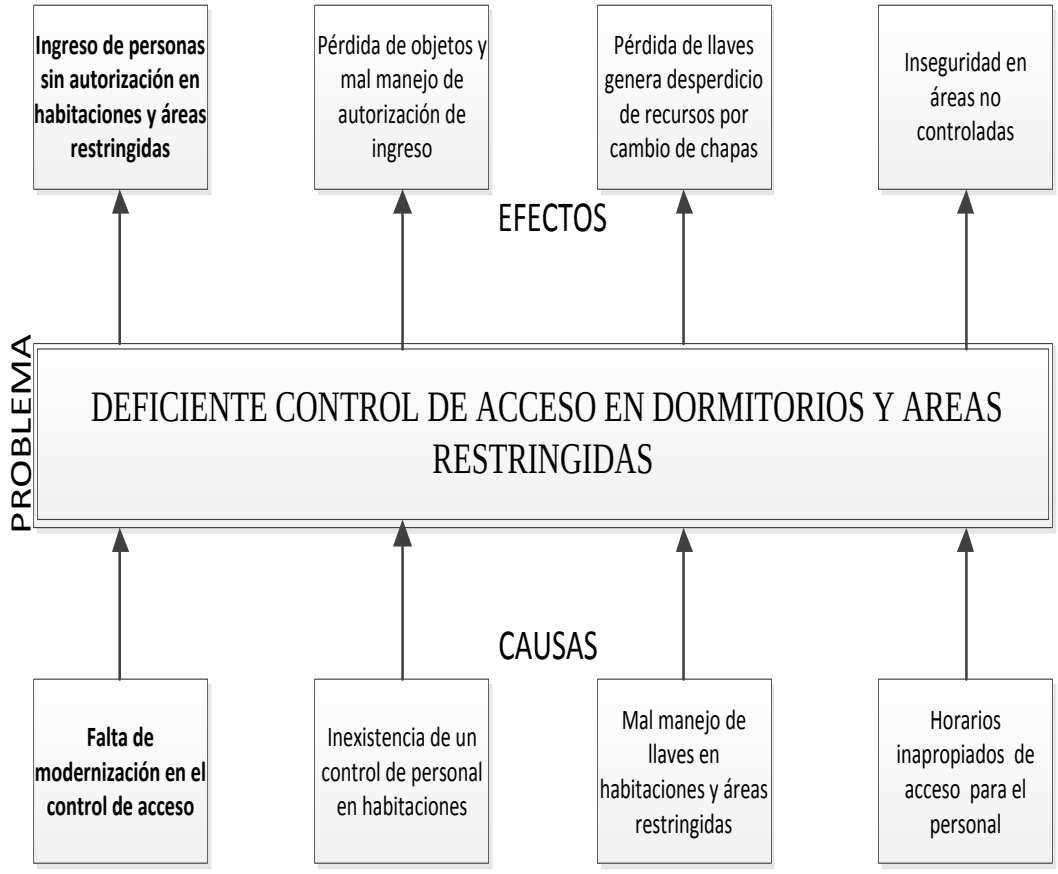


Figura 1.1: Árbol de problemas

Realizado por el investigador

Los sistemas electrónicos permiten tan solo con un clic controlar entradas y salidas, además de guardar un registro de cuándo y en donde entra un individuo gracias a soluciones tecnológicas confiables y seguras.

La falta de modernización no se toma en cuenta para la construcción de zonas restringidas y lugares privados lo que produce inseguridad en la entrada de personas sin autorización en dichas zonas.

En hoteles en donde se hospedan personas con objetos de valor son vulnerables a pérdidas en los momentos que se realiza el aseo o mantenimiento del dormitorio, gracias al control de acceso se puede tener un registro de personal que ingreso a una habitación o lugar restringido con la hora y el momento exacto.

Las personas encargadas del ingreso a habitaciones deben tener cuidado con el manejo de demasiadas llaves las cuales por el uso y abuso llegan a perderse provocando un desperdicio de recursos al momento de cambio de chapas e inseguridad al momento de la perdida.

Por la seguridad y tranquilidad de los huéspedes es importante poder asegurar que sólo las personas autorizadas acceden al dormitorio.

El control de acceso instalado en suites de hoteles o en apartamentos permite controlar además del acceso, que el personal de servicio ingrese en las horas convenidas para llevar a cabo una labor de limpieza o mantenimiento de un equipo.

1.2.3 Prognosis

Al no existir horarios de ingreso y un control de acceso a habitaciones y áreas restringidas, la seguridad de las pertenencias y objetos de valor estará vulnerable a pérdidas y robo.

1.2.4 Formulación del problema

¿Cómo afecta el deficiente control de acceso a la seguridad de dormitorios y áreas restringidas del Hotel Destiny?

1.2.5 Preguntas directrices

- ¿Qué políticas de seguridad se plantearon en el proceso de construcción en el Hotel Destiny?
- ¿Qué vulnerabilidades de seguridad existen en dormitorios y áreas restringidas del entorno?
- ¿Qué propuesta permitirá la dotación de seguridad en dormitorios y áreas restringidas mediante la implementación de un sistema de control de acceso?

1.2.6 Delimitación

- **Campo:** Electrónica
- **Área:** Control y Comunicación
- **Aspecto:** Seguridad en el Control de Acceso
- **Delimitación espacial:** El siguiente trabajo de investigación será realizado en el Hotel Destiny ubicado en la provincia de Tungurahua, Cantón Baños en el sector de Centro calles Oscar Efrén Reyes entre las calles Ambato y Vicente Rocafuerte.
- **Delimitación temporal:** La presente propuesta será se desarrollará en el periodo de 6 meses a partir de su aprobación por el Consejo Directivo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.3 Justificación

El presente proyecto de investigación se ejecuta por la necesidad de tener un moderno y tecnológico sistema de control de acceso en habitaciones y áreas restringidas en el Hotel Destiny que además ofrecerá servicios de hospedaje vip, sala de eventos, bar discoteca, comedor, garaje, áreas de recreación, centro de cómputo, salas de entretenimiento y descanso, la mayoría estarán dotadas de un control de ingreso para tener un registro computarizado en caso de presentarse cualquier tipo de problemas en dichas instalaciones del hotel.

Los conocimientos teórico prácticos adquiridos en la carrera de Electrónica y Comunicaciones se pondrán en práctica a su máximo nivel por la investigación y análisis técnico práctico que se realizará para saber cuál es el sistema con mayor tecnología y costo que beneficiará directamente al Hotel Destiny y en especial a sus huéspedes quienes contarán con una mayor seguridad.

El impacto del presente proyecto beneficiará directamente a todos los que visiten las instalaciones del Hotel Destiny al sentir seguridad de sí mismos y sus pertenecías, además de ser el único en todo el cantón Baños que poseerá tecnología en el control de acceso y seguridad.

También se desea facilitar al personal que trabaja en el Hotel que con una sola identificación poder realizar el desempeño de aseo y otras tareas según horarios establecidos por el área técnica.

La mayoría de empresas interesadas en vender los equipos cuentan con tecnología de punta, así como con distintos equipos de control de acceso y seguridad los cuales estarán sujetos a pruebas técnicas lo que facilitará el diseño e implementación.

Los sistemas de Control de Acceso disminuyen los costos e incrementan los niveles de seguridad, la factibilidad económica como tecnológica se ve presente gracias al gran interés de beneficiar al hotel en todo el sentido de comodidad y seguridad para los visitantes.

1.4 Objetivos de la investigación

1.4.1 Objetivo general

- Analizar el efecto del deficiente control de acceso en la seguridad de dormitorios y áreas restringidas en el Hotel Destiny.

1.4.2 Objetivos específicos

- Indagar las políticas planteadas en el proceso de construcción del Hotel Destiny.
- Analizar las vulnerabilidades de dormitorios y áreas restringidas del entorno.
- Plantear una propuesta que permita la dotación de seguridad de dormitorios y áreas restringidas mediante la implementación de un control de acceso.

CAPITULO II

MARCO TEÓRICO

2.1 Antecedentes Investigativos

En varias visitas realizadas a la Biblioteca de la Facultad y después de una revisión teórica de proyectos de tesis doy constancia de que el proyecto presentado en este documento no ha sido diseñado ni estructurado, por estudiantes de la facultad o maestros, quedando libre de cualquier responsabilidad legal y en total libertad para realizar dicha propuesta.

2.1.1 Temas investigados en internet:

Título: "DISEÑO DE UN SISTEMA DE CONTROL DE ACCESO UTILIZANDO LA TECNOLOGÍA DE IDENTIFICACIÓN RFID PARA LA EMPRESA SOLUCIONES G4 DEL ECUADOR CIA. LTDA." Modalidad: TEMÍ – Escuela Politécnica Nacional Año: 2009. Autor: Pablo Walter Pipíales Angamarca cuyas conclusiones son:

- "Se ha alcanzado el objetivo de proporcionar a la empresa Soluciones G4 del Ecuador una solución de seguridad basada en la tecnología RFID la cual permita brindar seguridad, control y administración de los accesos a un inmueble"

- "La tecnología de identificación por radiofrecuencia tiene muchas ventajas, las cuales están basadas principalmente en ofrecer una seguridad electrónica inviolable, ya que la información de identificación asociada a un objeto o

usuario está almacenada en un chip, lo que impide la alteración del mismo por parte de terceros, a diferencia de un código de barras el cual puede ser clonado simplemente con una fotocopia."

Título: "CONTROL DE ACCESO" Modalidad: Proyecto de investigación. Instituto Tecnológico Culiacán Año: 2008. Autor: Sánchez Vejar Néstor Alonso, cuyas conclusiones son:

- "El control de acceso electrónico nos brinda una mayor seguridad cuando se trata de mantener una administración eficiente y funcional de áreas importantes, incluso para mantener un registro de entradas y salidas."

- "Definitivamente que la tecnología aplicada a los sistemas de seguridad ha venido a revolucionar la forma en cómo se administran los accesos y se monitorean las áreas importantes."

- "El sistema de control de acceso nos permite administrar los accesos de una forma profesional y eficiente; para llevar a cabo esta tarea se debe seleccionar el nivel de seguridad que se requiere para así hacer uso del dispositivo más adecuado para el control de las áreas más restringidas."

2.2 Fundamentación Legal

El presente proyecto de investigación "CONTROL DE ACCESO PARA LA DOTACIÓN DE SEGURIDAD EN DORMITORIOS Y ÁREAS RESTRINGIDAS EN EL HOTEL DESTINY" se basara en la "LEY ESPECIAL DE TELECOMUNICACIONES" y a los Art. 1 y Art. 10, que puedan afectar el uso de equipos que emitan señales de radio frecuencia, e implicar una violación a los artículos antes mencionados.

2.3 Categorías Fundamentales

2.3.1 Gráficos de Inclusión Interrelacionados

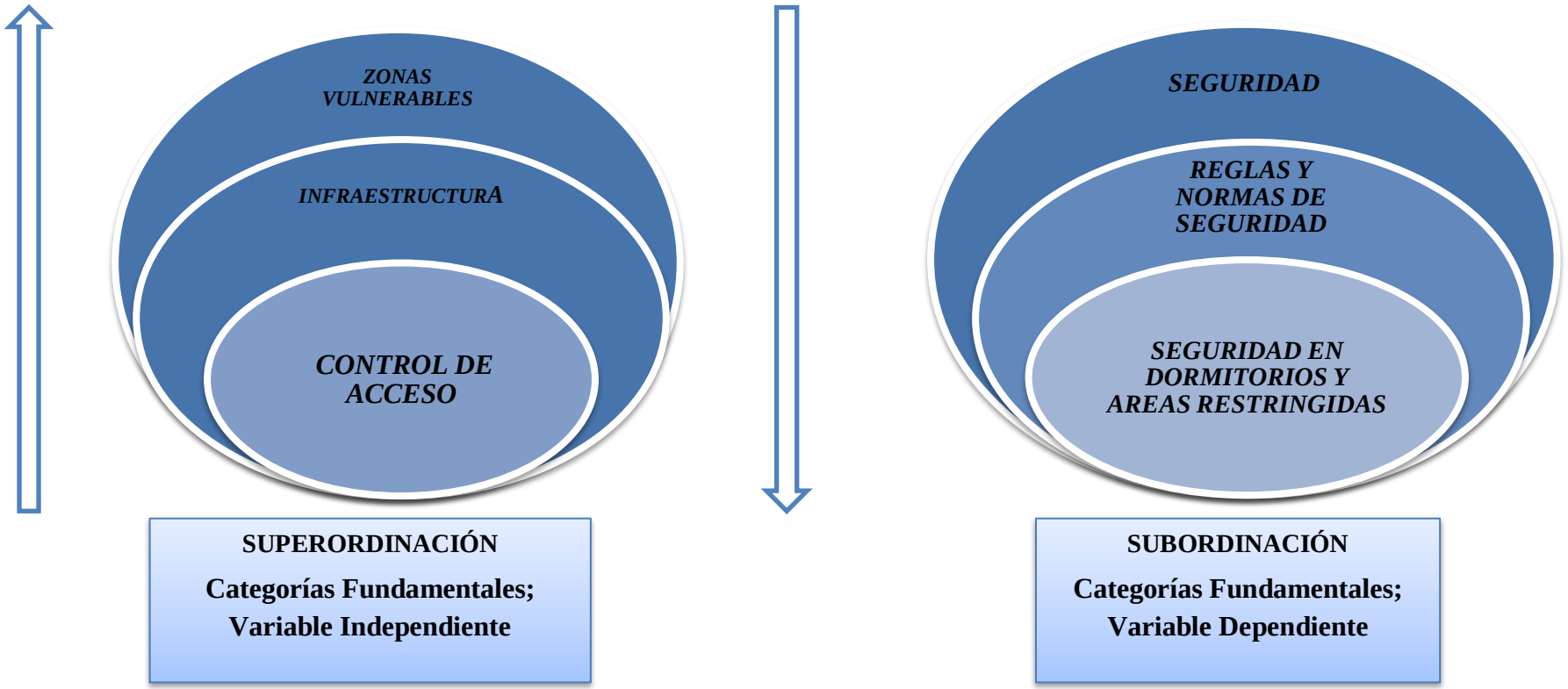


Figura 2.1: Gráficos de Inclusión Interrelacionados

Realizado por el investigador

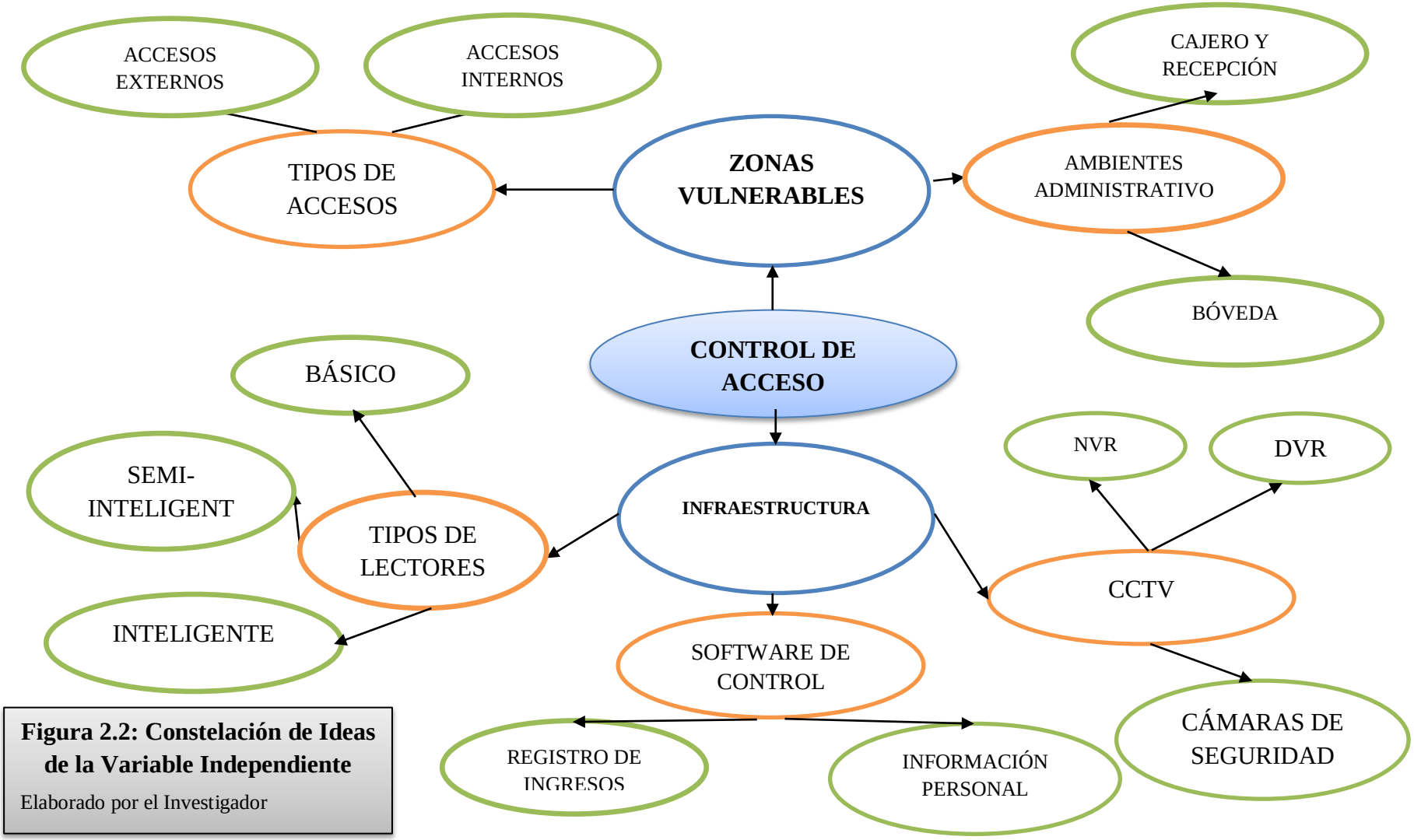


Figura 2.2: Constelación de Ideas de la Variable Independiente

Elaborado por el Investigador

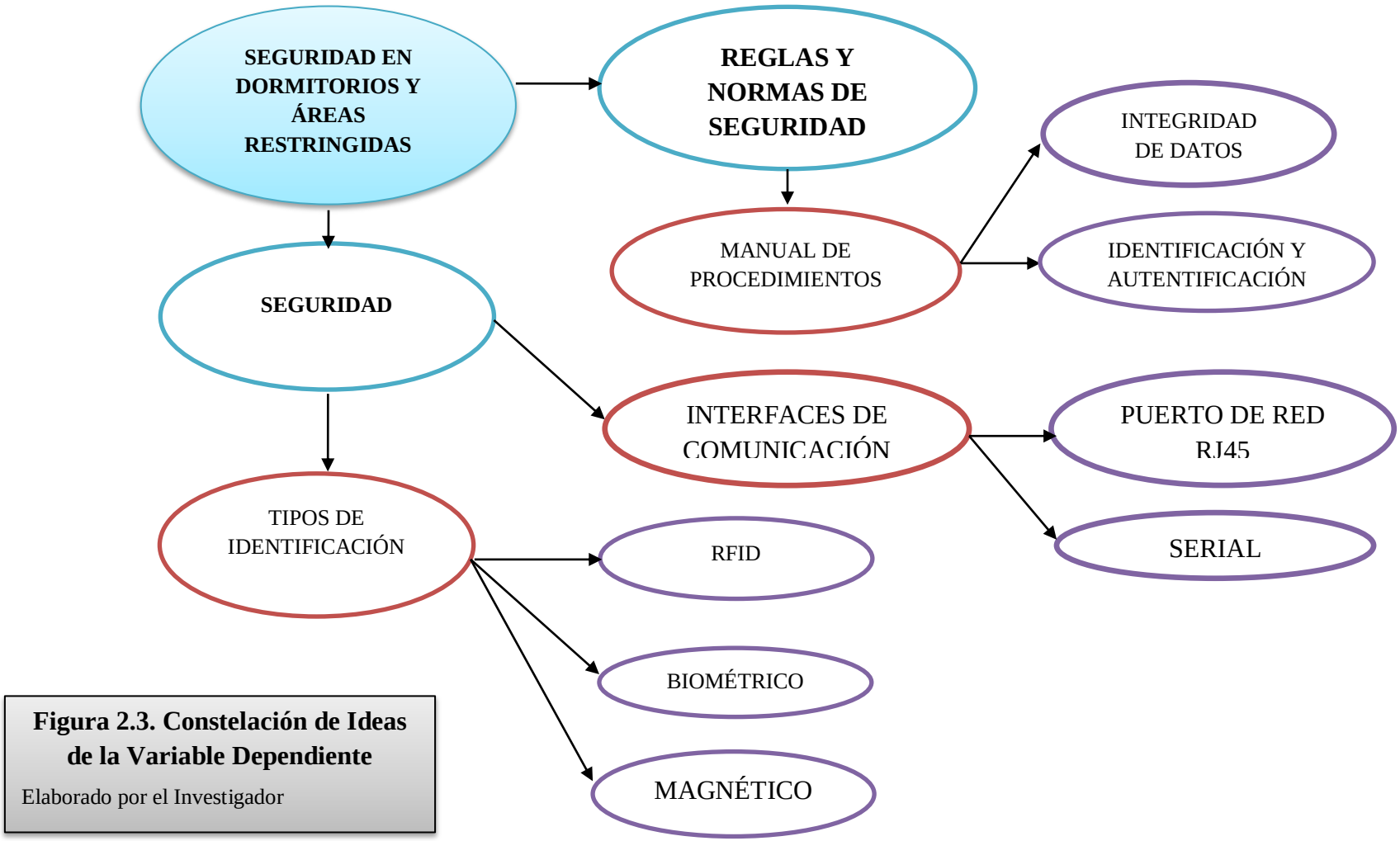


Figura 2.3. Constelación de Ideas de la Variable Dependiente

Elaborado por el Investigador

2.3.2 Visión Dialéctica de la Conceptualización que sustentan las variables

2.3.3 Marco conceptual de la Variable Independiente

2.3.3.1 CONTROL DE ACCESO

El control de acceso lleva un registro de ingreso y salida, en un área física controlada, los individuos que ingresan deben portar un código de activación, identificación o mediante un rasgo del mismo como huella digital, voz, entre otros. Al sistema informático conectado a los equipos de control le corresponde la revisión de la base de datos antes de consentir el ingreso, esto se realiza según prioridad de las zonas restringidas y otras que se hace por control.

En la fig. 2.4 se puede observar la infraestructura de un control de accesos diseñado para edificios donde se lleva un estricto control de ingreso, y el personal que trabaja ahí debe llevar su respectiva identificación para el ingreso a zonas restringidas y áreas administrativas dentro de las instalaciones del edificio.

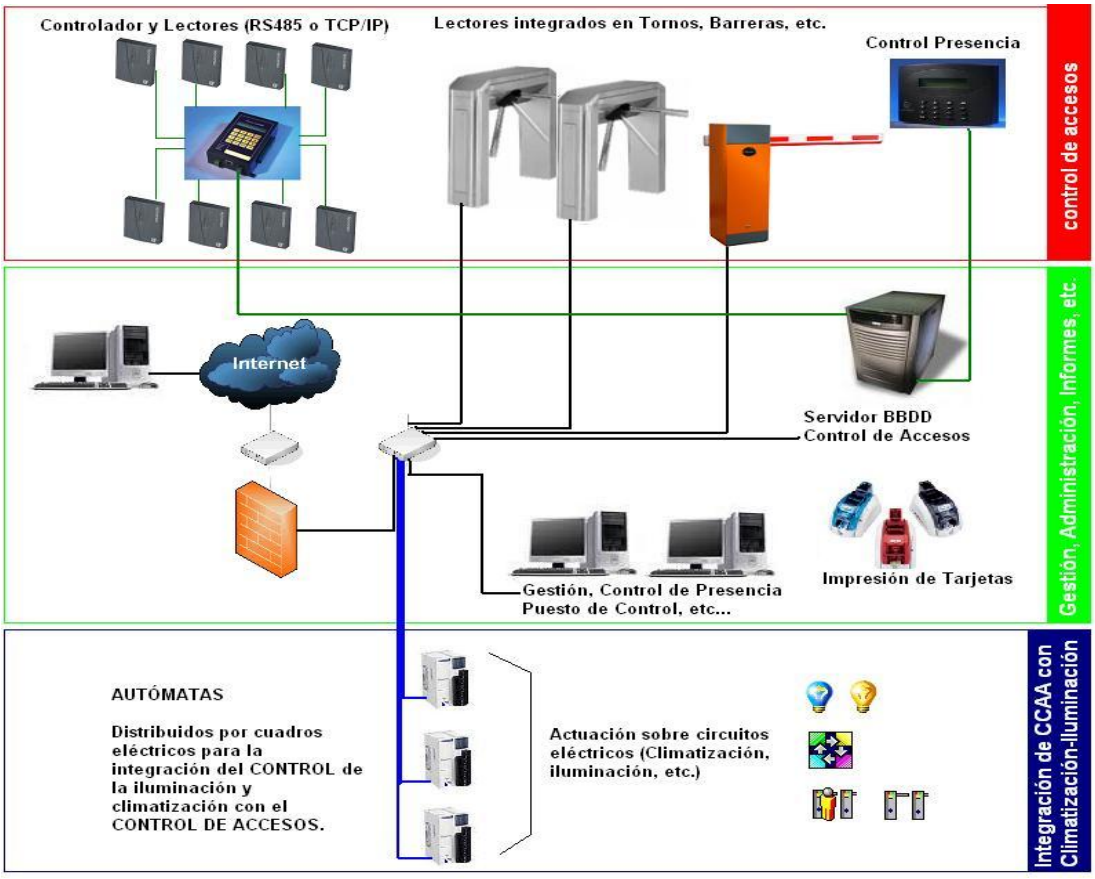


Fig. 2.4: Infraestructura De Un Control De Acceso

Fuente:http://www.isseguridad.com.ar/ficha_reporte.php?cate=SOLUCIONES%20-%20Control%20de%20Accesos

El control de acceso es, en realidad, un fenómeno diario. Una cerradura en una puerta de coche es esencialmente una forma de control, llegando hasta la necesidad de un guardia como un antiguo elemento de control, gracias al desarrollo tecnológico podemos contar con estrictos controles totalmente electrónicos.

2.3.3.2 INFRAESTRUCTURA DEL CONTROL DE ACCESO

El control de acceso es la barrera física de ingreso o salida, que permite conceder la entrada a un lugar o instalación, en la fig. 2.4 se observa los equipos que conforman dicho sistema:

- **Cerraduras magnéticas.-** Las cerraduras magnéticas funcionan vinculadas a un registro que las activa o desactiva mediante un sistema electrónico.
- **Sistema Informático.-** El sistema electrónico está conectado en conjunto con todos los equipos de control, puede automatizar rápidamente el proceso y registro de eventos, cuenta también con lectores que pueden ser de varios tipos, como un teclado numérico que con una clave anteriormente provista por el administrador del sistema funciona, el lector de tarjetas con bandas magnéticas entre otros.
- **Lectores de tarjetas.-** Los lectores no toman una decisión de acceso sino que envían generalmente un número de tarjeta a un software de seguridad que verifique el número en la tabla de autorización de ingreso.

2.3.3.3 CIRCUITO CERRADO DE TELEVISIÓN

Los sistemas de circuito cerrado de televisión llamados por sus siglas CCTV son muy utilizados para resguardar vigilar y monitorear zonas de alto, medio y bajo peligro, donde se pueden presentar actos de todo tipo, en la fig. 2.5 se visualiza su configuración esquemática en donde se observa las cámaras que pueden ser de varios tipos, con o sin movimiento, una estación de vigilancia donde se observa en vivo las actividades de cada cámara, son grabadas y procesadas, en caso que se denuncie una anormalidad en el área vigilada.

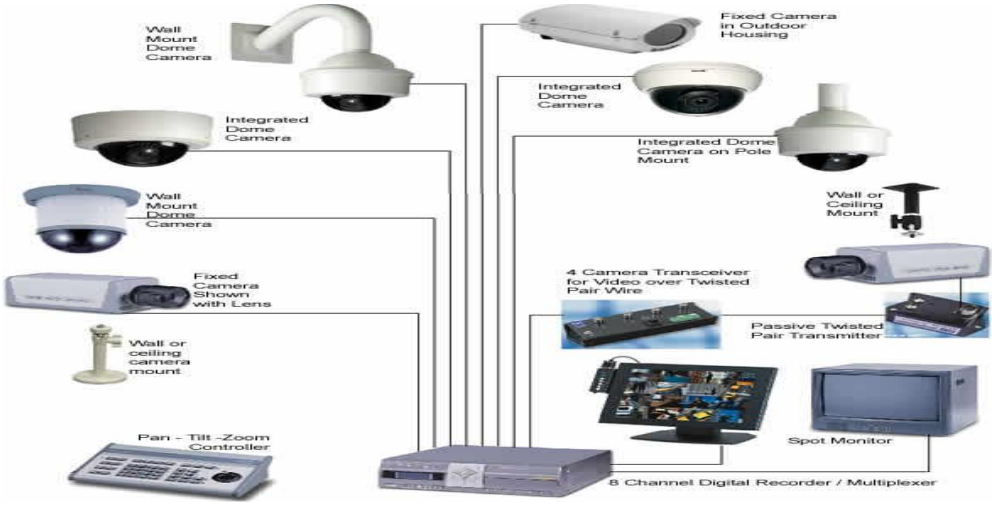


Fig. 2.5: Esquema de un CCTV

Fuente: http://www.accesor.com/esp/art2_query.php?fam=5

Estos sistemas se basan en una PC o DVR a los cuales se conectan todas las cámaras de seguridad y son los encargados de gestionar las imágenes y almacenarla digitalmente.

En la fig. 2.6 se observa el ingreso a las cámaras remotamente a través de internet, las mismas tienen una dirección electrónica que permite mediante una clave de administrador o usuario, controlar y ver online la actividad de cada una de ellas.

La configuración de los sistemas CCTV permite enviar correos electrónicos y activar alarmas en caso de detectar movimiento, dependiendo del tipo de cámara.

Fig. 2.6: CCTV En Internet Fuente: http://www.accesor.com/esp/art2_query.php?fam=5

Un sistema CCTV debe permitir realizar identificaciones durante o después del suceso que está visualizando. Por eso es muy importante definir qué función van a cumplir y donde serán colocadas las cámaras.

2.3.3.4 TIPOS DE CÁMARAS DE SEGURIDAD

En la fig. 2.7 se pueden ver los distintos tipos de cámaras de seguridad que se detallan a continuación:

- **Cámaras para interiores.-** Las cámaras para interiores son las más populares como por ejemplo la de mini domo. Existen tanto para blanco y negro como para color, ofrecen una gran calidad y resolución. Son económicos y muy efectivas.

Fig. 2.7: Tipos de cámaras

Fuente: http://e-dyario.com/actualidad/2011/06/13/varios-tipos-de-camaras-cctv/

- **Cámaras ocultas:** Las cámaras ocultas se pueden definir como módulos adaptables a diversos accesorios, tales como detectores de humos, relojes, muñecos, cuadros, lámparas, estas pueden ser conectadas directamente a un DVR o traer incorporada memoria interna de almacenamiento.

- **Cámaras con movimiento y control de lente,** denominadas PTZ cámaras motorizadas, permiten ser controladas por los controles a distancia, girándolas arriba, abajo, izquierda y derecha, algunas permiten acercar y alejar la imagen.

- **Cámaras para exteriores.-** Las cámaras para exteriores están preparadas para soportar las inclemencias meteorológicas, tales como humedad, viento, agua. Asimismo, muchas de las cámaras interiores se pueden adaptar al exterior a través de accesorios, tales como carcasas de seguridad.

- **Cámaras de visión nocturna.-** Las cámaras de visión nocturna son cámaras que incorporan leds infrarrojos que permiten vigilar bajo la obscuridad como la descrita anteriormente, en la obscuridad la imagen se visualiza en blanco y negro nos permite una mayor resolución.
- **Cámaras inalámbricas.-** Las cámaras inalámbricas son muy pequeñas, que están compuestas por la propia cámara y un receptor de radiofrecuencia que se conecta a un televisor o bien a un video-grabador a través de un receptor."
- **Cámaras IP.-** Las cámaras Ip son cámaras que permiten trabajar su señal de video a través de una red local o internet gracias a que las mismas incorporan internamente todos los dispositivos de transferencia de imagen y procesamiento de la misma, que ha dado lugar a una nueva tecnología: video vigilancia por IP, es de muy fácil montaje y existen varios tipos de las mismas.

2.3.3.5 GRABADOR DE VIDEO DIGITAL

Un grabador de video digital como se muestra en la fig. 2.8 es más conocido por sus siglas DVR(Digital Video Recorder), es un dispositivo que internamente incorpora un sistema de grabación de video en formato digital, este se compone de hardware y software destinado para la conexión y comunicación con video cámaras analógicas que transfieren imagen y en algunos casos audio, las mismas se pueden configurar para la detección de movimiento y por otra el software, que proporciona diversas funcionalidades para el tratamiento de las secuencias de vídeo recibidas, acceso a guías de programación y búsqueda avanzada.

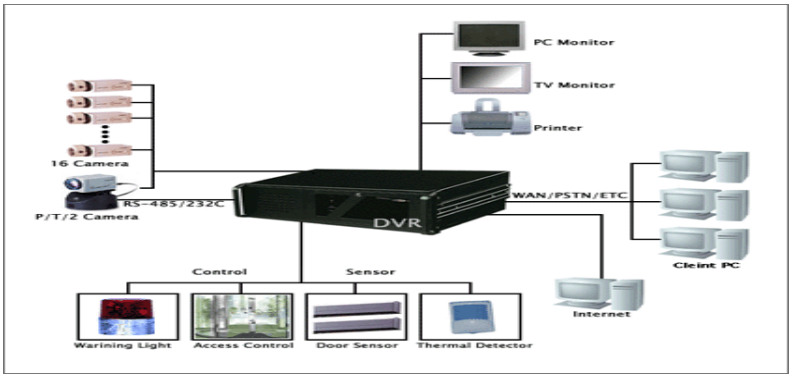


Fig. 2.8: DVR

Fuente: http://www.vigicam.cl/dvr.htm

2.3.3.6 GRABADOR DE VIDEO EN RED

El grabador de video en red con sus siglas de NVR (network video recorder) toma la entrada de vídeo a través de una red, en lugar de conectar directamente a un DVR que es codificado y procesado en el DVR, mientras que el video en un NVR se codifica y se procesa en la cámara, y va directo a la NVR para su almacenamiento o visualización remota.

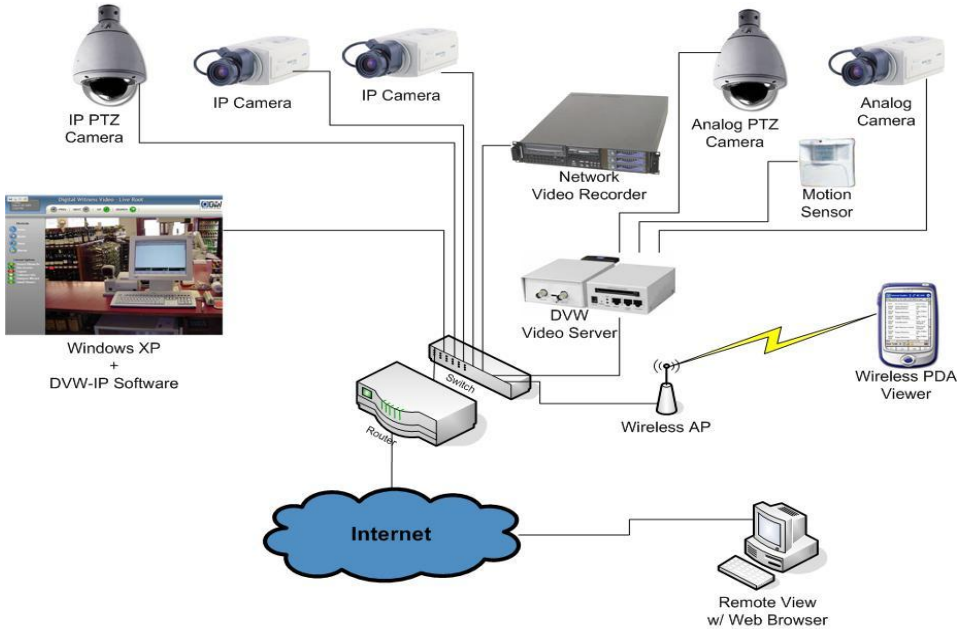


Fig. 2.9: DVR en red e Internet

Fuente: http://www.labass-investigations.com/nvr.htm

Un NVR se conecta en conjunto como se muestra en la fig. 2.9 donde es el encargado de enlazar el sistema de video vigilancia de un edificio a la nube de internet para visualizarlo remotamente, además el DVR no contiene ningún tipo de hardware de captura de vídeo dedicada. Sin embargo, el software normalmente se ejecuta en un dispositivo dedicado, por lo general con un sistema operativo integrado. Existen sistemas híbridos que incorporan funciones de ambos una NVR y DVR, estos son por lo general también se conoce como NVR.

2.3.3.7 TIPOS DE LECTORES DE IDENTIFICACIÓN

El control de acceso necesita obligatoriamente la autorización de apertura de una entrada, en esta etapa se presentan distintos tipos de dispositivos electrónicos que activan el sistema concediendo el acceso entre estos tenemos los siguientes.

2.3.3.8 LECTOR BÁSICO (NO INTELIGENTE)

El lector básico se conecta directamente a un sistema informático, que funciona en conjunto con un computador, es compatible con los distintos sistemas operativos como Windows, GNU Linux, Mac OS, en fig. 2.10 se observa un lector básico RF Tiny fabricado por Prox Point, el lector de tarjetas de proximidad es capaz de leer el número de tarjeta o PIN y lo remite a un panel de control en tiempo real.

Fig. 2.10: Lector Básico (RF Tiny RF LOGICS, Prox Point HID)

Fuente: http://www.consumer.es/tecnologia/hardware//07/15/177799.php

2.3.3.9 LECTORES SEMI-INTELIGENTES

Los lectores semi-inteligentes a diferencia de los básicos incorporan todas las entradas y salidas necesarias para controlar el hardware de la puerta de bloqueo, contacto de puerta, botón de salida, pero no tomar ninguna decisión de acceso.

Fig. 2.11: Lectores Semi-inteligentes InfoProx™ Lite IPL200/IPL210

Fuente: http://www.consumer.es/web/es/tecnologia/hardware/.php

Cuando un usuario presenta una tarjeta o ingresa un PIN, el lector envía la información a su sistema informático de control, como lo hace el lector Lite IPL200/IPL210 que se observa en la fig. 2.11 que se conecta a través de un RS-485 de autobús, esperando la respuesta de aprobación para la apertura del sistema.

2.3.3.10 LECTORES INTELIGENTES

Igual que el Semi-inteligente a los lectores que están conectados a un panel de control a través de un bus RS-485 o por conexión de puerto de red. De ahí envía las actualizaciones de configuración y eventos que suceden periódicamente.

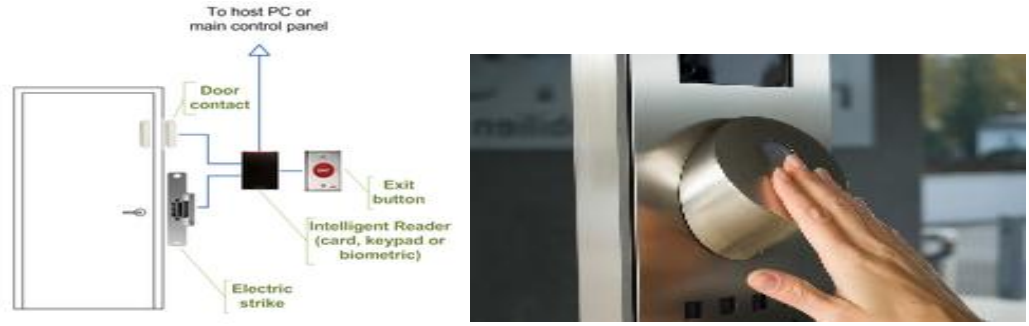


Fig. 2.12: Lectores Inteligentes (topología, Info Prox IPO200)

Fuente: http://www.cemsys.com/pressreleases.php?id=35

En la fig. 2.12 se detalla el lector biométrico Info Prox IPO200 que tiene todas las entradas y salidas necesarias para controlar el hardware de la puerta, también tienen memoria y potencia de procesamiento para tomar decisiones de forma independiente para conceder el acceso.

2.3.3.11 SOFTWARE DE CONTROL DE ACCESO

El software o paquete de seguridad es subministrado por la empresa que distribuye todo el paquete de seguridad, los dispositivos son compatibles con los distintos sistemas operativos, y no funcionara con otro a menos que este estandarizado y evaluado con otros sistemas de uso gratuito los cuales existen por cientos en internet.

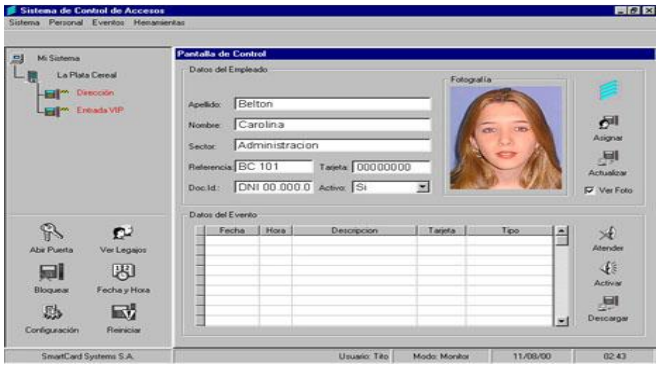


Fig. 2.13: Software especializado en control de accesos

Fuente: http://www.scssa.com.ar/control-de-acceso.htm

Muchas empresas suelen contratar paquetes especializados de software como se observa en la fig. 2.13, estos sistemas se encargan de reforzar la seguridad en su sistema de base de datos, cuando se trata de operar con algún tipo de software de seguridad siempre es mejor que lo haga un especialista en sistemas, para así ahorrarnos el riesgo que corremos de cometer algún error y producir alguna falla en el sistema entero de la empresa.

En la base de datos se puede almacenar distintos tipos de información, como nombre, cedula, tipo de sangre, entre otros, la información personal de las personas de las que trabajan en tareas de aseo y limpieza, y en caso de pérdida a través del software poder bloquear la identificación y asignar una nueva. . Los registros de ingreso serán manejados por bases de datos dedicados de cada programa que se instalen en la empresa.

2.3.3.12 ZONAS VULNERABLES

Una zona vulnerable es un lugar de una empresa, local, edificio, donde existe riesgo de robo o pérdida de objetos como se observa en la fig. 2.14 donde un delincuente roba un auto en un estacionamiento al no tener protección, pueden ser substraídos fácilmente, donde una persona sin vigilancia pueda hacer de las suyas.

Fig. 2.14: Zonas de vulnerable a robo

Fuente: http://www.definicionabc.com/general/robo.php

Para detectar cuáles son las vulnerabilidades de tu empresa, lo primero que debemos hacer es un diagnóstico de cómo están las siguientes áreas:

- Espacio físico en donde existen objetos de valor y no hay vigilancia.
- Espacios físicos donde existe acumulación de personas.
- Donde se encargan objetos de valor.
- Donde no existe una iluminación inadecuada.
- Lugares de fácil acceso.

La capacidad de prevenir dichos eventos se da gracias a la tecnología actual, se puede identificar los riesgos que llevan a las zonas a ser vulnerables y tomar en cuenta lo siguiente:

- Sistema de alarmas y video vigilancia.
- Personal de seguridad privada.
- Selección de empleados de alta confianza.
- Resguardo de la administración y zona de cobro de la empresa
- Resguardo de información contable de la empresa.

Para evitar los incidentes de diferentes tipos se opta por aplicar técnicas de seguridad previa un análisis de la zona.

Se deben tomar en cuenta las principales zonas vulnerables en nuestro caso:

Bóveda, Cajero, Recepción, Habitaciones, zonas vip, bar, accesos internos a pasillos, accesos externos al establecimiento.

2.3.3.13 TIPOS DE IDENTIFICACIÓN

Las formas de identificación son objetos físico/tangible, un pedazo de conocimiento, o una faceta de ser físico de una persona, que permite un acceso individual a una instalación física dada o a un sistema de información computarizado.

2.3.3.14 TARJETA MAGNÉTICA

La identificación de una persona se realiza por la lectura electrónica de las pistas de una banda oscura magnéticamente codificada que suele estar colocada en el reverso de una tarjeta plástica, fabricada especialmente para un uso específico y largo tiempo de vida de la misma.

Fig. 2.15: Lectores de tarjetas para control de acceso

Fuente: http://www.archiexpo.es/prod/sss-siedle/lectores-de-tarjeta-magnetica-para-control-de-acceso-11224-322923.html

En la fig. 2.15 se observa un lector de tarjetas utilizado en el control de acceso a un área administrativa, la tarjeta la banda está compuesta por partículas ferromagnéticas incrustadas en una matriz de resina capaz de almacenar cierta cantidad de información mediante una encriptación determinada que polariza dichas partículas.

Las pistas o tracks de la banda magnética son grabadas o leídas mediante contacto físico al pasar las tarjetas a través de una cabeza lectora/escritora. Sus ventajas:

- económico
- fácil de usar por costumbre de las tarjetas bancarias
- fácil de codificar bajo demanda

2.3.3.15 SENSOR BIOMÉTRICO

Los sensores biométricos en especial de huella digital se encuentran presentes en varios dispositivos cuya función principal es la de conceder el acceso ya sea a información o a un lugar en específico, utilizando alta tecnología en el proceso de identificación con procesador interno para el proceso de información.

Fig. 2.16: Sensor biométrico para el control de acceso

Fuente: http://www.directindustry.es/prod/bioaccez-controls/sensores-biometricos-lectores-de-vena-dactilar-39706-396431.html

El lector biométrico de huella digital permite controlar que solo las personas autorizadas ingresen a determinadas áreas de su empresa, se instala en la puerta como se muestra en la fig. 2.16 conectado a un sistema informático. Este tipo de lector se utiliza para generar reportes de ingresos de personal a las bóvedas de bancos, centros de investigación, cárceles de máxima seguridad, entre otros.

2.3.3.16 IDENTIFICACIÓN POR RADIO FRECUENCIA

La identificación por radiofrecuencia es un sistema muy conocido en la actualidad se trata de un dispositivo donde se almacena información y se realiza la recuperación de datos de forma por decir inalámbrica mediante etiquetas que en su interior incorporan tags, transponer RFID que de forma electromagnética se graban y almacenan información. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio.

Fig. 2.17 Lector de tarjetas de proximidad mediante RFID

Fuente: http://www.hotfrog.es/Empresas/AIKE-Seguridad-y-Domotica_104646/Lectores-de-tarjetas-RFID-12443

Las tecnologías RFID se agrupan dentro de las denominadas Auto ID (identificación automática), su uso aumento en esta última década gracias a los grandes resultados que aporta su tecnología.

En la fig. 2.17 se muestra una etiqueta RFID pequeña que van adheridos a una tarjeta, similar a una pegatina, que puede ser adherida o incorporada a un producto, animal o una persona. Contienen antenas para permitirles recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID. Las etiquetas pasivas no necesitan alimentación eléctrica interna, mientras que las activas sí lo requieren. Una de las ventajas del uso de radiofrecuencia (en lugar, por ejemplo, de infrarrojos) es que no se requiere visión directa entre emisor y receptor. Según sus estándares tienen una distancia máxima para la transmisión, que varía de acuerdo al modelo y fabricante de la misma.

2.3.3.17 INTERFACES DE COMUNICACIÓN

Las interfaces de comunicación son herramientas que permiten manejar e intercambiar datos entre un computador y dispositivos de lectura o transmisión de datos, generalmente están integrados en la tarjeta madre de los mismos y sus diferentes periféricos, también permiten la intercomunicación entre dos computadores que tengan conexión para la trasmisión de datos, gracias a la tecnología actual se pueden utilizar adaptadores que transforman una señal a otra.

2.3.3.18 PUERTO SERIE

La comunicación serial consiste en el envío de un bit de información de manera secuencial, ésta es, un bit a la vez y a un ritmo acordado entre el emisor y el receptor. En la fig. 2.18 se observa la distribución de pines de datos que existen en el conector los cuales se encuentran estandarizados y se usan a nivel internacional.

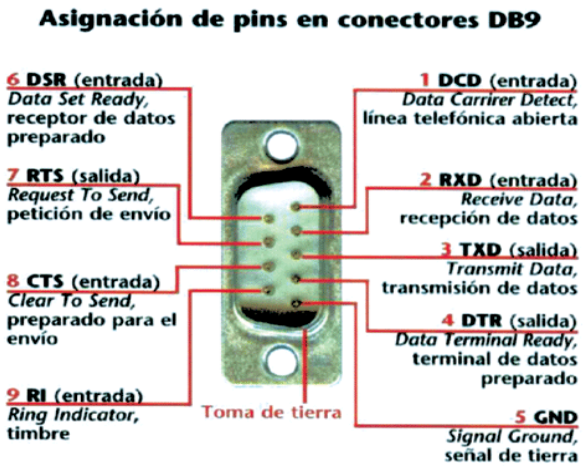


Fig. 2.18: Diagrama de conexión de un puerto serial DB9

Fuente: http://perso.wanadoo.es/pictob/comserie.htm

Un puerto serie o serial es una interfaz de comunicaciones de datos digitales, frecuentemente utilizado por computadoras y periféricos, donde la información es transmitida bit a bit enviando un solo bit a la vez, en contraste con el puerto paralelo que envía varios bits simultáneamente, existen adaptadores que permiten utilizar un puerto USB para este tipo de interfaz, debido a que algunos fabricantes no toman en cuenta el puerto para sus computadores.

2.3.3.19 PUERTO DE RED RJ45

Es un conector de forma especial que contiene 8 terminales de conexión que son utilizados para conexión entre dispositivos, en el computador viene en la mayoría de los casos incorporado a la tarjeta madre, para la conexión de área local, su velocidad de transmisión varía según el estándar y el protocolo de red, en los últimos años se ha optado por incluirlo en la mayoría de dispositivos de seguridad y otros para interactuar fácilmente con ellos mediante una red local e internet.

Fig. 2.19: Cámara de seguridad con puerto de red

Fuente: http://www.priceminister.es//camara-ip-h-264-con-wifi.html

También se lo encuentra en dispositivos de control de acceso como ejemplo la cámara de la fig. 2.19, donde se la observa desde una estación de video vigilancia que usa el monitoreo atreves de una conexión IP, la configuración permite que visualice remotamente desde cualquier parte del mundo.

2.3.3.20 SEGURIDAD

El concepto de seguridad para la empresa es variado y tiene varios conceptos, consecuentemente diversas aplicaciones y funciones. De pronto, encontramos distintas áreas y formas de seguridad: Seguridad e Higiene, Seguridad Industrial, Seguridad Patrimonial, etc. Lo que nos puede llevar a la confusión. Sin duda es muy importante que se deba procurar la adecuada administración de todas ellas para lograr la seguridad integral de la empresa.

Las normas y reglas de seguridad se especifican de acuerdo al lugar y decisión del personal encargado del resguardo en una empresa.

En todas las empresas se involucra el concepto de seguridad, independientemente de que esta área se lleve a cabo en forma adecuada o inadecuada, sin antes realizar estudios previos, y con la ayuda de profesionales en el área.

2.3.3.21 REGLAS Y NORMAS DE SEGURIDAD

Los sectores turísticos cuentan con hoteles de primera clase en donde se alberga una gran cantidad de turistas en especial extranjeros, resulta de suma importancia definir y acotar que dentro del establecimiento los huéspedes cuentan con un plan de seguridad que garantiza su estadía tomando en cuenta los siguientes literales:

- ¿El Huésped percibe la seguridad del establecimiento?
- ¿El hotel utiliza la seguridad en su estrategia de promoción al mercado?
- ¿El personal le hace percibir la seguridad del establecimiento al huésped?

Como respuesta a las interrogantes formuladas se toma en cuenta:

- **Filosofía:** se entiende por filosofía a un concepto motivacional permanente que orienta a la institución y a cada departamento de la misma a lograr sus objetivos orientados a satisfacer las necesidades de los huéspedes.
- **Normas:** Es el conjunto de pautas o reglas sobre el que se basa el funcionamiento de la empresa y en especial el departamento de seguridad.
- **Organización:** es el sistema de seguridad que permite la materialización del objetivo la seguridad del establecimiento y sus huéspedes.

La seguridad hotelera se debe considerar desde dos puntos de vista:

Desde el Huésped del establecimiento: su desplazamiento por motivos turísticos tiene una necesidad básica que es la búsqueda de un estado de bienestar integral, por lo que busca una total seguridad durante su desplazamiento y la falta de la misma le genera miedo.

La inseguridad es una variable de valoración totalmente subjetiva, ya que es interpretada de distinta manera de acuerdo al segmento del que se forma parte la tercera edad le da un determinado valor que es distinto al segmento de jóvenes y difiere del segmento de segunda edad.

El Huésped entiende que la seguridad es una parte intrínseca del servicio en el hotel donde se hospedan, por eso en el proceso de construcción se debe:

- Intervenir en el proceso de diseño arquitectónico y urbanístico del hotel relacionado a la seguridad.
- Establecer las normas de seguridad del establecimiento.
- Implementar la inspección de seguridad durante el funcionamiento del mismo.
- Llevar un análisis estadístico sobre seguridad (Identificar las tendencias)

Del sistema hotelero hacia el huésped:

- El componente humano corresponde a los recursos humanos relacionados en forma directa o indirecta con la seguridad en el establecimiento
- El componente tecnológico está basado en la infraestructura y equipamiento técnico con fines preventivos y predictivos de protección activa y pasiva.
- El rango de equipamiento tecnológico va desde un control de accesos hasta llegar a lo que podemos denominar como "edificio inteligente".

2.3.3.22 MANUAL DE PROCEDIMIENTOS

El modelo metodológico de la implementación del sistema de seguridad está basado en la elaboración de un Plan Director de Seguridad. Este plan debe estar integrado por un conjunto de programas con procedimientos analíticos, de inteligencia y operativos que permitan prevenir y detectar cualquier actividad no deseada en el establecimiento.

2.3.3.23 IDENTIFICACIÓN Y AUTENTIFICACIÓN

Se denomina Identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación y como respuesta una acción de consentimiento o reprobación.

Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas, como en los siguientes casos:

- Clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN.
- Varios tipos de tarjetas de identificación como ejemplos, tarjeta de banda magnética, tarjeta de proximidad RFID.
- Huellas digitales o la voz, reconocimiento facial.
- Patrones de escritura, reconocimiento de caracteres.

2.3.3.24 INTEGRIDAD DE DATOS

La integridad de datos viene siendo desde hace mucho tiempo muy importantes para la constitución de una empresa, la cual dispone de datos potencialmente deseados por la competencia, los cuales al tenerlos a mano infringen un peligro por la manipulación de los mismos, debido a eso se toma en cuenta un plan para proteger la integridad de datos, como los que se incluyen a continuación:

- **Normalización de datos**
    - Explica el proceso que consiste en perfeccionar las definiciones de datos para eliminar grupos repetidos y dependencias innecesarias.
- **Reglas de empresa para el acceso a datos**
    - Explica la forma en que las reglas de empresa controlan la manipulación de los datos y quien tiene acceso a los mismos.
- **Integridad referencial**
    - Describe la forma en que la integridad referencial evita que se dañen los datos.
- **Validación de datos**
    - Explica la comprobación de intervalos, la validación de campos y formas más complejas de validación de datos.

En la actualidad existen soluciones informáticas que permiten fácilmente proteger los datos con encriptaciones de seguridad que imposibilitan obtener los mismos sin tener la debida autorización para la manipulación de los mismos.

2.3.4 Hipótesis

La falta de una propuesta de control de acceso afecta a la seguridad de dormitorios y áreas restringidas del Hotel Destiny.

2.3.5 Señalamiento de Variables

2.3.5.1 Variable independiente

Control de acceso

2.3.5.2 Variable dependiente

Seguridad de dormitorios y áreas restringidas

CAPITULO III

METODOLOGÍA

3.1 Enfoque

El presente proyecto de investigación "Control de acceso para la dotación de seguridad en dormitorios y áreas restringidas en el Hotel Destiny" tuvo un enfoque cuali-cuantitativo, porque el investigador se involucró directamente en el tema, analizo, tomo decisiones y planteo una propuesta de seguridad de acuerdo a los requerimientos técnicos que presento el Hotel, con el asesoramiento proporcionado por el tutor y encargado del diseño de la parte tecnológica en el Hotel.

3.2 Modalidad de la investigación

3.2.1 Investigación de campo

El investigador estuvo en contacto directo con el problema "deficiente control de acceso en dormitorios y áreas restringidas", por lo cual fue necesario obtener la mayor cantidad de información de acuerdo a los objetivos del proyecto tanto fuera como dentro de la empresa.

3.2.2 Investigación Bibliográfica - Documental

La recopilación de información fue bibliografía – documental, se revisó información de diversos autores, documentos de funcionamiento de distintos equipos, manuales de software, los cuales permitieron tener un criterio de comparación de características técnicas, físicas, económicas, con lo que se seleccionó dichos equipos que brindan el control de acceso y cumplió las necesidades que se plantearon en la solución del problema.

3.3 Nivel de Investigación.

En el presente proyecto se realizó los siguientes niveles de investigación:

Exploratorio.- Nos permite conocer las características del problema, estudiar la realidad del entorno, teniendo una visión clara del entorno.

Descriptivo.- Permite comparar posibles soluciones al problema, predecir los distintos comportamientos de los distintos controles de acceso.

Explicativo.- Se dirige a responder las causas de los eventos que conllevan el problema.

3.4 Población y Muestra

3.4.1 Población

El presente trabajo de investigación se realizó en el Hotel Destiny y la población con la que se trabajó fue; los propietarios del Hotel, encargados de la construcción, Hoteles y hostales de prestigio en la zona, que no contaron más allá de 20.

POBLACIÓN	NUMERO
Propietarios	2
Encargados de la construcción	3
Hoteles y hostales aledaños	15
Total	20

Tabla 3.1: Datos de la muestra

3.4.2 Muestra

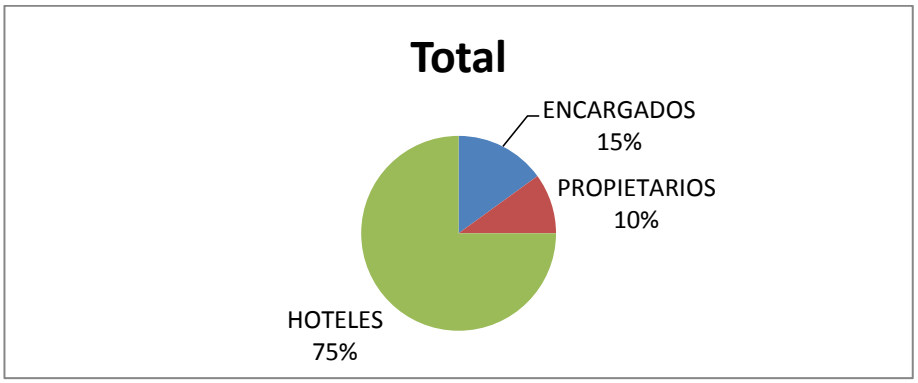


Fig. 3.1: Datos de la muestra a investigar

Realizado por el investigador

Como la población es reducida se trabajó con todo el universo.

3.5 Operacionalización de Variables

Conceptualización	Dimensiones	Indicadores	Ítems	Técnica - Instrumento
Control de Acceso: Es un sistema electrónico con el cual controlamos entradas y salidas permitiendo conocer quien entra cuando entra y a donde entra cada individuo autorizado en el sistema de registro.	Sistema de información computarizado. Infraestructura del control de acceso	• Software para el Control • Base de datos • Información del individuo • Equipos • Topología • Tipos de identificación. • Autentificación	¿Qué métodos de control de acceso utiliza para la seguridad de su establecimiento? ¿Conoce usted algún tipo de software (programa) de seguridad para el control de acceso? ¿Considera usted que es importante la presentación de identificación de los individuos que ingresan y se hospedan en su establecimiento? ¿Estaría dispuesto a tomar medidas de seguridad implementando equipos de control de acceso en su establecimiento? ¿Usted lleva un registro de las personas que ingresan a su establecimiento?	• Técnica: Encuesta, entrevista, observación directa • Instrumento: Cuestionarios, Ficha de campo

Tabla 3.2: Operacionalización de la Variable Independiente

Realizado por el investigador

Conceptualización	Dimensiones	Indicadores	Ítems	Técnica - Instrumento
Seguridad En Dormitorios Y Áreas Restringidas: Permite el control de intrusos a lugares o áreas donde existan objetos o pertenencias de valor.	Accesos internos Accesos externos	• Zona de alta seguridad • Zona de media seguridad • Zona de baja seguridad • Zonas de circulación • Zonas circunvecinas	¿Dentro de un establecimiento cuales son las principales zonas vulnerables a la delincuencia? ¿En los alrededores de su propiedad se han suscitado actos delictivos? ¿En el diseño de la edificación que criterios técnicos se consideraron para dotar de seguridad al edificio? ¿Considera usted que la seguridad es importante para la reputación de su establecimiento?	• Técnica: Encuesta, entrevista, observación directa • Instrumento: Cuestionarios, Ficha de campo

Tabla 3.3: Operacionalización de la Variable Dependiente

Realizado por el investigador

3.6 Recolección De La Información

3.6.1 Plan de recolección de la Información

Para la recolección de la información, se realizaron encuestas a los Hoteles y Hostales turísticos aledaños, empleando como técnica la encuesta ya que el presente trabajo se va a realizo como solución al problema y fue necesario conocer la situación actual de la inseguridad que viven los hoteles de la ciudad de Baños.

3.6.2 Procesamiento de la Información

1.- Revisión de la información

2.- Tabulación

3.- Estudio estadístico

4.- Gráficos

3.6.3 Análisis e interpretación de la información

1.- Análisis de los resultados

2.- Interpretación

4.- Conclusiones y Recomendaciones

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Situación actual

En la Fig. 4.1 se muestra el Hotel Destiny en su fase anterior de construcción tanto la infraestructura como el presupuesto, fueron asignados para la compra y diseño del control de acceso y video vigilancia.

Fig. 4.1 Hotel Destiny en fase de construcción

Elaborado por el investigador

Ciertas modificaciones fueron realizadas en el interior, para la dotación de los distintos equipos que funcionarán en el área de control que se construirá conforme avance la obra en la edificación.

Fig. 4.2 Conductos para el cableado

Realizado por el investigador

Antes de la terminación del proceso de construcción como se muestra en la fig. 4.2 en el interior, se logró adecuar conductos de tubería para el sistema de cableado C.C.T.V. (Circuito Cerrado de Televisión) que complementa el control de acceso en el hotel, solo queda la elección de equipos que entren en el presupuesto asignado para la compra de los dispositivos.

4.2 Análisis de resultados

Los datos obtenidos en esta investigación se adquirieron a través de unas encuestas realizadas en el sector hotelero de la ciudad de Baños, los mismos que fueron tabulados de acuerdo a las preguntas planteadas, analizadas e interpretadas de forma ordenada como se podrá observar a continuación.

4.3.1 Encuesta dirigida a Hoteles y Hostales de la Ciudad de Baños

Total de la muestra encuestada: 15 (Hoteles y Hostales)

El objetivo de la presente encuesta es para recopilar información sobre el deficiente control de acceso en dormitorios y áreas restringidas que presentan los distintos establecimientos dentro del perímetro central.

4.3.1.1 Pregunta 1

¿Cómo califica usted la seguridad en el interior de los dormitorios y áreas restringidas de su establecimiento?

- Excelente ☐ Buena ☐ Regular ☐

RESPUESTAS	CANTIDAD	PORCENTAJE
Excelente	3	20%
Bueno	5	33%
Regular	7	47%
Total	**15**	**100%**

Tabla 4.1 Pregunta 1

Elaborado por el investigador

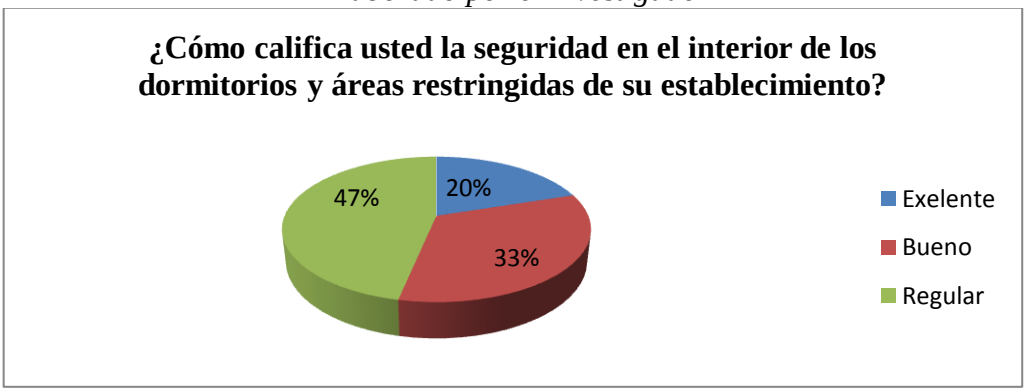


Fig. 4.3 Grafico estadístico (Pregunta 1)

Elaborado por el investigador

Análisis e interpretación:

En la pregunta 1 el 47% de los dueños o encargados de los Hoteles y Hostales manifiesta que la seguridad en el interior y áreas restringidas es regular lo que indica que habrá un descontento por parte de los huéspedes en caso exista perdida ya que no se toman medidas adecuadas indispensables , el 33% indica que existe un buen control de seguridad pero no lo suficiente para cumplir con la demanda, el 20% es consiente que existe una excelente seguridad lo que indica una buena imagen, protección y confianza con los huéspedes.

Conclusión:

Después de un análisis se puede notar que existe un descuido por parte de los Hoteles y Hostales que no toman la seguridad como una norma principal de atención al cliente lo cual afecta directamente al establecimiento y consecuentemente al huésped que hará notar la mala imagen que tiene un hotel en caso exista una perdida.

4.3.1.2 Pregunta 2

¿Conoce usted algún tipo equipo o software (programa) de seguridad para el control y supervisión de personas que se hospedan en su establecimiento?

- Si ☐
- No ☐

RESPUESTAS	CANTIDAD	PORCENTAJE
Si	4	27%
No	11	73%
Total	**15**	**100%**

Tabla 4.2 Pregunta 2

Elaborado por el investigador

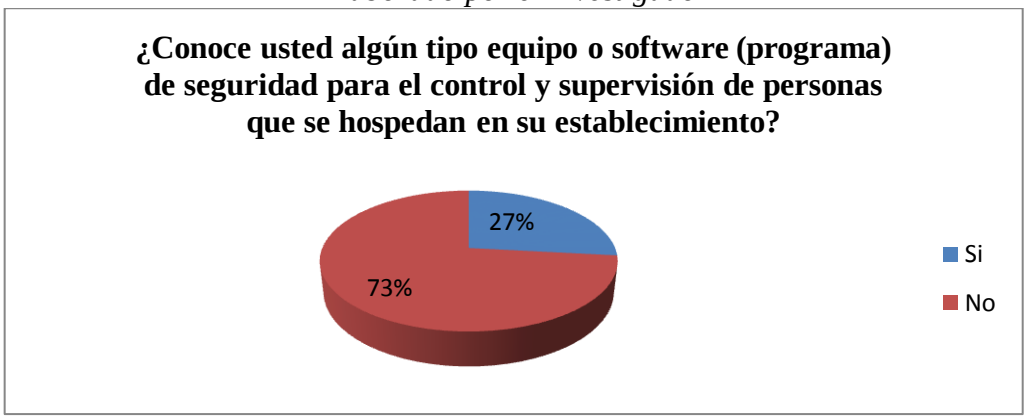


Fig. 4.4 Grafico estadístico (Pregunta 2)

Elaborado por el investigador

Análisis e interpretación:

En la pregunta 2 el 73% de los dueños y encargados presentes en el momento de la encuesta aseguraron que no usaban ni conocían ningún programa de control, en el cual solo registran en cuadernos en el mejor de los casos, el otro 27% indica que si usan programas para la supervisión y control de sus huéspedes, esto se da en hoteles de mayor categoría por salvaguardar la integridad de los huéspedes.

Conclusión:

Podemos concluir que el ambiente hotelero entre sus puntos débiles ante la seguridad en la mayor parte no cuenta con un correcto sistema de supervisión de huéspedes, la gran mayoría no muestra interés por corregir esto, produciendo inseguridad en el interior del establecimiento propenso a pérdidas de objetos, es necesario dotar de un sistema donde se pueda controlar las áreas donde existe afluencia de personas.

4.3.1.3 Pregunta 3

¿Al momento del ingreso de huéspedes usted solicita algún tipo de identificación para el registro del mismo?

- Si ☐
- No ☐

RESPUESTAS	CANTIDAD	PORCENTAJE
Si	9	60%
No	6	40%
Total	**15**	**100%**

Tabla 4.3 Pregunta 3

Elaborado por el investigador

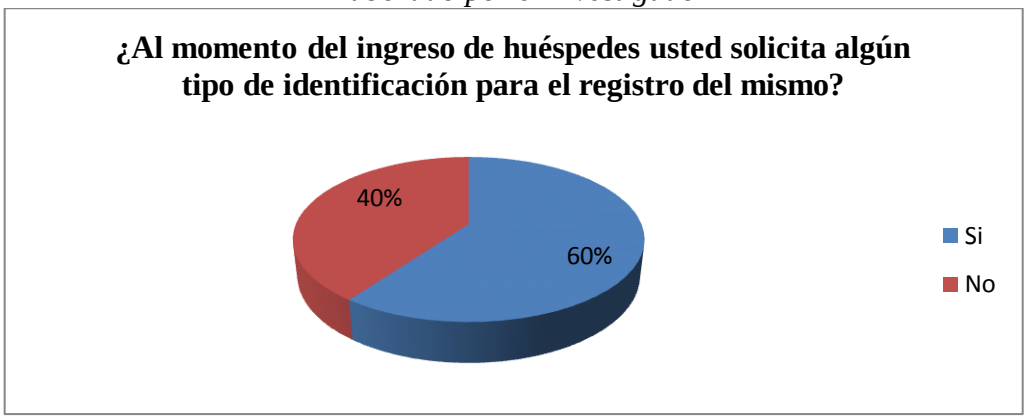


Fig. 4.5 Grafico estadístico (Pregunta 3)

Elaborado por el investigador

Análisis e interpretación:

En la pregunta 3 el 60% de los dueños y encargados aseguraron que si solicitan identificación antes del ingreso de huéspedes debido a que se han suscitado actos delictivos dentro de los establecimientos, el otro 40% no lo hace en parte porque los huéspedes son ocasionales por cortos periodos de tiempo.

Conclusión:

Se puede concluir que los establecimientos hoteleros se manejan de distintas maneras, la mayoría solicita identificación al momento del ingreso de los huéspedes pero cuando las personas se quedan por un corto periodo de tiempo no lo hacen, esto causa inseguridad ya que al no conocer la identidad de los hospedantes pueden existir actos delictivo, es necesario contar con la identificación de todos los huéspedes para brindar seguridad a los demás.

4.3.1.4 Pregunta 4

¿Estaría dispuesto a tomar medidas de seguridad implementando equipos de control de acceso en su establecimiento?

- Si ☐
- No ☐

RESPUESTAS	CANTIDAD	PORCENTAJE
Si	10	67%
No	5	33%
Total	**15**	**100%**

Tabla 4.4 Pregunta 4

Elaborado por el investigador

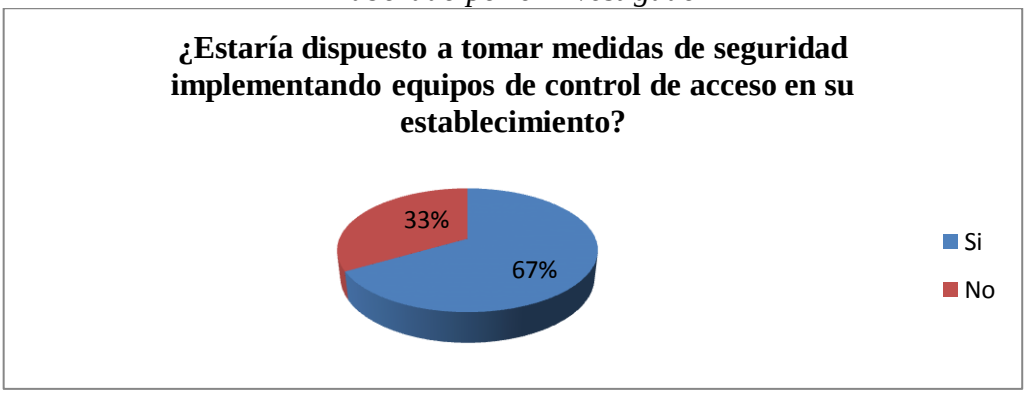


Fig. 4.6 Grafico estadístico (Pregunta 4)

Elaborado por el investigador

Análisis e interpretación:

En la pregunta 4 el 67% de los encargados les gustaría contar con sistema de control de acceso como puntos principales, el fácil resguardo de habitaciones y áreas restringidas por otra parte el fácil uso y administración en vez de llaves entre otros, el otro 33% indica que no es necesario debido a que sus establecimientos son de baja categoría y la tecnología no va con ellos.

Conclusión:

Se puede ver que la gran mayoría está interesado en contar con un control de acceso debido a que facilita en muchos aspectos la funcionalidad de la administración de habitaciones en donde se puede dar el aseo con una sola identificación en caso de pérdida una fácil asignación de identificación, es necesario contar con un control de acceso para fortalecer la seguridad y la administración de las distintas áreas.

4.3.1.5 Pregunta 5

¿Realiza usted una supervisión semanal o mensual de los objetos en cada habitación y área restringida después del ingreso del personal de aseo o de los huéspedes?

- Si ☐
- No ☐

RESPUESTAS	CANTIDAD	PORCENTAJE
Si	12	80%
No	3	20%
Total	**15**	**100%**

Tabla 4.5 Pregunta 5

Elaborado por el investigador

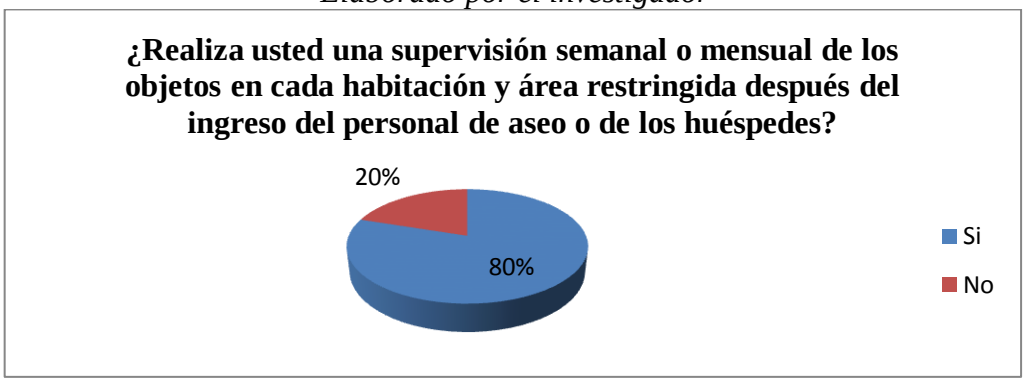


Fig. 4.7 Grafico estadístico (Pregunta 5)

Elaborado por el investigador

Análisis e interpretación:

En la pregunta 5 el 80% de los encargados si realiza una supervisión de los objetos y pertenencias de cada habitación en especial de las áreas restringidas debido a que frecuentemente se cambia el personal de aseo y no cuenta con la suficiente confianza, por otra parte apenas el 20% de los encargados no realiza una supervisión de los objetos en cada habitación y áreas.

Conclusión:

Se puede concluir que los encargados de los establecimientos si realizan la adecuada supervisión en habitaciones y áreas restringidas donde garantizan seguridad de sus propias pertenencias solo una mínima parte no lo hace porque cree que en verdad no poseen artículos que sean de valor en su interior, en el hotel ya que al ser de alta categoría se contara con artículos de valor es necesario este tipo de control con video vigilancia u otros métodos.

4.3.1.6 Pregunta 6

¿Dentro de su establecimiento el personal dedicado al resguardo de la seguridad es?

- Suficiente ☐
- Poco ☐
- Insuficiente ☐

RESPUESTAS	CANTIDAD	PORCENTAJE
Suficiente	5	33%
Poco	7	47%
Insuficiente	3	20%
Total	**15**	**100%**

Tabla 4.6 Pregunta 6

Elaborado por el investigador

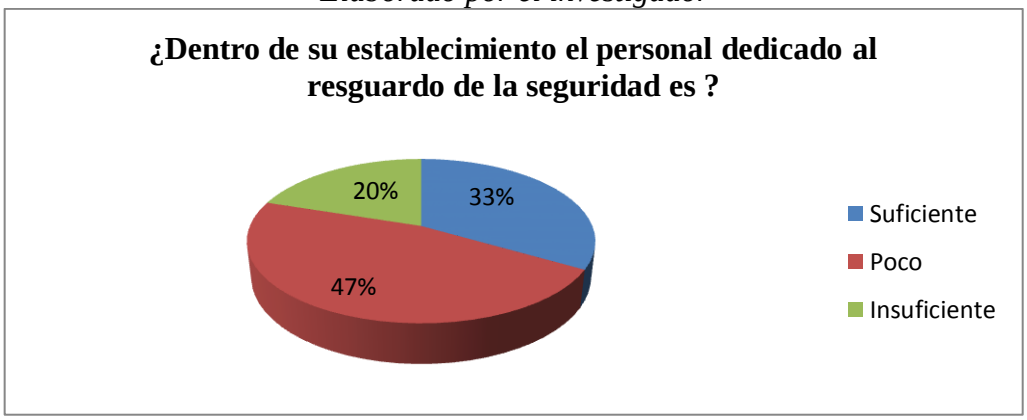


Fig. 4.8 Grafico estadístico (Pregunta 6)

Elaborado por el investigador

Análisis e interpretación:

En la pregunta 6 el 47% de los encuestados calificaron como poca la seguridad que tienen dentro de sus instalaciones, el 33% lo califica como suficiente y un 20% califico como insuficiente la seguridad en dormitorios y áreas restringidas.

Conclusión:

Se puede concluir que en la mayor parte de encuestados sí presta atención a la seguridad sin embargo un bajo porcentaje no toma atención en prestar medidas de seguridad dentro de sus establecimientos debido a la falta de presupuesto en alguno de los casos, o que sus establecimientos son pequeños y es fácil el control de seguridad, se puede tomar algunas alternativas para el control de seguridad con ayuda de personal o soluciones tecnológicas.

4.3.1.7 Pregunta 7

¿En el interior de su establecimiento y los alrededores se han suscitado actos delictivos?

- Sí ☐
- No ☐

RESPUESTAS	CANTIDAD	PORCENTAJE
Sí	12	80%
No	3	20%
Total	**15**	**100%**

Tabla 4.7 Pregunta 7

Elaborado por el investigador

Fig. 4.9 Grafico estadístico (Pregunta 7)

Elaborado por el investigador

Análisis e interpretación:

En la pregunta 7 el 80% indica que se han suscitado actos delictivos dentro y fuera del establecimiento mostrando el riesgo existente en la zona, el 20% indica que no se han producido actos delictivos.

Conclusión:

Se concluye que un alto porcentaje de establecimientos se ha visto afectado por la delincuencia que hay en la ciudad de Baños la mayor parte indica que no es permanente sino que se presenta en días de alta concentración de personas y en las noches de los fines de semana, el otro porcentaje indica que no ha sido víctima de los amigos de lo ajeno por estar en zonas en donde existe una vigilancia permanente, al existir este riesgo hay que tomar medidas de precaución la mayor parte del tiempo garantizando la conformidad de los huéspedes.

4.3.1.8 Pregunta 8

¿Considera usted que la seguridad es importante para la reputación de su establecimiento?

- Si ☐
- No ☐

RESPUESTAS	CANTIDAD	PORCENTAJE
Si	11	73%
NO	4	27%
Total	**15**	**100%**

Tabla 4.8 Pregunta 8

Elaborado por el investigador

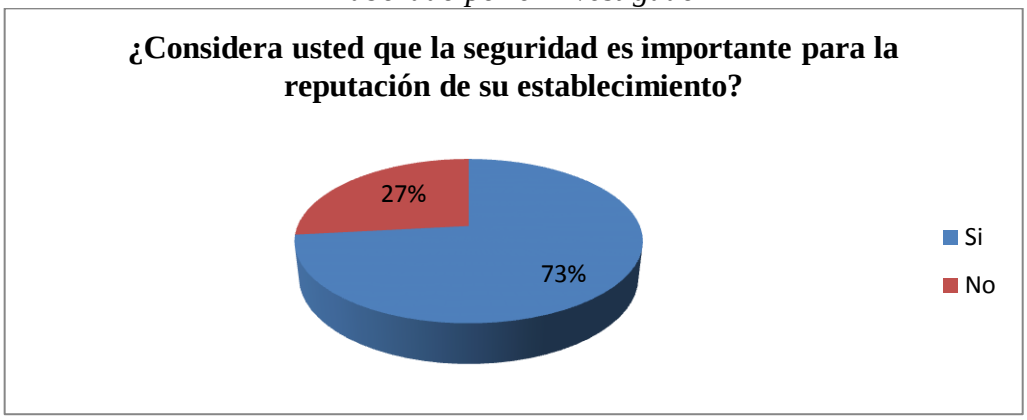


Fig. 4.10 Grafico estadístico (Pregunta 8)

Elaborado por el investigador

Análisis e interpretación:

En la pregunta 8 el 73% de los encuestados indica que al tener como un servicio indispensable la seguridad es de gran importancia para mantener y mejorar la reputación de sus establecimientos, mientras que el 27% mantiene una propuesta negativa a los clientes al no interesarse por la seguridad de los mismos.

Conclusión:

En la actualidad se practica una libre competencia, al ofrecer servicio de hospedaje es primordial para el prestigio de los establecimientos contar con medidas de seguridad para salvaguardar la integridad de sus huéspedes y ellos siempre se sentirán atraídos por estos beneficios que presten los distintos sitios de hospedaje en la ciudad, al ser pretender tener un hotel con tecnología de punta se escogerán los equipos adecuados que cumplan con las funciones de seguridad.

4.3.2 Análisis de requerimientos

Antes de empezar con la propuesta se realizó una entrevista al encargado del diseño eléctrico, de la construcción y encargado de la instalación eléctrica además a los propietarios del mismo, cabe decir que la entrevista se la hizo hace 8 meses atrás cuando el edificio estaba en construcción debido a que se podían hacer modificaciones previas a la terminación de acabados en el interior.

El principal objetivos fue establecer los puntos exactos de equipos que tienen que estar presentes antes de la instalación del control de acceso y sistema cerrado de televisión.

La entrevista se basa en 8 preguntas acerca de la infraestructura y la planeación que existe en el cableado, al final de cada pregunta se realizó el análisis e interpretación respectiva sobre las respuestas obtenidas donde se establece conclusiones confiables para el presente proyecto.

4.3.2.1 PREGUNTA 1: ¿En el diseño de la edificación que criterios técnicos se consideraron para dotar de seguridad al edificio?

Los entrevistados manifestaron en la mayor parte que el edificio contaría con una alarma de sensor de movimiento, un máximo de 4 cámaras en toda la infraestructura y además la contratación de un guardia para la supervisión del mismo sin pensar de los actos delictivos que se pueden dar en el interior y exterior del Hotel.

Análisis e interpretación:

Según se puede entender existe un leve conocimiento de acontecimientos delictivos que pueden suceder en el interior de un hotel, al mantener un índice de huéspedes extranjeros poseen pertenencias de valor por lo cual es necesario supervisar todo tipo de actividad en el interior para prevenir la perdida, es necesario contar con un sistema de video vigilancia además del control de acceso con registro de identificaciones.

4.3.2.2 PREGUNTA 2: El hotel cuenta con la infraestructura para la instalación de equipos de seguridad.

Según manifiestan los encargados de la construcción si se tomó en cuenta ductos extra en caso de adaptación de un sistema de seguridad pero nunca se pensó en un cuarto de control para la misma, además solo están centralizadas en cada piso no existen puntos exactos donde estén ubicadas cámaras o cualquier tipo de control.

Análisis e interpretación:

Gracias a la decisión del constructor se cuanta con los ductos para el sistema de video vigilancia es necesario elegir los puntos de control además de un cuarto de equipos donde este centralizado cualquier tipo de sistema que se utilice.

4.3.2.3 PREGUNTA 3: En la planificación de la construcción se estableció un cuarto para el control de equipos de seguridad y otros.

Dentro de los planos de construcción no se señala un lugar dedicado al área de control, las personas encargadas de la construcción manifiestan que no se estableció dicho cuarto de control.

Análisis e interpretación:

Antes de la implementación de cualquier sistema de control es necesario tener un espacio para los equipos en donde solo el administrador tenga acceso, es posible la planificación gracias a que se encuentra en construcción.

4.3.2.4 PREGUNTA 4: ¿En el interior de áreas restringidas como bodegas y administración se planifico algún tipo de seguridad especial?

Los encargado responden que si está planificado la seguridad mediante cerraduras especiales y sensores de movimiento porque almacena gran cantidad de objetos de valor como licores de marca y vajillas de porcelanito entre otros.

Análisis e interpretación:

Es necesario establecer exactamente los ambientes que necesitan un control más estricto de ingreso para esto se establecerá el acceso más controlado y según la necesidad cámaras con sensores de movimiento y grabación automática.

4.3.2.5 PREGUNTA 5: En la edificación se planifico zonas especiales en donde exista concentración de personas.

Según indican en el diseño existen zonas en donde se prestara servicio de computadoras con internet además de un bar y un comedor en donde es necesario que exista un control de seguridad.

Análisis e interpretación:

En el estudio de zonas vulnerables se planificara el resguardo mediante cámaras de alta definición para una más fácil identificación en caso de pérdidas.

4.3.2.6 PREGUNTA 6: En la planificación de recursos tecnológicos se tomó en cuenta un control de acceso a las habitaciones

Los encargados responden que no se tiene previsto ningún tipo de control más que los normales con cerradura normal y acceso a una llave después del registro en recepción.

Análisis e interpretación:

Según se asigne el presupuesto para la seguridad se podrá analizar equipos que ayuden al control de acceso en cada habitación, también en las zonas restringidas en donde existan objetos de pertenencia del hotel.

4.3.2.7 PREGUNTA 7: En la planificación administrativa el hotel contara o no con un plan de seguridad, para evitar perdida de objetos y robo

Según lo expuesto por los entrevistados el plan aún no se encuentra elaborado pero si se tiene previsto normas y reglas para que el personal de trabajo ayude al control de pérdidas de objetos

Análisis e interpretación:

El Hotel cuenta con 30 habitaciones capacidad para 120 huéspedes existe la necesidad de este tipo de plan de seguridad según se pueda establecer de acorde al tipo de necesidades que se presenten día a día.

4.3.2.8 PREGUNTA 8: En la planificación del hotel se dispone la instalación de un software especializado en resguardo y seguridad

Según manifiestan propietarios y encargados si se tiene planificada la instalación de software que ayude con el resguardo y seguridad solo es necesario escoger el tipo y aplicaciones de dicho programa.

Análisis e interpretación:

En este caso se puede realizar una comparación de los distintos tipos de programas que están en el mercado para ver el que cumpla con las necesidades que se establezcan en las políticas de seguridad.

CAPITULO V

5.1. CONCLUSIONES Y RECOMENDACIONES

5.1.1 Conclusiones

- Actualmente la ciudad de Baños recibe un alto índice de visitantes lo cual hace que sea vulnerable a actos delictivos, por lo cual es necesario contar con un sistema de seguridad interno como externo para prevenir cualquier tipo de violación a la seguridad.
- Es necesario llevar un registro de los accesos para identificar a él o los individuos que rompan las reglas establecidas de seguridad.
- Gracias a los datos obtenidos en las encuestas se puede concluir que tanto las áreas restringidas como las habitaciones, deben contar con un control de acceso debido a que siempre se reportan perdidas de objetos en áreas y zonas sin control.
- El Hotel cuenta con un presupuesto e infraestructura necesaria se puede empezar con la compra de equipos e implementación de un sistema cerrado de televisión y de control de acceso.
- Para el diseño e implementación se cuenta con toda la información necesaria de planos en donde se especifica cada área del Hotel.
- Es necesario la implementación de un circuito cerrado de televisión, en donde se pueda realizar detección de movimientos en áreas restringidas y zonas de alta concentración de personas.

5.1.2 Recomendaciones

- Se debe contar con sistemas de seguridad que ayuden al control e identificación de personas que hacen abusos violando cualquier tipo de regla o norma de seguridad.
- Se recomienda llevar siempre un registro digital de los accesos a las zonas en donde existen pertenencias de valor.
- Siempre es importante ofrecer la seguridad como un recurso indispensable dentro de todo establecimiento.
- Llevar a cabo la supervisión del personal que realiza trabajos de aseo al no contar con la suficiente confianza.
- Además como recomendación en las principales zonas en donde existe riesgo de actos delictivos instalar cámaras que ayuden con la video vigilancia de los mismos.

CAPITULO VI

PROPUESTA

6.1. Datos Informativos

a. Título

"CONTROL DE ACCESO PARA LA DOTACIÓN DE SEGURIDAD EN DORMITORIOS Y ÁREAS RESTRINGIDAS EN EL HOTEL DESTINY"

b. Ubicación

- **Provincia:** Tungurahua
- **Cantón:** Baños
- **Lugar:** Hotel Destiny, calle Oscar Efrén Reyes y Ambato

c. Tutor

- Ing. M.Sc. Mario García

d. Autor

- Sr. Jairo Santiana

6.2. Antecedentes de la Propuesta

El control de acceso comenzó como tal con proveedores nacionales e internacionales de equipos de seguridad que cada vez presentaron dispositivos con altas prestaciones, partiendo desde modelos básicos hasta los que llegan a tener la más alta tecnología electrónica, en diversos tipos de sistemas de control, todo esto con el fin de satisfacer las demandas en el campo de la seguridad para los distintos tipos de empresas y su necesidad de estar al par con la seguridad.

Con este antecedente el Hotel Destiny busca ofrecer la más alta calidad en atención a sus clientes y proporcionar los beneficios que hoy la tecnología en

control de accesos puede ofrecer, además de ser el único en la ciudad en contar con este tipo de equipos de seguridad para mantener un alto prestigio del mismo.

6.3. Justificación

La propuesta planteada se puede justificar desde varios puntos de vista, por una parte el Hotel en el cumplimiento de estándares de calidad de servicio y atención al cliente presentara un moderno sistema de control de acceso en sus habitaciones y áreas administrativas, por otro facilita el labor de limpieza en las habitaciones ya que el personal con una sola identificación puede llevar a cabo la labor mientras que con llaves la perdida confusión, evitar que se clonen las llaves y evitar el abultamiento facilitan la labor, en caso de pérdida no hace falta el cambio de cerraduras tan solo con volver a elaborar una nueva identificación se podrá volver a tener acceso, además de contar con el respaldo por parte de los propietarios y encargados de la construcción, y su costo beneficio, así como planos de la edificación diagramas de conexión eléctrica entre otros documentos importantes para el correcto desenvolvimiento en el planteamiento de la propuesta.

6.4. Objetivos

6.4.1 Objetivo General

- Diseñar un sistema de control de acceso para la dotación de seguridad de habitaciones y áreas restringidas en el Hotel Destiny.

6.4.2 Objetivos Específicos

- Determinar que equipos y software de control de acceso satisfacen las necesidades técnicas y económicas para beneficio del hotel.
- Diseñar un circuito cerrado de televisión que complemente el sistema de control de acceso, para la identificación visual de personas que quieran vulnerar el sistema de control.
- Analizar las distintas áreas que deben contar con vigilancia y control de acceso dentro y fuera del hotel
- Establecer un punto de control, y la ubicación de equipos y cámaras para su respectiva vigilancia.

6.5 Análisis de Factibilidad

6.5.1 Factibilidad técnica

La factibilidad técnica está presente gracias a empresas nacionales que presentan disponibilidad de equipos y técnicos capacitados en la instalación y mantenimiento de los mismos.

En un análisis de mercado se puede encontrar varios distribuidores que cuentan con catálogos de equipos de última tecnología en stock o bajo pedido, la experiencia en el campo de la seguridad por parte del investigador y el apoyo del encargado del diseño tecnológico del hotel se complementan para hacer un proyecto totalmente viable en el Hotel.

6.5.2 Factibilidad Operativa

El proyecto es operativo ya que el hotel Destiny se encuentra en fase de construcción y presenta la infraestructura para el diseño e implementación del control de acceso en sus distintas áreas.

6.5.3 Factibilidad Económica

El hotel Destiny cuenta con un presupuesto para la investigación e integración de sistemas de seguridad en donde se contempla un control de accesos, lo que significa que al realizar la inversión es justificada por el ahorro a largo plazo que conlleva implementar el uso de tecnología para el servicio que presta el hotel.

6.6 Fundamentación

6.6.1 Sistemas electrónicos de seguridad

Un sistema es un objeto compuesto de elementos que se relacionan con al menos algún otro componente; puede ser material o conceptual.

Como se observa en la fig. 6.1 todos los sistemas tienen composición, estructura y entorno, pero sólo los sistemas materiales tienen mecanismo, los sistemas

tecnológicos dirigidos a proteger los inmuebles, bienes y habitantes contra amenazas y peligros se denominan sistemas de control y seguridad.

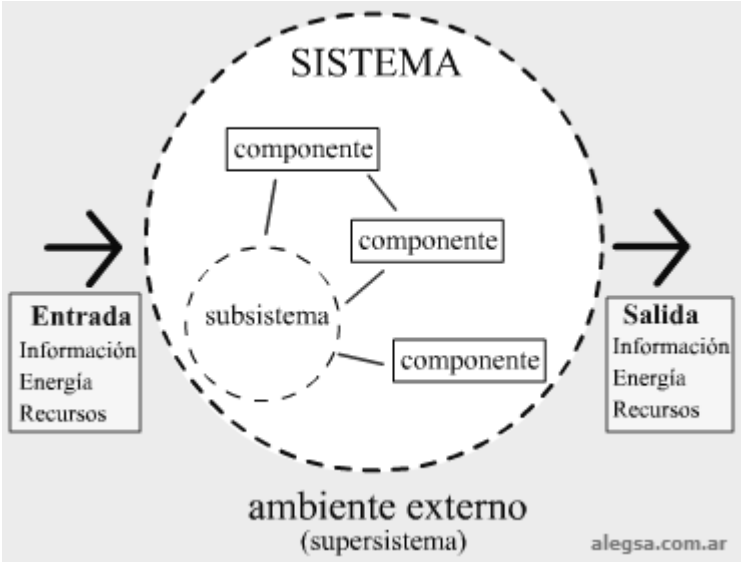


Fig. 6.1 Composición de un Sistema

Fuente: http://www.alegsa.com.ar/Dic/sistema.php

Los sistemas de seguridad y alarmas en el contexto del edificio, empresa y hogar se pueden clasificar en varias áreas:

- Alarmas de Intrusión (movimiento, presencia, presión, etc.)
- Alarmas Técnicas (incendio, humo, inundación/agua, gas, fallo de suministro eléctrico, fallo de línea telefónica, etc.)
- Alarmas Personales (SOS y asistencia)
- Sensores de movimiento computarizados
- Alarmas con monitores tecnología GSM
- Control de accesos
- Video Vigilancia (IP / ANALÓGICA)

Existe una gran variedad de alarmas y sistemas de seguridad, tanto a nivel de diseño, funcionamiento y aplicaciones como la tecnología utilizada. Se hace una breve descripción tecnológica general.

Para tomar decisiones hay que especificar todos los factores que se quieren controlar desde distintos puntos de vista y poder realizar una elección que beneficie a todo el entorno que se quiere controlar.

6.6.2 La seguridad se puede evaluar de acuerdo a varios criterios:

a. **Disponibilidad:** Asegurar que los elementos se consideran accesibles cuando sea necesario por las personas autorizadas en el software encargado de la administración de equipos y poder realizar tareas de mantenimiento y corrección de fallas según sea el caso.
b. **Integridad:** Que no exista violación de la integridad de áreas o documentos que se quiera proteger mediante la incorporación de equipos de seguridad.
c. **Confidencialidad:** Garantizar que sólo las personas autorizadas tengan acceso al lugar controlado y monitoreado mediante métodos de identificación y autentificación, además de un sistema de video vigilancia.
d. **Trazabilidad (o " prueba "):** Asegurar que los intentos de acceso y el acceso se registran en los elementos considerados como un registro de ingreso almacenado en una base de datos que solo pueda ser visto por el administrador o grupo encargado del sistema.

6.6.3 Amenazas

Las principales amenazas a las que un sistema de seguridad puede enfrentar son:

a. **Un usuario del sistema:** La inmensa mayoría de los problemas relacionados con la seguridad de un sistema de seguridad es el usuario, por lo general personal que tiene acceso y hacen abuso del mismo en casos forman parte de bandas que se dedican a este tipo de acciones.
b. **Un atacante:** Alguien se las arregla para entrar en el sistema, legítimamente o no, y entonces el acceso a datos o programas a los que se supone que no tienen acceso, por ejemplo, utilizando las vulnerabilidades conocidas y no corregidas software o mediante el robo o falsificación de una identificación.
c. **Un programa malicioso:** Un programa destinado a los daños o perjuicios a los recursos del sistema se ha instalado (por accidente o maliciosa) en el sistema, abriendo la puerta a la intrusión o la modificación de datos, los datos personales pueden ser recogidos sin el conocimiento del usuario y volver a utilizar con fines comerciales o maliciosos.

d. Una pérdida: Repercute en el manejo inadecuado del objeto o identificación de acceso, personas inescrupulosas que hacen uso de estos con fines maliciosos causando vulnerabilidad en el sistema de seguridad y datos.

El hotel Destiny cuenta con una visión de vanguardia en donde se integrara varios tipos de sistemas tecnológicos, entre estos el sistema de seguridad, plenamente en nuestro caso centrado al control de accesos como solución al problema planteado con anterioridad, y evitar este tipo de amenazas

6.6.4 Control de Accesos

Los Sistemas de control de acceso son una excelente solución de seguridad para grandes empresas con pocos o muchos empleados.

El control de acceso permite convenientemente permitir el acceso a zonas de las empresas sólo es necesaria una identificación por cada empleado de forma individual.

Fig. 6.2 Ejemplos de control de acceso.

Fuente: http://www.tecnego.com/

Como se muestra en la fig. 6.2 algunos tipos de control de acceso la mayoría de las veces el uso de una identificación con una banda magnética con la información codificada. Teclados, escáneres de huellas digitales y otro tipo de tecnología también puede ser incorporado a un sistema de control de acceso, dependiendo de las necesidades de seguridad y las consideraciones prácticas.

Un buen control de acceso puede ayudar mediante el diseño de un sistema que responde a sus necesidades de seguridad específicas de las empresas. Un sistema de control de acceso fácil y rentable proporciona a la empresa la seguridad necesaria, así como de numerosos otros beneficios.

Los Sistemas de control de acceso también puede utilizarse eficazmente en las pequeñas empresas, hoteles, e incluso complejos de apartamentos y dormitorios del colegio, en donde se necesita tener un registro de ingreso.

Esta tecnología puede ahorrar ya que evita el cambio de cerraduras por perdida y le permitirá sentirse seguro en el entorno. Cómodo y fácil de utilizar se está convirtiendo en una opción de seguridad popular cada año.

6.6.5 La forma de control de acceso en sistemas de trabajo

La mayoría de los sistemas de control de acceso básico llevan un registro de cuándo y quién entra en determinada puerta cuando se abrió. Sin el código de identificación o la tarjeta de identificación, la puerta permanece bloqueada.

Otros complejos sistemas de control de acceso pueden incluir también una característica de horario, la hora de sus empleados en el momento de su entrada y la hora de ellos cuando se vayan. En este caso, es importante elegir un sistema de control de acceso con el software que sea compatible con su software de horarios y asistencia debidamente planificados.

6.6.6 Integración

El control de acceso puede integrarse en un sistema general de seguridad. Se presenta la posibilidad de seleccionar un sistema que funcione bien con un circuito cerrado de televisión, sistemas de alarma y otros elementos de seguridad ya existentes.

Incluso para integrar equipos de control de acceso a los sistemas de seguridad de datos en el sistema global.

Como se muestra en la fig. 6.3 la integración de tarjetas de identificación para varias actividades dentro de la empresa.

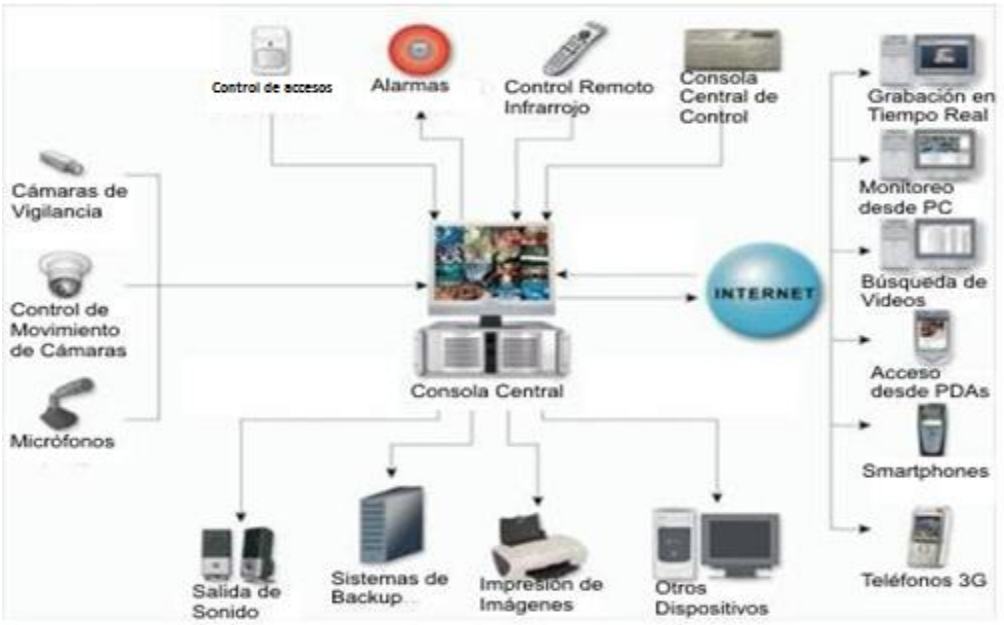


Fig. 6.3 Integración global de un sistema de control

Fuente: http://www.aresseguridad.es/p/es/sistemas-de-seguridad/control-accesos/control-de-accesos-completo.php

6.6.7 Escoger el correcto Control de Acceso

El primer paso para elegir el correcto sistema de control de accesos es examinar técnicamente los requerimientos necesarios de la empresa, además pensar en cambios futuros que se le puedan dar como el incremento de puntos de control de empleados entre otros, optar por preguntas que ayuden a descartar todas las dudas sobre el sistema que necesitamos.

- ¿Cuántas puertas o puntos de control deben contar con un sistema de control de acceso?
- ¿Cuántos empleados necesitan identificación para el acceso? (La cantidad de empleados y el volumen de negocios están presentes)
- ¿Quiere controlar las salidas, así como las entradas?
- ¿Qué tipo de identificación se necesita, RFID, teclados, biométrico, otros?
- ¿Se necesita un control visual en las entradas, realizar una identificación física de la persona que ingresa?

Otros aspectos como tomar en consideración:

- El tipo de empresa en el que se implementara el sistema de control,
- Diferenciar que una pequeña empresa no necesita de un escáner de huellas biométrico ya que el personal no es en gran número son fáciles de identificar,
- Una gran empresa con un alto sistema de seguridad puede requerir un control de acceso en distintos niveles de seguridad por zonas horarios múltiple, con muchas características de seguridad avanzada integrada en uno solo y un software de control de gran escala.

Estas preguntas le ayudarán a determinar el alcance necesario para su sistema de control de acceso. Si sólo se desea controlar una única puerta, es sencillo hacerlo con un teclado en la entrada puede ser más que suficiente.

En empresas de mayor tamaño hay que tomar el tiempo necesario para buscar varias propuestas de sistemas de control de acceso. Ver no sólo los costos, sino también la propuesta global, y la manera en la que responde a los distintos tipos de necesidades.

El control de acceso para el sistema de seguridad de la empresa será más fácil de utilizar, mantener y vigilar. Se integraran características de seguridad actuales, con lo que ahorra dinero.

6.6.8 Características

Una de las más importantes características del sistema de control de acceso a tener en cuenta es la facilidad de uso de su sistema.

Los empleados pueden estar utilizando el sistema de control de acceso varias veces al día, por lo que debe ser fácil de usar, y no requieren una formación especial en el uso y adaptación al mismo.

La identificaron por PIN son el medio más común para autenticar a los empleados un sistema de control de acceso.

En la fig. 6.4 se puede ver un sistema de control instalado en el acceso a zonas restringidas de una cooperativa de ahorro y crédito de la cuidad de Ambato y un ejemplo de varios tipos de control de accesos.

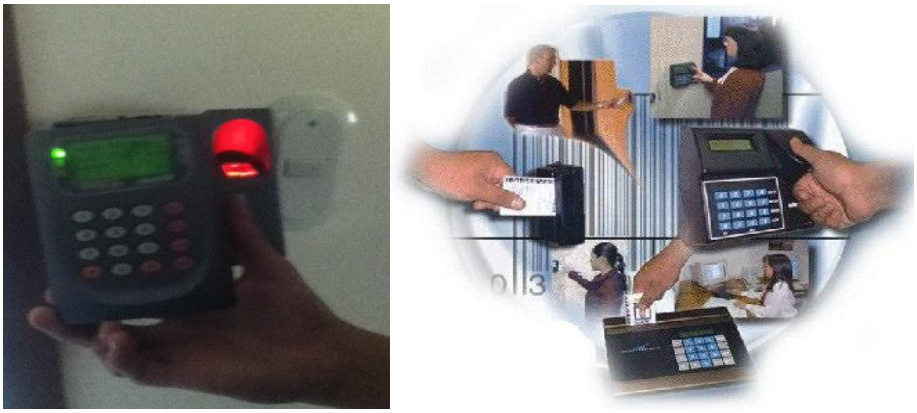


Fig. 6.4 Control de accesos

Elaborado por el investigador

La manera más frecuente de utilizar es un dispositivo similar a una tarjeta de crédito para cajeros automáticos, otra forma que utilizan más las empresas son lectores de tarjetas de proximidad, que permite a los empleados simplemente acercar la tarjeta al lector. Estos son particularmente útiles si el sistema de control de acceso que se instaló en la puerta de un parqueadero o similar.

Las características de los sistemas de control de acceso se pueden controlar fácilmente a través de interfaces online. Muy útil al momento de realizar una supervisión o mantenimiento, las copias de seguridad son otro elemento importante, ya que sin ello la auditoria de las cerraduras no sería posible, eliminando así la seguridad de los edificios.

6.6.9 El control de acceso como una medida de seguridad

El control de acceso es una medida útil de seguridad. Con el uso de cerraduras electrónicas se evita que las llaves se pierdan o sean robadas, el sistema de control de acceso en caso de robo o pérdida permite desactivar las identificaciones asignadas anteriormente, además de vigilar las actividades de los empleados y violaciones a los horarios que se puedan dar.

Un sistema de control de acceso se puede integrar en el conjunto del sistema de seguridad existente, en los últimos años la tendencia a integrar control de acceso al sistema general de seguridad ha aumentado, todo por crear un entorno seguro para sus empleados como una parte del sistema en general.

El control de acceso puede ser incluso necesario para los contratos de los gobiernos y de otros entornos de trabajo seguros.

Si su empresa está en esta situación, y ha descubierto qué características de seguridad pueden ser necesarias para que su sistema de control de acceso se adapte a las necesidades de sus clientes de manera más eficaz y adecuada.

Un control de acceso bien instalado y con un correcto uso y mantenimiento se encargará de la seguridad, no sólo de su propiedad, sino también de sus huéspedes, clientes, e incluso sus empleados, además permitirá limitar el acceso de los empleados a las zonas de alta seguridad de un edificios, y puede incluso integrar múltiples zonas en el sistema de control de acceso.

Esta puede ser una característica especialmente útil para las grandes empresas con empleados que trabajan en varias ubicaciones.

Una sola tarjeta de identificación ID puede permitir a un usuario el acceso a las zonas que necesiten consentir el acceso, para hacer su trabajo de manera eficaz.

6.6.10 Utilización en el lugar de trabajo

Como se indica en la fig. 6.5 El control de acceso mediante tecnología RFID, instalado en una puerta con acceso a una oficina en donde se pueden asignar varios tipos de identificación como ejemplo, ID de administrador, ID de usuario, ID de aseo, en caso de pérdida la ID es desautorizada en el software de control, y en caso se intente utilizar ya no será consentido el ingreso.

La introducción de calidad en el control de acceso parte desde la ID del usuario que se lee a través de teclados, lectores biométricos, lectores de tarjetas de proximidad entre otros que están en la entrada y salida de lugares de trabajo con

restricciones de acceso, estas se pueden instalar según los requerimientos que se necesiten.

Además de guardar un registro, en donde se vigila estrictamente cada acción de los usuarios si alguien entro en un horario no planificado, será fácil la detección de anormalidades que se puedan dar en cada área de trabajo, así como la velocidad de los tiempos de entrada y salida en la institución de trabajo en donde la puntualidad como regla de seguridad debe prevalecer.

Fig. 6.5 Lector de tarjetas de proximidad

Fuente: http://www.tarjetashid-mifare-rfid.com/Lector_Proximidad_RFID_LP100.html

Los sistemas de seguridad de Control de acceso también puede hacer más simple proceso de rotación de empleados, como la insignia de identificación de acceso puede ser desactivado. El proceso de obtener las claves de vuelta, ni preocuparse de las entradas no autorizadas a la empresa.

Un sistema de control de acceso puede ser una adición útil a la seguridad, tanto para las pequeñas y grandes empresas, y será apreciada por los empleadores y los empleados.

6.6.11 Funciones de seguridad

Una serie de valiosas características de seguridad están disponibles con muchos sistemas de seguridad de control de acceso.

La más obvia característica de seguridad de un sistema de control de acceso es la capacidad de limitar el acceso específicamente a una determinada puerta, y de registrar las entradas en el edificio, o una zona del edificio, se puede integrar en general con funcionalidad en una forma perfecta de la insignia ID empresa.

Un sistema de control de acceso también puede permitir que el administrador convenientemente habilite o inhabilite el acceso en áreas específicas de la construcción, y fácilmente limitar el acceso a mayores zonas de seguridad.

Muchos de los controles de acceso a sistema de seguridad de las compañías existentes se integrarán a las funciones de seguridad en su sistema de control de acceso. Los sistemas de control de acceso, o bien la incorporación de teclados o sensores junto a tarjetas o biometría puede ser una opción de alta seguridad.

La más alta tecnología en control de accesos para la seguridad es la biometría que permite el acceso a través de huella dactilar escáneres, lectores de palma u otras características físicas individuales.

Las nuevas características en sistemas de control de acceso pronto podría permitir la integración de los tradicionales de control de acceso a los sistemas de seguridad corporativa con la seguridad informática. Esto reduciría los posibles problemas de seguridad, y agilizar el proceso de permitir el acceso tanto a las propiedades físicas y virtuales.

6.6.12 Costos

Los costos pueden varían ampliamente entre los distintos sistemas de control de acceso, todo va en función de:

- Número de puertas o zonas con control de ingreso
- Si permite la libre salida o cuenta con control de salidas
- Tipo de características de seguridad
- Sistema independiente o centralizado
- Integración de alarmas y sensores de presencia

Un teclado de entrada es bastante asequible, sin embargo, un sistema biométrico de huella dactilar puede ser muy costoso en las inversiones de las empresas.

Al considerar los gastos asociados a un sistema de control de acceso con fines de seguridad, también tiene que calcular los gastos ligados a la computadora

controladora, cerraduras necesarias para las puertas, así como los gastos de cada equipo y tarjeta a futuro que se pueda utilizar.

Mientras más características se agreguen al control de acceso, más caro será. Algunas características que pueden ser una inversión rentable para su negocio incluyen la posibilidad de fijar el calendario a las cerraduras en las puertas, para permitir el acceso del público en algunas horas y sólo el acceso de los empleados a otros, batería de respaldo en caso de pérdida energética.

Básicamente el control de acceso debe pasar por un análisis técnico económico, ver lo que actualmente se requiere controlar las distintas zonas, lugares, áreas y en base a un crecimiento de la empresa plantear posibles soluciones a un futuro cercano, como la implementación de más puntos de control, la integración de nuevos métodos de identificación entre otros.

Como ejemplo en una empresa que dispone de un bajo número de empleados se puede optar por un sistema básico de control como, teclados numéricos o tarjetas de proximidad, sin embargo si el número de empleados incrementa con el tiempo se deben optar por sistemas de más seguridad en la identificación del usuario como ejemplo la huella dactilar, palma de la mano.

6.6.13 Componentes y funciones de un Control de Accesos

Un **sistema de control de acceso** es un conjunto de dispositivos interactuando entre sí que permite en su gran mayoría:

- Restringir la apertura de puertas o accesos mediante algún medio mecánico.
- Identificar al usuario de acuerdo con parámetros establecidos para determinar si el acceso es permitido o denegado.
- Registrar y auditar los eventos de acceso por usuario y por puerta.
- Programar la autorización o desautorización del acceso relacionando a cada usuario.
- Permitir funciones adicionales de seguridad y funcionalidad.

6.6.14 Restringir la apertura de puertas o accesos mediante algún medio mecánico.

Este medio mecánico debe ofrecer la seguridad que será efectivo al impedir la apertura de la puerta y resistir a los posibles intentos de violación.

Cada uno de estos medios tiene sus ventajas, desventajas y características particulares.

Estos pueden ser:

6.6.14.1 Electroimanes

El electroimán se ilustra en la fig. 6.6 está formado por una bobina y un núcleo de hierro colocado en el interior del mismo, el núcleo de hierro se imanta por influencia de campo magnético creado por la bobina durante el paso de la corriente por sus espiras, resultando un campo más intenso que el producido por la bobina, estos presentas sus ventajas y desventajas.

Fig. 6.6 Electroimán

Fuente: http://www.alsemexicana.com/control-de-acceso/control-de-acceso.html

- Permiten flexibilidad de programación y proporcionan una poderosa sujeción de las puertas medida en presión que se control según voltaje.
- En sus diversos modelos la mayoría son costosos.
- Requieren instalaciones difíciles y modificaciones a las puertas y al inmueble.
- Dependen del suministro eléctrico para mantener la puerta cerrada. Esto los hace necesitar un respaldo para el suministro eléctrico por una batería o unidad UPS.
- El cable que le suministra la energía eléctrica al electroimán es su punto más vulnerable, ya que al cortarlo éste se abrirá y dejará de cumplir con su función, además si se ejerce una fuerte presión este se abrirá.

6.6.14.2 Las contrachapas eléctricas

Como se observa en la fig. 6.7 la contrachapa se usa en puertas de aluminio, madera, fdm entre otros tipos de material. Al igual que la chapa eléctrica, el control de acceso manda un impulso eléctrico de 12 v. Mientras este impulso este presente, la contrachapa permite abrir libremente la puerta. Cuando desaparece este impulso, la contrachapa bloquea la puerta. Es común poner un cierra puertas automático a la puerta para que este siempre este bloqueada y la contrachapa funcione adecuadamente. Igualmente presentan ventajas y desventajas:

Fig. 6.7 Contrachapas eléctrica

Fuente:http://www.alsemexicana.com/control-de-acceso/control-de-acceso.html

- Son soluciones sencillas y económicas.
- No ofrecen una sujeción confiable para la puerta, es decir, son relativamente fáciles de abrir o forzar por intrusos.
- Así como los electroimanes, dependen del suministro eléctrico para operar.
- La diferencia con respecto a los electroimanes es que si su suministro eléctrico llegara a interrumpirse la cerradura eléctrica permanecerá cerrada.
- Son fácilmente adaptables a cualquier tipo de entorno.
- Tiene un botón de control de apertura desde el interior.

6.6.14.3 Los cilindros electrónicos para cerraduras

Los cilindros electrónicos como se observa en la fig. 6.8 pueden ser acoplados a distintos sistemas de chapas, en donde se necesite una mayor autonomía de funcionamiento ya que existen varios tipos de cilindros como ejemplo uno que no necesita tener alimentación incorporada en este caso la llave envía un impulso electrónico que activa el sistema de la puerta.

Son soluciones económicas y confiables.

Fig. 6.8 Cilindro electrónico

Fuente: http://www.alsemexicana.com/control-de-acceso/control-de-acceso.html

- Funcionan con sus propias baterías, por lo que no dependen de un suministro eléctrico externo.
- Su fuerza de sujeción depende de la cerradura en la que se instalen, de manera que no está limitada de antemano.
- En algunos casos el cilindro no tiene alimentación. La llave proporciona la energía para abrir.
- Posibilidad de combinar en la misma instalación cilindros electrónicos, cerraduras electrónicas y cilindros mecánicos
- Todos los elementos de control se encuentran protegidos en el interior del cilindro: unidad de control, lector y mecanismo de condena.

6.6.15 Identificar al usuario de acuerdo con parámetros establecidos para determinar si el acceso es permitido o denegado.

Los medios de identificación de usuarios son varios en resumen se pueden presentar varias opciones como se indicaba anteriormente, es preferible realizar un estudio antes de la implementación de los mismos en la fig. 6.9 se muestran algunos sistemas de control.

Los medios de identificación de usuarios son:

- Teclados para digitación de códigos alfanuméricos
    - Montados
    - Personales y portátiles
- Tarjetas de proximidad
- Botones de control remoto
- Dispositivos biométricos
    - Lector de huella digital
    - Lector de iris
    - Identificación de rasgos faciales
- Tarjetas magnéticas

Fig. 6.9 Sistemas de control de acceso

Fuente: http://www.alsemexicana.com/control-de-acceso/control-de-acceso.html

6.6.16 Registrar y auditar los eventos de acceso por usuario y por puerta

De esta manera se puede saber cuál usuario y en qué momento está entrando o saliendo a través de los accesos controlados. También debe indicar qué usuario intentó tener acceso fuera del horario o días permitidos.

Esto es importante para:

- Conocer los hábitos de los usuarios del inmueble y tomar medidas disuasivas oportunamente.
- Generar registros que puedan deslindar responsabilidades en caso de pérdida o robo de objetos.
- Respaldar otros sistemas de seguridad como CCTV.
- Proteger la información del sistema de control de asistencias.

6.6.17 Programar la autorización o desautorización del acceso relacionando a cada usuario con horarios, fechas, u otras condiciones de acceso

Programar el comportamiento que las puertas o accesos, que deben tener para cada usuario en diferentes condiciones:

- Horarios establecidos de ingreso, como ejemplo para el aseo o mantenimiento de una zona.
- El acceso a cierta puerta puede estar condicionado a que otra puerta esté cerrada como ejemplo el ingreso a uno bóveda debe estar condicionado a que la puerta de administración este cerrada.
- Para tener acceso a cierta área dos o más usuarios deben identificarse ante el dispositivo, ya sea cada quién su número en un teclado, o dando a leer su huella digital.
- Acceso controlado en tiempo real por un sistema de monitoreo.
- Tener el control mediante acceso remoto al sistema de accesos en caso exista la denuncia de perdida de identificación y poder realizar el bloqueo.

6.6.18 Permitir funciones adicionales de seguridad y funcionalidad

Ejemplos de esto puede ser el programar una apertura con retardo (delay). Es decir, que aún de que la identificación sea positiva, la puerta o dispositivo tardará cierto tiempo, programado con anterioridad, en permitir el acceso. Además de conectar un sistema de alarma en caso el acceso sea manipulado o forzado para la apertura, en casos extremos el bloqueo permanente del acceso y accesos aledaños.

6.6.19 Componentes detallados de un control de acceso

Para poder tomar una elección más detallada de los componentes que pueden formar un control de acceso, se realiza un resumen de componentes.

Si estás pensando en implantar un sistema de control de acceso efectivo y eficaz en tus instalaciones, y sin gastarte un dineral, necesitarás estos elementos básicos:

6.6.19.1 Infraestructura informática

En la mayoría de sistemas de control de acceso se requiere tener un ordenador como se indica en la fig. 6.10 y un software de control de accesos que controla los permisos de acceso. En muchos casos existe hardware adaptado de las mismas compañías que permite habilitar las identificaciones y obtener reportes del uso de las mismas.

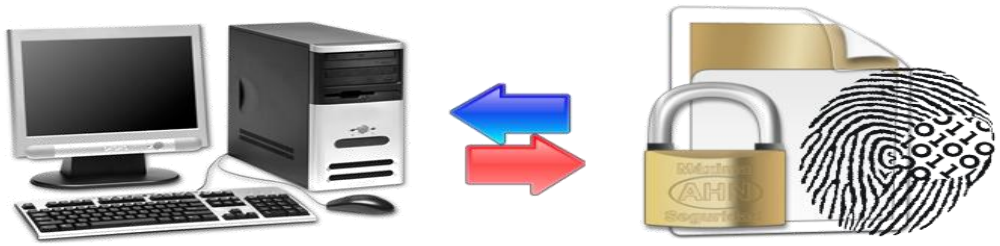


Fig. 6.10 Pc para el control de acceso

Elaborado por el investigador

Además se puede aprovechar para la gestión de datos personales (dirección, cumpleaños etc.) o de horarios y zonas de preferencia (por ejemplo en un centro deportivo) que puede resultar útil en un programa de fidelización de clientes.

6.6.19.2 Sistema de identificación

Lo infaltable en los sistemas de control de acceso y lo que los hacen llamar así es la manera de conceder el acceso, siempre se requerirá de una identificación que certifique que la persona que ingrese este en el sistema, hay varias maneras pero solo se nombraran las de relevancia para el proyecto como por ejemplo un lector que transmite los datos identificativos al software, que entonces permite o deniega el acceso a la zona controlada.

La solución más económica y versátil de porta datos son tarjetas plásticas, que por un lado ofrecen la lectura electrónica con chip, banda magnética o código de barras, y por otro lado permiten la personalización mediante una fotografía o el nombre del titular. Además son fáciles de llevar en la cartera como brazalete en sus diversas prestaciones.

6.6.19.3 Barreras de acceso

Otra parte importante ocupan las barreras como torniquetes trípode, pasillos motorizados, portillos o barandillas, las cuales impiden el paso físicamente.

Fig. 6.11 Barrera de control mediante cerraduras electromagnéticas

Fuente: http://www.alsemexicana.com/control-de-acceso/control-de-acceso.html

Los distintos sistemas de seguridad tienen un rango muy amplio en sus funcionalidades, desde una sola función limitada (por ejemplo un alarma local de apertura de una puerta) a la realización de una sola acción hasta sistemas amplios que controlan toda la seguridad dentro de una vivienda o edificio, además de permitir distintos tipos de configuraciones de seguridad.

6.6.19.4 Central de alarmas

La Central de alarmas es el dispositivo que controla el sistema según su programación y la información que recibe se procesa en hardware especializado o una computadora con software de seguridad.

Como se puede ver en la fig. 6.12 también es el componente responsable de la comunicación del sistema de seguridad con el exterior, como avisos a una C.R.A (Central Receptora de Alarmas), o el inquilino o propietario del edificio.

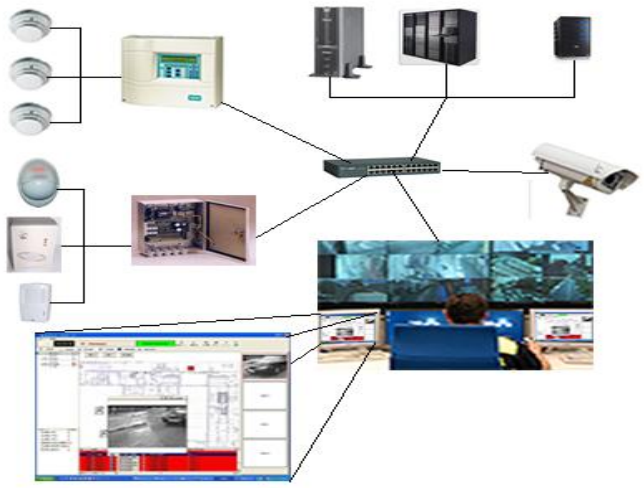


Fig. 6.12 Integración completa de un sistema de seguridad

Fuente: http://www.ralco-networks.com/not.php?noticia=47

La centralita puede además incluir la conexión del sistema de seguridad con otros sistemas del edificio y hogar digital, tanto recibiendo, como emitiendo información.

6.6.19.5 Detector de Movimientos

El detector es un sensor que monitoriza el entorno y detecta cambios o anomalías:

- Movimiento
- Presencia
- Presión
- Apertura de puertas y ventanas
- Presencia de agua, gas, humo, fuego, etc.

Todo se transmite al sistema mediante una conexión centralizada como se observa en la fig. 6.12 que se encarga de informar los acontecimientos en tiempo real y de ser necesario configurar acciones que ayuden a la inmediata intervención de las personas encargadas.

6.6.19.6 Medio de Transmisión

El medio de transmisión es la infraestructura que transporta la información entre los distintos dispositivos del sistema de seguridad puede ser por un cableado propio, por la redes de otros sistemas (red eléctrica, red telefónica, red de datos) o de forma inalámbrica según permitan los distintos tipos de equipos.

6.6.19.7 Interfaces de presentación

Las interfaces se refieren a los dispositivos y sus distintos formatos en los que se muestra la información del sistema para los usuarios (o para otros sistemas) y a través de los cuales se puede interactuar con el sistema (botones, teclados, voz, web, móvil, etc.).

6.6.19.8 Sirenas

Las sirenas son componentes que pueden generar un sonido alto combinado con un aviso luminoso. Tienen varios objetivos, tanto avisar a los inquilinos y a la gente alrededor, como asustar y molestar a posibles intrusos en casos de robo e intrusión. Pueden estar situados tanto en el interior como en el exterior del inmueble protegido, pueden contar con un subministro de energía independiente de la red eléctrica ya que al cortar la alimentación esta no funcionaria.

6.6.19.9 Micrófonos y Altavoces

Los micrófonos y altavoces son componentes que permiten grabar los sonidos que se captan dentro y fuera del inmueble, avisar de posibles intrusos, y mantener una comunicación bidireccional con personas dentro del inmueble.

6.6.20 Integración y funcionalidades adicionales

Muchos sistemas de seguridad permiten la conexión y comunicación con otros sistemas dentro de un edificio o el hogar, puede por ejemplo emitir una señal si detecta movimiento en el exterior para que el sistema de domótica recoja esa señal y encienda la luz exterior y baje las persianas. Pero también puede integrar las funcionalidades de domótica, telecomunicaciones directamente en el mismo sistema, que pueden variar desde funcionalidades muy sencillas, como encender una luz, hasta la gestión total de la instalación domótica edificio u hogar.

6.6.20.1 Control Propio

Generalmente los sistemas de seguridad pueden ser instalados, mantenidos y gestionados o bien por el propietario directamente, o bien por empresas profesionales y homologadas de seguridad, que den respaldo de sus productos.

6.6.21 Control de acceso mediante sistemas cerrados de televisión

En un mercado en donde el auge de la implementación de sistemas de seguridad existe un sin número de soluciones en cuanto a cámaras y sus accesorios, por lo que es necesario realizar un estudio técnico de los requerimientos que se necesitan antes de la implementación ya que los costos de algunos equipos que ofrecen muchas características que algunas veces son desaprovechadas en su totalidad.

Comenzaremos diciendo que ambas tecnologías, tanto la análoga como la ip utilizan un sensor análogo de imagen que puede ser de dos tipos CCD o CMOS. Actualmente la gran mayoría las cámaras análogas del mercado utilizan exclusivamente un sensor CCD, mientras que las cámaras IP pueden utilizar cualquier de los dos.

La señal análoga proveniente del sensor es entonces convertida a una señal digital desde el convertidor Analogo-Digital de la cámara y luego es enviada a un circuito DSP.

Para una cámara IP la imagen es posteriormente comprimida internamente y transmitida vía IP y será entonces almacenada en un NVR (Network Video

Recorder) que no es otra cosa que un software montado sobre algún sistema operativo recibiendo la señal IP.

Para una cámara Análoga la señal vuelve a ser convertida a Análoga por el convertidor Análogo-Digital y transmitido entonces al DVR (Digital Video Recorder) donde será comprimida y almacenada.

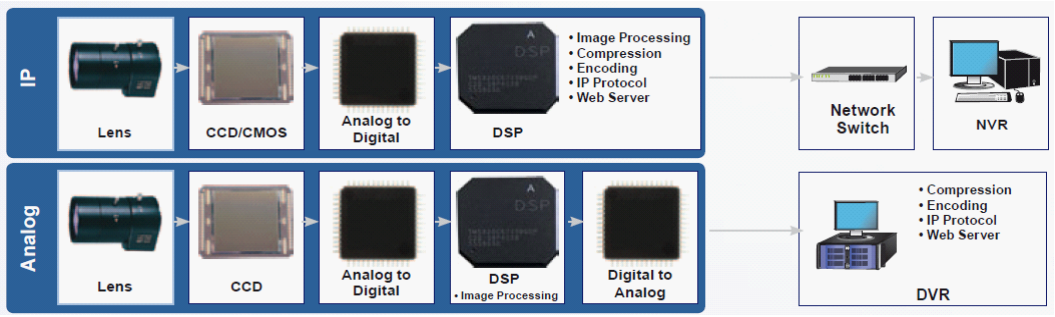


Fig. 6.13 Conversión de imagen

Fuente: http://www.tecnofenix.com.ar/site/index.php?option=com_jefaq&view=faq&Itemid=90

6.6.22 Cámaras Ip

Es necesario conocer este tipo de cámara, su característica principal es que se puede implementar en una red de datos ya existente, en la actualidad para mayor facilidad de instalación y acoplamiento se utiliza cámaras wireless que trabajan en frecuencias desde los 2.4 Ghz hasta 5.8 Ghz en muchas prestaciones y con grandes alcances dentro de zonas en donde es difícil realizar un cableado de red.

Una Cámara IP se podría definir como una cámara que digitaliza y procesa imágenes análogas, las comprime internamente y luego transmite la información del video a través de una conexión TCP/IP.

Las cámaras IP nos pueden ofrecer una calidad de imagen Mega Pixel, cosa que no pueden hacer las análogas, en cambio las cámaras IP tienen problemas en condiciones con baja luminosidad, una gran ventaja es que se puede enviar la alimentación eléctrica mediante el cable de red con tecnología Poe.

Como se observa en la fig. 6.14 una cámara de red, también llamada cámara IP, puede describirse como una cámara y un ordenador combinados para formar una única unidad que incluyen un objetivo, un sensor de imagen, uno o más procesadores y memoria.

Figura 6.14 Cámaras de red alámbrica como inalámbrica

Elaborado por el investigador

Para la visualización se puede usar una computadora. Además puede utilizarse el software embebido en la cámara o bien si se requiere armar un sistema de grabación con múltiples cámaras se utilizan software más complejos. Algunos limitados y gratuitos y otros de uso profesional. Dependiendo de la utilidad buscada del sistema de cámaras.

6.6.23 Cámaras Analógicas

Una Cámara Análoga se podría definir como un sensor CCD que digitaliza la imagen y la procesa, pero antes de poder transmitir la imagen necesita volver a procesarla para que esta pueda ser recibida por un DVR, un Monitor, una Grabadora, o lo que sea. Las cámaras Análogas no integran Web Server, ni compresores, no requiere de ningún mantenimiento a parte del físico (limpieza de polvo el contorno y el lente de visión.

Fig. 6.15 Cámaras analógicas

Elaborado por el investigador

Las cámaras Análogas operan perfectamente en diferentes condiciones de luz además de contar con sensores que activan el sistema nocturno de la cámara. Una cámara análoga no comprime la imagen, si no que esta función la hace el DVR,

con lo cual dispone de un mejor Hardware para hacer esta función incrementando tanto la calidad del video como la cantidad de frames por segundo a procesar.

Las cámaras análogas Transmiten el Video tal cual sin compresión con lo cual las imágenes obtenidas son iguales a las captadas por la cámara sin pérdida de calidad debida a la compresión.

Las cámaras Análogas son significativamente mucho más económicas. No requieren de ningún otro periférico adicional para transmitir video.

El cable normalmente utilizado es cable Coaxial (aunque se puede utilizar también UTP con Transceptores). Usando Transceptores la distancia máxima del cableado sobre un UTP cat. 5e es de cerca de 1 milla.

6.6.24 Lentes

Estos son los ojos de la cámara y depende de la medida que se use se obtendrá un ángulo y una distancia de observación diferente. De acuerdo al CCD que tenga la cámara es el tipo de lente que debe utilizarse, por ej., para una cámara de un 1/3" se debe usar un lente también de 1/3", sino obtendremos una imagen con aro alrededor.

Comparando una lente con nuestros ojos, con una cámara de un 1/3" montada sobre los hombros y una lente de 8mm. Se obtiene la misma imagen nuestros ojos. En la siguiente tabla se muestra el área que cubre un lente de 1/3" a 10 metros de distancia. Se toma los parámetros de

LENTE HORIZONTAL VERTICAL

- 2,8 17,1 mts 12,9 mts
- 4 12 mts 9 mts
- 6 8 mts 6 mts
- 8 6 mts 4,5 mts
- 12 4 mts 3 mts
- 16 3 mts 2,3 mts

También existen lentes que tienen varias medidas, estos se llaman vari focales, permiten tener en un mismo lente diferentes medidas y ángulos con solo mover un aro en forma manual, el más común es 3,5-8 mm.

Otro tipo de lente es el de zoom motorizado que va desde el gran angular o normal hasta el teleobjetivo con un motor que mueve el lente y se controla a distancia, ahora como saber cuándo usar este tipo de lentes, bien si tenemos que controlar un lugar donde tenemos que observar lugares a distancias cercanas y lejanas, es en caso donde es recomendable su uso.

Las medidas más comunes en estos lentes son 4-48 mm o 8-80 mm

6.6.25 Cable

Hay distintas formas para que la señal que envía la cámara llegue al monitor

El cable que se utiliza para la instalación de una cámara o un monitor de C.C.T.V. es un coaxial, que está compuesto por un vivo en el centro aislado con poliuretano y una malla que lo envuelve, todo recubierto por una vaina de PVC. De acuerdo los lugares por donde deba pasar el cable y la distancia que haya entre cámara y monitor es el tipo que se debe usar, distancias cortas hasta 300 mts es el RG-59 y en distancias más largas hasta 600 mts Es el RG-11, en ambos casos se detallaran sus características más adelante. Siempre y en cualquiera de las situaciones es recomendable que el cable sea el denominado pesado porque al tienen mayor cantidad de malla tiene una mayor aislación a posibles interferencias.

- **RG-59:** Se utiliza donde la longitud del cable no supera los 300 mts Impedancia del cable: 75 ohms Conductor central: Resistencia menor a 15 ohms para 300 mts. Cumple normas para movimiento o flexión Cobre sólido (NO baño de cobre) Malla de cobre para conductor externo.
- **RG-11** Se utiliza donde la longitud del cable no supera los 600 mts. Impedancia del cable: 75 ohms Conductor central: Resistencia menor a 6 ohms para 300 mts. Cumple normas para movimiento o flexión Cobre sólido (NO baño de cobre)Malla de cobre para conductor externo.

6.6.26 Directrices para seleccionar una cámara

Dada la variedad de cámaras analógicas como de red disponible, resulta útil conocer de algunas directrices para seleccionar el tipo que mejor se adapte a sus necesidades técnicas como económicas.

6.6.27 Definir el objetivo de video vigilancia.

Determinará el campo de visión, el ángulo de visión de cobertura de la cámara, la ubicación de la cámara y el tipo de cámara u objetivo requerido. Las imágenes con un nivel de detalle más elevado ósea mientras más resolución resultan muy útiles para la identificación de personas u objetos.

6.6.28 Zona de cobertura.

Determinará el tipo y el número de cámaras que se utilizarán dentro de una zona sin dejar puntos ciegos en donde no exista cobertura. Para una ubicación concreta, se debe establecer el número de zonas de interés, el grado de cobertura de dichos espacios y tomar en consideración si éstos están situados relativamente cerca unos de los otros o si existe una separación notable entre ellos, es decisión técnica como económica porque al cubrir todos los espacios se necesitara un número elevado de dispositivos incrementando el costo.

6.6.29 Criterios importantes

Al realizar una instalación de elementos de video vigilancia hay que tomar en cuenta algunos elementos importantes que ayudan a la vida útil de los equipos:

- **Sensibilidad y condiciones lumínicas:** En entornos exteriores, debe considerarse la utilización de cámaras diurnas y nocturnas. Hay que tener en cuenta la sensibilidad lumínica que se requiere y si es necesario el uso de iluminación adicional o luz especializada, como lámparas IR con sensores que los activen al detectar obscuridad.
- **Carcasa:** Si la cámara va a situarse en el exterior o en entornos que requieran protección frente al polvo, la humedad o los actos vandálicos, es necesario utilizar carcasas lo suficientemente resistentes a la lluvia y cambios climáticos.

- **Vigilancia visible u oculta.** Es necesario conocer qué tipo de cámara se necesita para los distintos tipos de áreas, para seleccionar carcasas y monturas que ofrezcan una instalación visible u oculta dentro de distintos tipos de adaptaciones que se les puede dar.
- **Calidad de imagen.** Es uno de los aspectos más importantes de cualquier cámara, en caso de que la prioridad sea la captura de objetos en movimiento, es importante que la cámara de red incorpore tecnología de barrido progresivo y además tenga una resolución óptima para identificar rostros de personas.
- **Resolución** Para las aplicaciones que exijan imágenes con un alto nivel de detalle, las cámaras con resolución megapíxel pueden ser la mejor opción.
- **Audio.** En caso de que sea necesario disponer de audio, debe evaluarse si se requiere audio mono direccional o bidireccional, las cámaras actuales en especial de tecnología ip incorporan audio bidireccional que puede ser configurado para trabajar incluso remotamente con el uso de internet.

6.6.30 Accesibilidad remota.

El principal beneficio de la conexión de las cámaras a la redes como se indica en la fig. 6.16 que a partir de ese momento el usuario puede visualizar imágenes de vigilancia desde cualquier ordenador conectado a la red, sin necesidad de ningún hardware o software adicional.

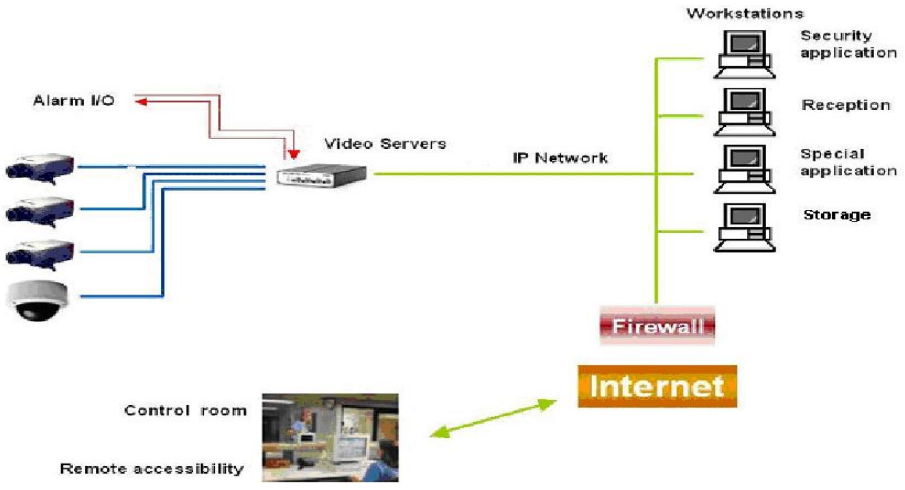


Fig. 6.16 Sistema de cámaras con acceso remoto

Fuente: http://www.yftelperu.com/comunicacion.html

En la actualidad la mayoría de equipos de video vigilancia dispone de un puerto para Internet tanto DVR como NVR, puede conectarse de forma segura desde cualquier parte del mundo para ver el edificio seleccionado o, incluso, una cámara de su circuito de seguridad. Con el uso de Redes Privadas Virtuales o intranets corporativas, se pueden gestionar accesos protegidos por contraseña a imágenes del sistema de vigilancia. Tan seguro como el pago por Internet, las imágenes y la información del usuario quedan seguras y sólo puede acceder a ellas el personal autorizado, de igual manera para administrar el sistema.

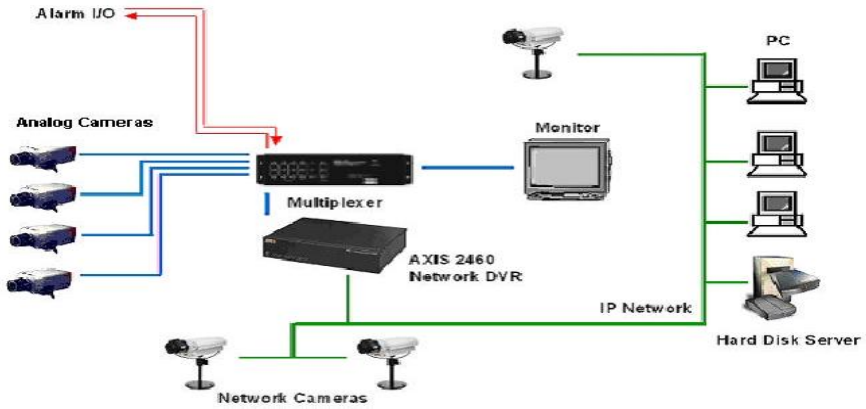


Fig. 6.17 Integración de cámaras ip con cámaras analógicas

Fuente: http://securitysystemsacademy.com/types-of-security-camera-systems-comparison-between-analogue-and-ip-security-cameras/

Es importante contar con una grabadora de video es un componente que graba imágenes y sonidos captados por las cámaras y micrófonos para poder ser revisados posteriormente, los componentes de un sistema de seguridad no tienen que estar físicamente separados como se indica en la fig. 6.17, sino que varias funcionalidades pueden estar combinadas, puede estar compuesto por una centralita, un detector de movimiento, una sirena y un teclado de interface.

Los sistemas de Seguridad actúan según:

- La programación horaria,
- La información recogida por los detectores del sistema,
- La información proporcionada por otros sistemas interconectados,
- La interacción directa por parte de los distintos usuarios (usuario final, gestor de sistema, CRA, etc.).

6.7 Metodología

El proyecto tendrá en consideración las siguientes fases en el diseño de Control de Acceso para el Hotel Destiny.

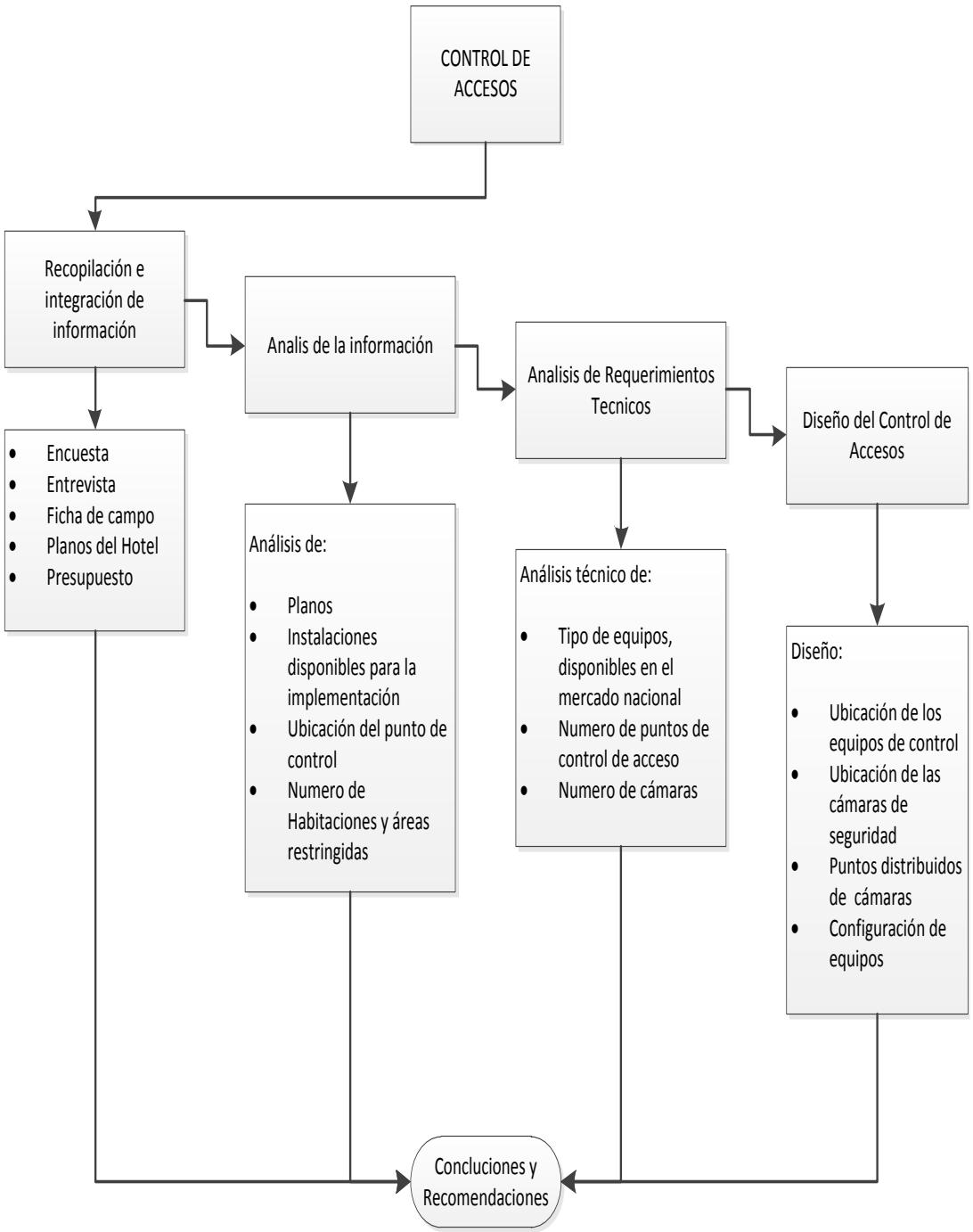


Fig. 6.18 Fases del proyecto de control de accesos

Elaborado por el investigador

6.8 Modelo Operativo

6.8.1 Recopilación de la información

6.8.1.1 Información del Hotel

- **Mapa de ubicación de la zona beneficiada**

Fig. 6.19 Mapa de ubicación del hotel en país

Elaborado por el investigador

- **Ubicación del Hotel Destiny en Baños**

Fig. 6.20 ubicación del hotel Destiny en el canto de Baños

Elaborado por el investigador

- **Fachadas del Hotel Destiny**

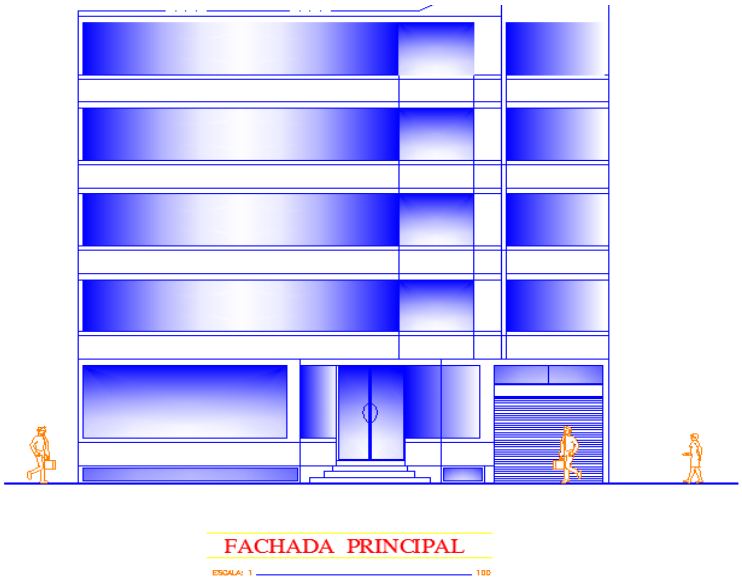


Fig. 6.21 Fachada frontal Hotel Destiny

Elaborado por el investigador

6.8.1.2 Presentación de planos y zonas del Hotel

Fig. 6.22 Foto actualizada del progreso de la construcción

Elaborado por el investigador

Cuando se empezó con la obra de construcción no se tenían establecidos todas las áreas y zonas del establecimiento, ahora se encuentra en el 90% de la construcción y se estableció los puntos precisos que serían en cada zona junto con una de las personas propietarias del hotel que se dará a conocer a continuación.

Para el estudio y planificación se presentan los planos que se utilizaron para la construcción del Hotel, donde se fijaran las zonas, descripción, riesgos y requerimientos de cada una para poner en marcha la propuesta del proyecto.

A continuación de esta presentación se realizara la contabilización del número total de dispositivos en las entradas como en el interior del hotel de control de acceso y de video seguridad que se necesitan para mantener la seguridad tanto en las entradas como en el interior del hotel.

Se presentan las áreas y zonas de todo el hotel:

- **Estacionamiento**

ESTACIONAMIENTO			
ZONA	**DESCRIPCIÓN**	**RIESGOS**	**REQUERIMIENTOS**
Entrada principal	Entrada de vehículos de huéspedes	Entrada de delincuentes	Un punto de control de video vigilancia alta definición
Ascensor	Ingreso al ascensor y parte del parqueadero	Ingreso de delincuentes, robo de accesorios de autos	Punto de control de video vigilancia definición estándar Punto de control de acceso
Parqueadero	Lugar donde permanecen autos de huéspedes durante su alojamiento	Robo de accesorios de autos	Dos puntos de control que cubran el resto del estacionamiento
Cuarto de maquinas	Lugar en donde se encuentran equipos de alta tensión	Electrocución, inundación por rotura de tuberías en caso de emergencia	Punto de control de video vigilancia definición estándar

Tabla 6.1 Detalles del estacionamiento

Elaborado por el investigador

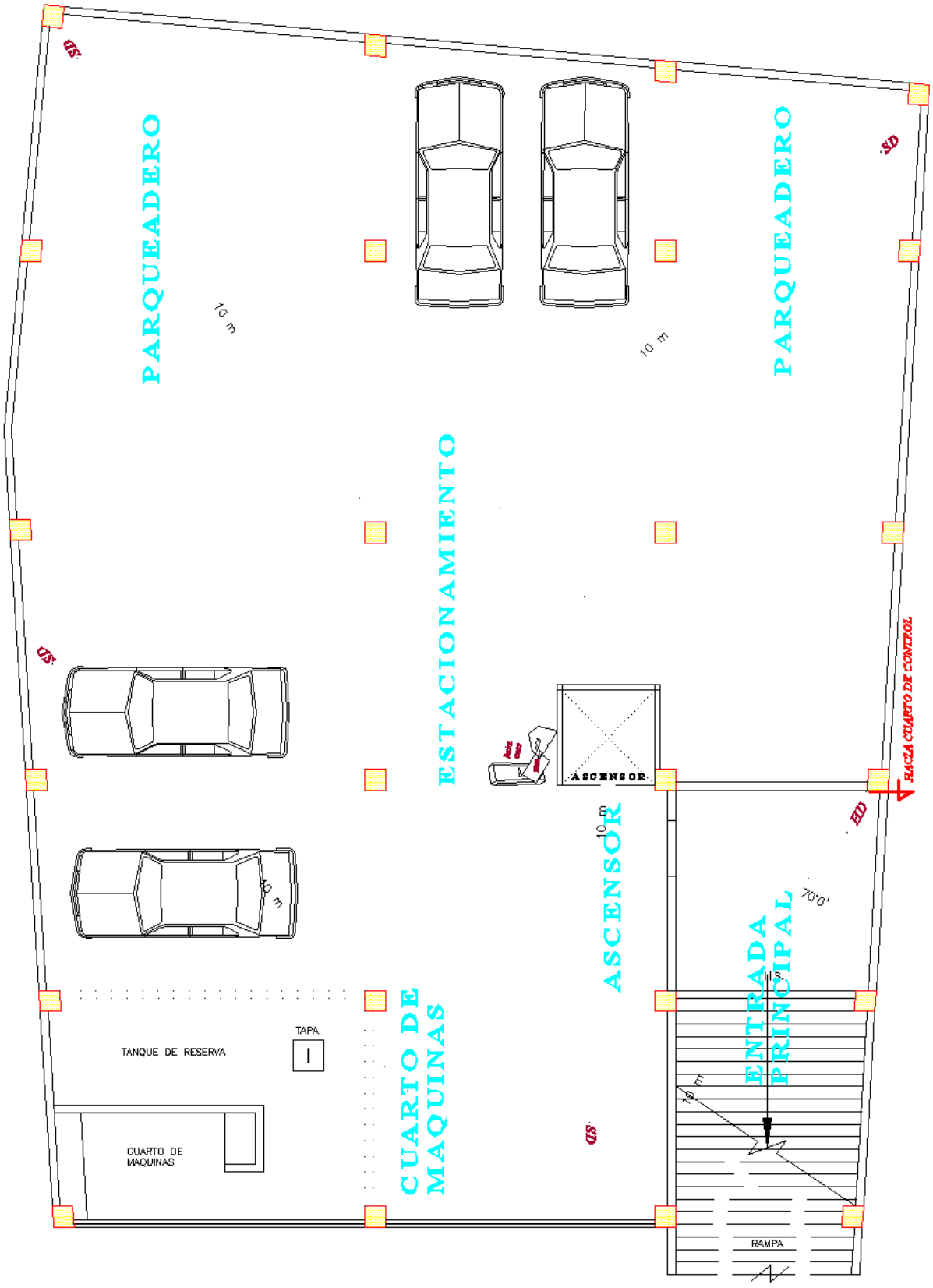


Fig. 6.23 Parqueadero del Hotel Destiny

Elaborado por el investigador

❖ **Planta baja**

PLANTA BAJA			
ZONA	**DESCRIPCIÓN**	**RIESGOS**	**REQUERIMIENTOS**
Ingreso principal	Entrada huéspedes al hotel y clientes del restaurant	Entrada de delincuentes, robo de pertenencias	Tres puntos de control en la entrada, tanto en el exterior cámaras de alta definición
Restaurant y sala de eventos	Lugar de alimentación de huéspedes como de visitantes	Ingreso de delincuentes, perdida de objetos	Punto de video vigilancia en un punto estratégico de definición estándar
Cocina	Lugar donde se prepara la comida del hotel	Acceso de personas no autorizadas	Un punto de video vigilancia con definición estándar
Administración	Lugar en donde se encuentran la administración	Perdida de objetos, dinero, ingreso intrusos	Un punto de video vigilancia de definición estándar
Cuarto de equipos	Lugar en donde se encuentra los equipos de comunicación	Robo de información del hotel, ingreso de intrusos	Un punto de video vigilancia además del control de acceso al cuarto
Pasillo	Lugar de transito de persona como de empleados	Perdida de objetos de bodega y habitaciones	Un punto de video vigilancia de definición estándar
Habitaciones	Lagar de alojamiento de huéspedes	Perdida de objetos personales así como ingreso de intrusos	Punto de video vigilancia que cubra las entradas así como el control de acceso en cada habitación

Tabla 6.2 Detalles de la planta baja

Elaborado por el investigador

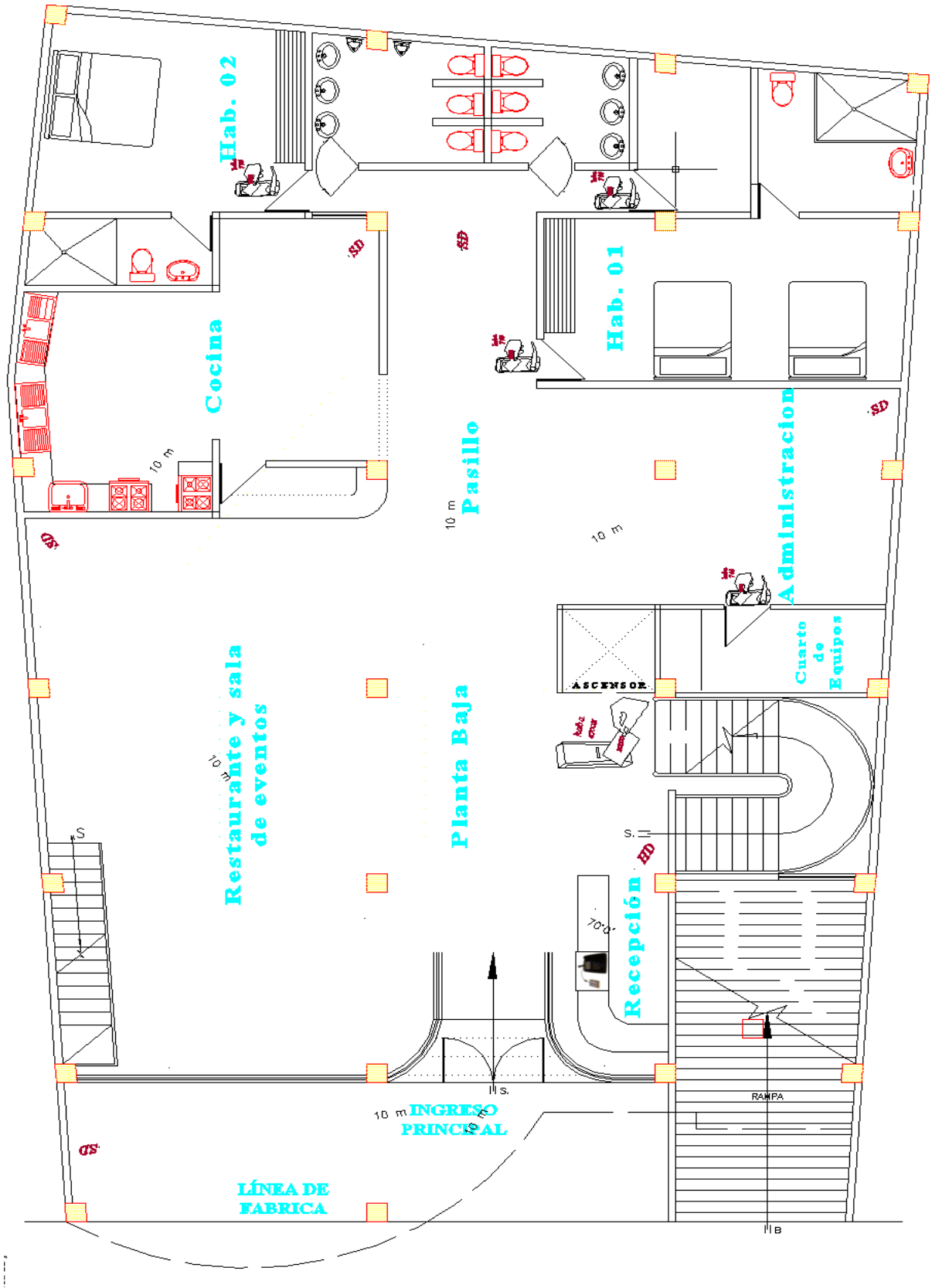


Fig. 6.24 Planta baja Hotel Destiny

Elaborado por el investigador

❖ **Primera planta**

PRIMERA PLANTA			
ZONA	**DESCRIPCIÓN**	**RIESGOS**	**REQUERIMIENTOS**
Bar cafetería	Lugar en donde se sirve alcohol en moderación además de café	Entrada de delincuentes, robo de pertenencias, perdida de objetos	Dos puntos de video vigilancia que cubran el área comprendida del bar
Ingreso al ascensor e ingreso al pasillo	Ingreso a la Primera planta y pasillo en donde se encuentra las habitaciones y bodega del bar	Ingreso de delincuentes, perdida de pertenencias, evitar que niños jueguen en el ascensor	Punto de video vigilancia con definición estándar, además de un punto de control de acceso en el ascensor para evitar el uso indebido
Pasillo	Ingreso principal a habitaciones y bodegas de esta planta	Ingreso de intrusos, perdida de objetos	Punto de video vigilancia definición estándar que cubra los ingresos en general que de una buena visión de lo que sucede
Bodega de licores	Lugar de almacenamiento de licores de alto costo del bar como de otras bebidas	Perdida de objetos, ingreso de intrusos	Punto de video vigilancia de definición estándar además de un punto de control de acceso a la bodega

Bodega de Pertenencias	Lugar en donde se realiza el encargo de pertenencias de los huéspedes que alcancen en la habitación o si su tiempo de hospedaje caduca se guarda ahí	Perdida de objetos de valor cae a cargo del hotel el cuidado	Punto de video vigilancia de alta definición así como el control de acceso de ingreso al cuarto
Habitaciones	Lugar de alojamiento de huéspedes	Perdida de objetos personales así como ingreso de intrusos o perdida por propios empleados del hotel	Punto de video vigilancia que cubra las entradas así como el control de acceso en cada habitación

Tabla 6.3 Detalles de la primera planta

Elaborado por el investigador

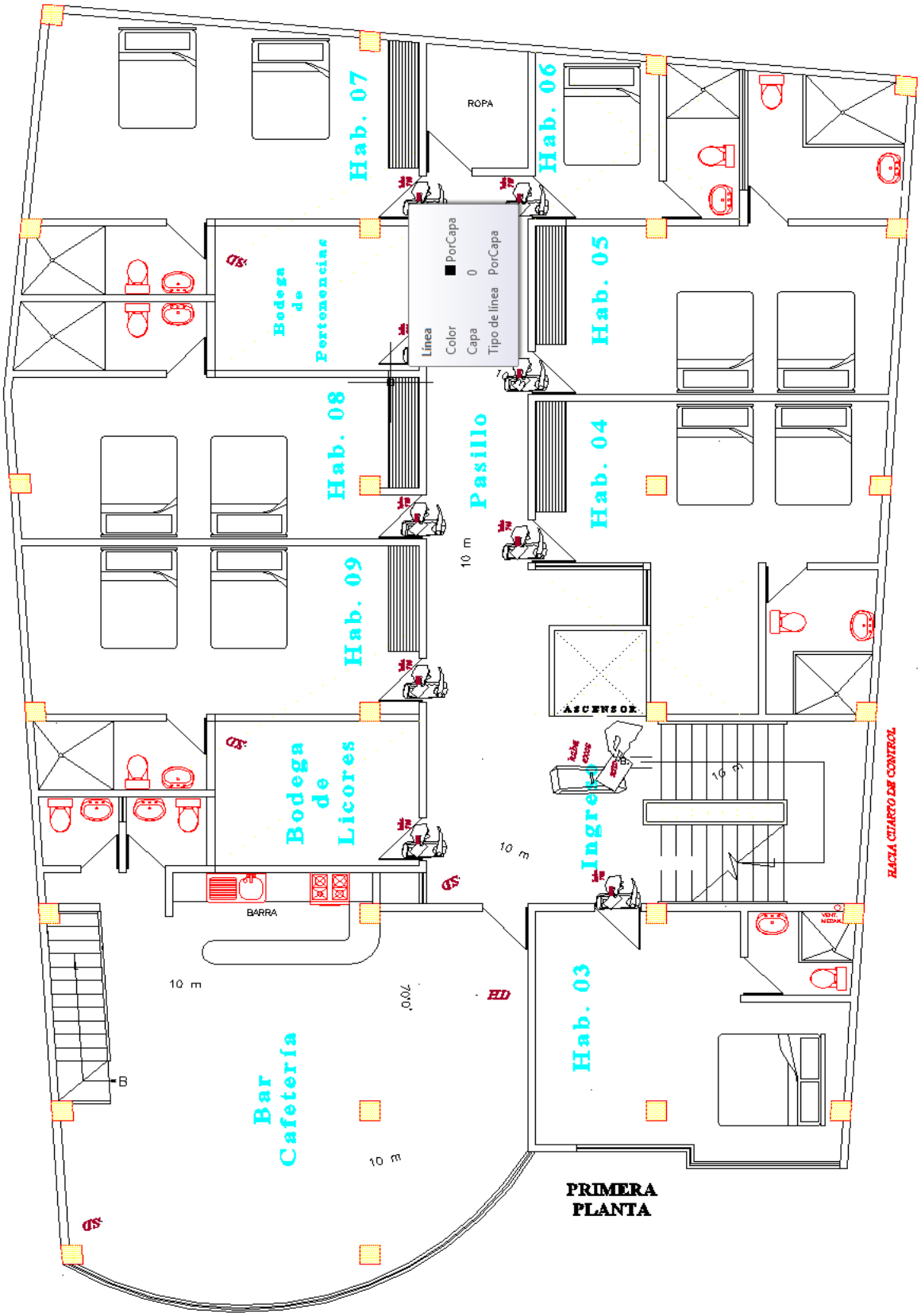


Fig. 6.25 Primera planta Hotel Destiny

Elaborado por el investigador

❖ **Segunda Planta**

SEGUNDA PLANTA			
ZONA	**DESCRIPCIÓN**	**RIESGOS**	**REQUERIMIENTOS**
Ingreso al ascensor e ingreso al pasillo	Ingreso a la Primera planta y pasillo en donde se encuentra las habitaciones y bodega del bar	Ingreso de delincuentes, perdida de pertenencias, evitar que niños jueguen en el ascensor	Punto de video vigilancia con definición estándar, además de un punto de control de acceso en el ascensor para evitar el uso indebido
Pasillo	Ingreso principal a habitaciones y bodegas de esta planta	Ingreso de intrusos, perdida de objetos	Punto de video vigilancia definición estándar que cubra los ingresos en general que de una buena visión de lo que sucede
Cuarto de computación	Lugar donde se encuentran computadores con navegación de internet para los huéspedes y visitantes	Robo de equipos, perdida de objetos	Punto de video vigilancia de definición estándar para el control en el interior del cuarto y control de acceso
Cuarto de juegos	Lugar donde se encuentra dos máquinas de juegos a disposición de los huéspedes y visitantes	Robo de equipos, perdida de objetos	Punto de video vigilancia de definición estándar para el interior del cuarto y control de acceso

Cuarto de recreación	Lugar en donde se pueden proyectar películas para el entretenimiento de los huéspedes y visitantes	Robo de equipos, perdida de objetos	Punto de video vigilancia de definición estándar para el interior del cuarto y control de acceso
Habitaciones y suite	Lugar de alojamiento de huéspedes, la suite cuenta con varios tipos de atractivos en su interior	Perdida de objetos personales así como ingreso de intrusos o perdida por propios empleados del hotel	Punto de video vigilancia que cubra las entradas así como el control de acceso en cada habitación

Tabla 6.4 Detalles de la segunda planta

Elaborado por el investigador

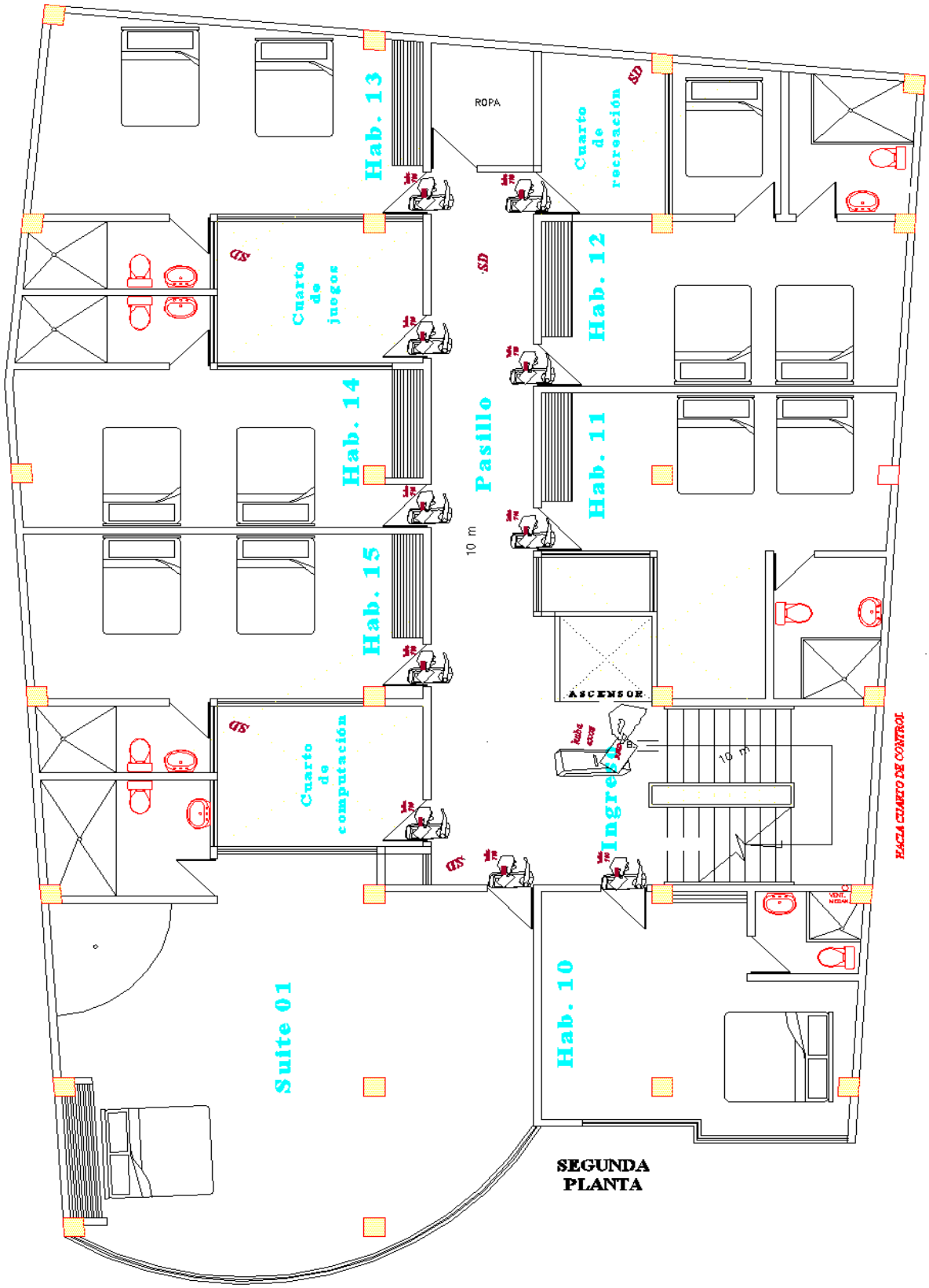


Fig. 6.26 Segunda planta Hotel Destiny

Elaborado por el investigador

❖ **Tercera planta**

TERCERA PLANTA			
ZONA	**DESCRIPCIÓN**	**RIESGOS**	**REQUERIMIENTOS**
Ingreso al ascensor e ingreso al pasillo	Ingreso a la Primera planta y pasillo en donde se encuentra las habitaciones y bodega del bar	Ingreso de delincuentes, perdida de pertenencias, evitar que niños jueguen en el ascensor	Punto de video vigilancia con definición estándar, además de un punto de control de acceso en el ascensor para evitar el uso indebido
Pasillo	Ingreso principal a habitaciones y bodegas de esta planta	Ingreso de intrusos, perdida de objetos	Punto de video vigilancia definición estándar que cubra los ingresos en general que de una buena visión de lo que sucede
Habitaciones y suite	Lugar de alojamiento de huéspedes, la suite cuenta con varios tipos de atractivos en su interior	Perdida de objetos personales así como ingreso de intrusos o perdida por propios empleados	Punto de video vigilancia que cubra las entradas así como el control de acceso en cada habitación

Tabla 6.5 Detalles de la tercera planta

Elaborado por el investigador

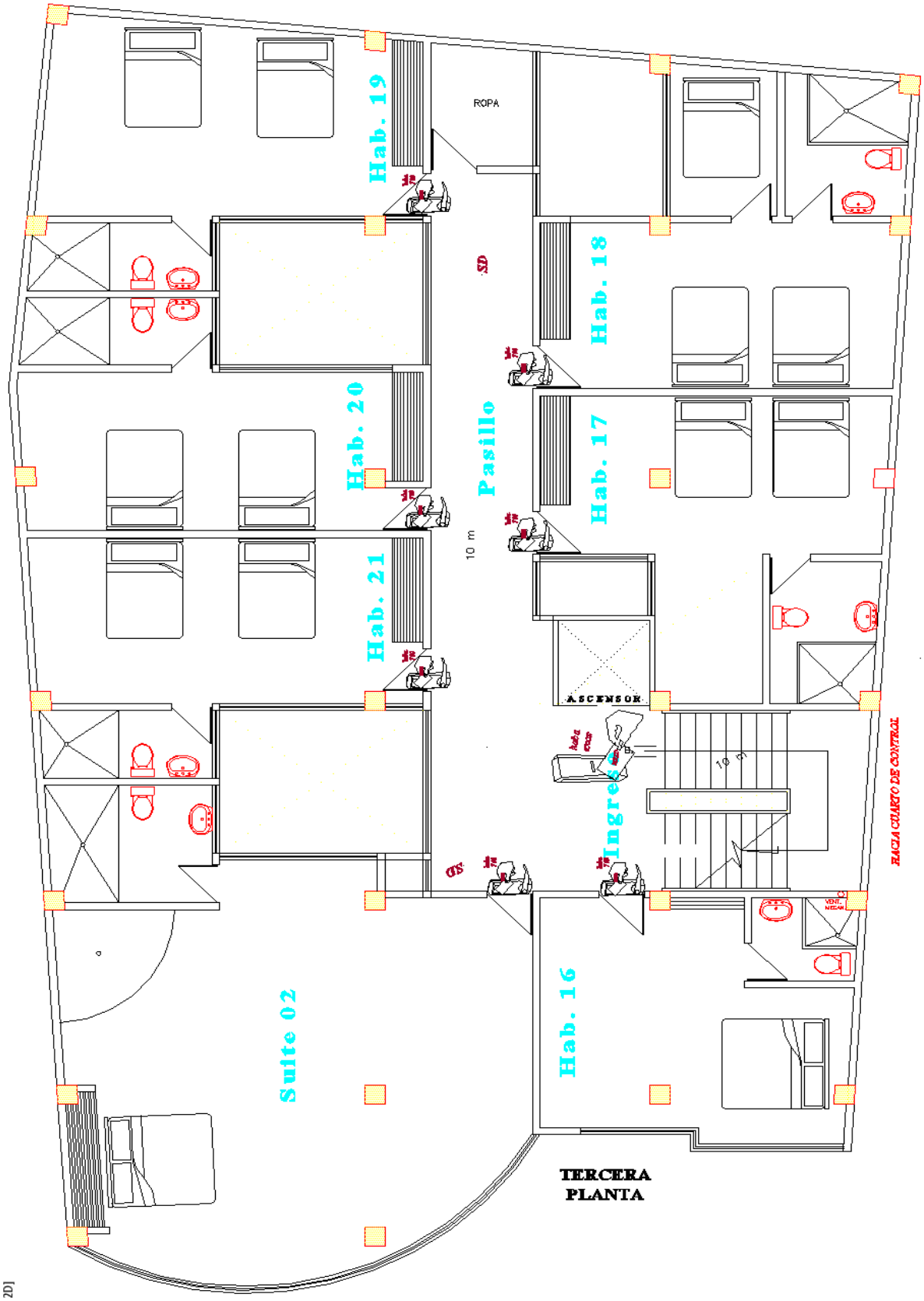


Fig. 6.27 Tercera planta Hotel Destiny

Elaborado por el investigador

❖ **Cuarta Planta**

CUARTA PLANTA			
ZONA	**DESCRIPCIÓN**	**RIESGOS**	**REQUERIMIENTOS**
Ingreso al ascensor e ingreso al pasillo	Ingreso a la Primera planta y pasillo en donde se encuentra las habitaciones y bodega del bar	Ingreso de delincuentes, perdida de pertenencias, evitar que niños jueguen en el ascensor	Punto de video vigilancia con definición estándar, además de un punto de control de acceso en el ascensor para evitar el uso indebido
Pasillo	Ingreso principal a habitaciones y bodegas de esta planta	Ingreso de intrusos, perdida de objetos	Punto de video vigilancia definición estándar que cubra los ingresos en general que de una buena visión de lo que sucede
Habitaciones y suite	Lugar de alojamiento de huéspedes, la suite cuenta con varios tipos de atractivos en su interior	Perdida de objetos personales así como ingreso de intrusos o empleados	Punto de video vigilancia que cubra las entradas así como el control de acceso en cada habitación

Tabla 6.6 Detalles de la cuarta planta

Elaborado por el investigador

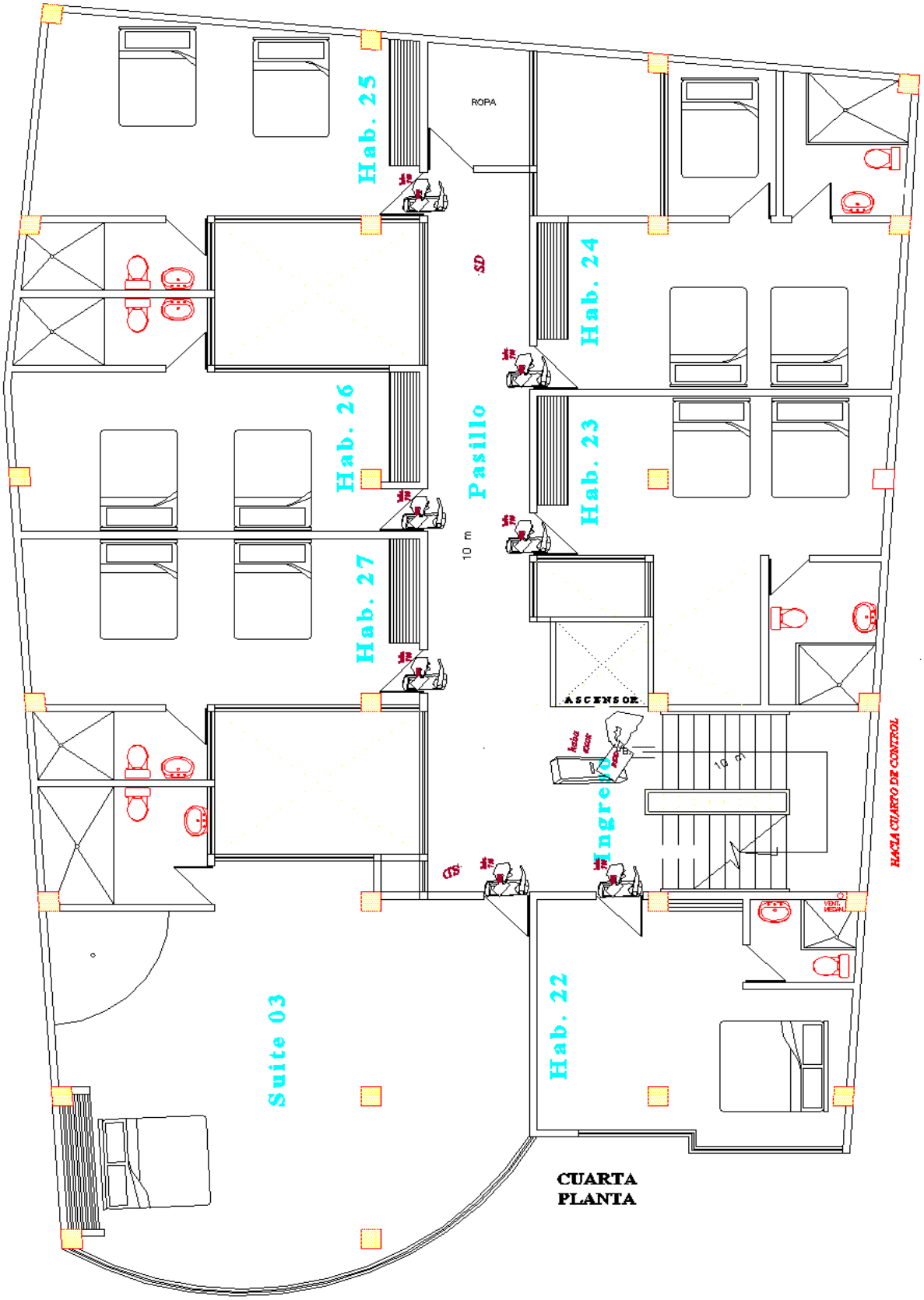


Fig. 6.28 Cuarta planta Hotel Destiny

Elaborado por el investigador

❖ **Terraza**

TERRAZA			
ZONA	**DESCRIPCIÓN**	**RIESGOS**	**REQUERIMIENTOS**
Cuarto de Sistema solar	Cuarto de equipos del sistema solar del Hotel	Control de fugas que se pueden producir	Un punto de control de video vigilancia definición estándar
Jacuzzi, turco y Baños	Lugar de relax de huéspedes del Hotel entre otros	Perdida de pertenencias, ingreso de delincuentes	Punto de control de video vigilancia definición estándar
Lavandería	Lugar en donde se lavan seca los accesorios del hotel	Robo de equipos, ingreso de intrusos	Punto de control de video vigilancia definición estándar Punto de control de acceso
Cuarto de descanso	Lugar de descanso para empleados que hagan doble turno	Perdida de objetos, ingreso de intrusos	Punto de control de video vigilancia definición estándar Punto de control de acceso

Tabla 6.7 Detalles de la terraza

Elaborado por el investigador

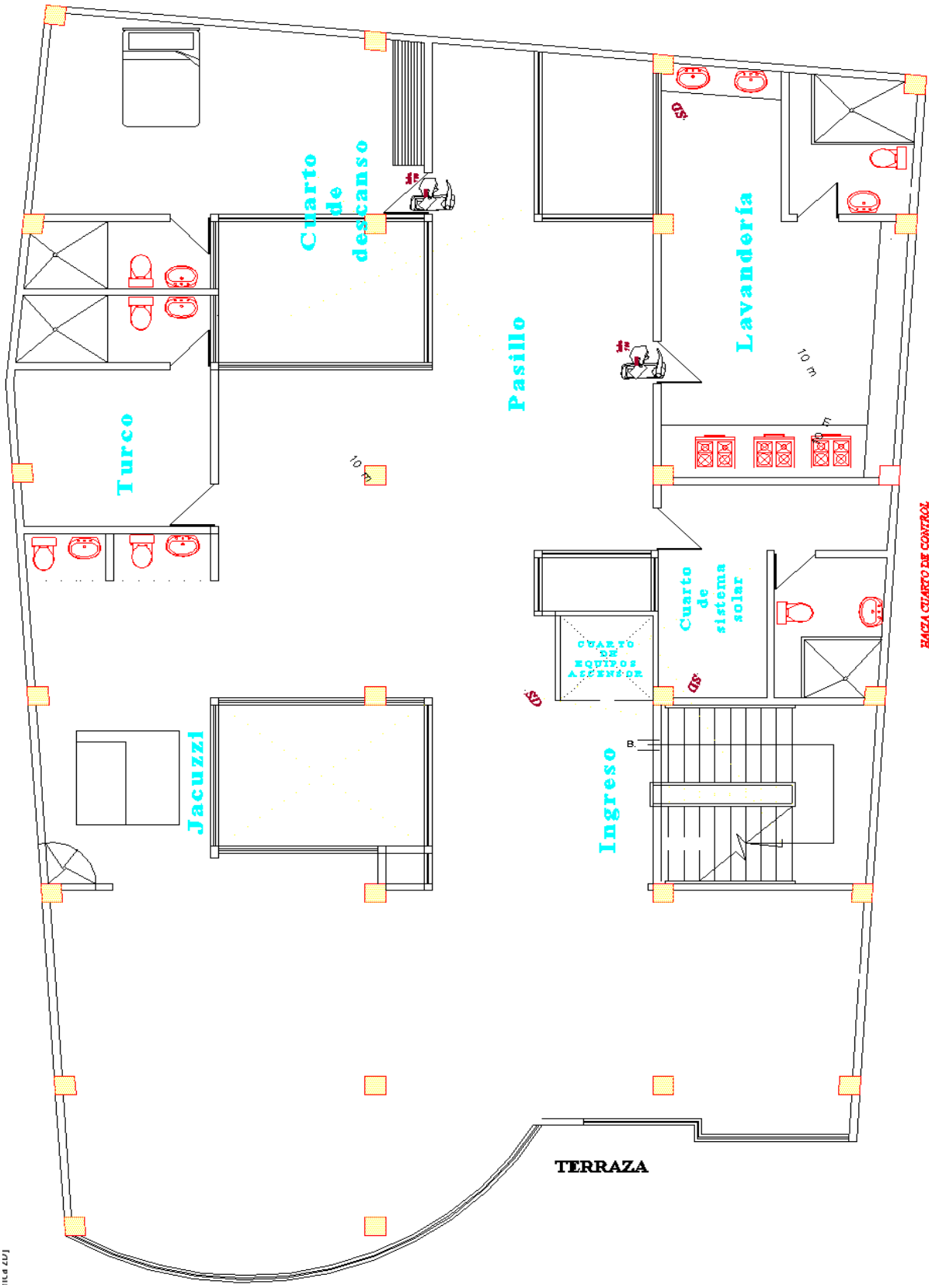


Fig. 6.29 Terraza Hotel Destiny

Elaborado por el investigador

Las presentes tablas se obtuvieron a través de los planos y en visitas realizadas para poder ver la realidad de cada área cabe recalcar que se planifico con 8 meses de anterioridad a la presentación del proyecto, los puntos de control están ya ubicados debido a que cuando esté terminada la construcción por motivos de estética no se pueden realizar muchas modificaciones en la infraestructura.

6.8.1.3 Distribución de requerimientos por zonas

En este punto se contabilizara los puntos exactos tanto de control de acceso como de video vigilancia la comparación y elección de equipos se realizara a continuación, para todo esto se cuenta con un presupuesto, debido a esto debemos ver las características necesarias que satisfagan las necesidades de seguridad que presenta cada zona y área restringida del hotel.

ANÁLISIS DE REQUERIMIENTOS				
PISO	**ZONA**	**CONTROL DE ACCESO**	**NUMERO DE CÁMARAS**	
			DEFINICIÓN ESTÁNDAR	**ALTA DEFINICIÓN**
Estacionamiento	Entrada principal			**X**
	Ascensor	**X**	**X**	
	Parqueadero		**XX**	
	Cuarto de maquinas		**X**	
Planta baja	Entrada principal Hotel y restaurant		**X**	**X**
	Ascensor	**X**		
	Restaurant	**X**	**X**	
	Cocina		**X**	
	Administración		**X**	
	Cuarto de equipos	**X**	**X**	
	Pasillo		**X**	
	Habitaciones	**XX**		

Primera planta	Bar cafetería		**X**	**X**
	Ingreso piso		**X**	
	Ingreso ascensor	**X**		
	Pasillo		**X**	
	Bodega de licores	**X**	**X**	
	Bodega de Pertenencias	**X**	**X**	
	Habitaciones	**XXXXXXX**		
Segunda planta	Ingreso piso		**X**	
	Ingreso ascensor	**X**		
	Pasillo		**X**	
	Cuarto de computación	**X**	**X**	
	Cuarto de juegos	**X**	**X**	
	Cuarto de recreación	**X**	**X**	
	Habitaciones y suite	**XXXXXXX**		
Tercera planta	Ingreso piso		**X**	
	Ingreso ascensor	**X**		
	Pasillo		**X**	
	Habitaciones y suite	**XXXXXXX**		
Cuarta planta	Ingreso al piso		**X**	
	Ingreso al ascensor	**X**		
	Pasillo		**X**	
	Habitaciones y suite	**XXXXXXX**		
Terraza	Cuarto de Sistema solar		**X**	
	Jacuzzi, sauna y Baños		**X**	
	Lavandería	**X**	**X**	
	Cuarto de descanso	**X**		
Total		44	26	4

Tabla 6.8 Contabilización total de requerimientos

Elaborado por el investigador

RESUMEN DE REQUERIMIENTOS		
CÁMARAS		CONTROL DE ACCESOS
DEFINICIÓN ESTÁNDAR	ALTA DEFINICIÓN	
26	4	46
Total = 30		Total = 46

Tabla 6.9 Resumen de requerimientos

Elaborado por el investigador

6.8.2 Consideraciones previas al diseño

Una vez que se ha obtenido los datos totales de requerimientos en cuanto a número de dispositivos tanto del control de acceso como del circuito cerrado de televisión es importante definir el tipo de tecnología a usarse en el diseño, debido a que existe un gran sin número de posibilidades al momento de elegir, cabe recalcar que se tiene un presupuesto asignado para equipos e instalación. Se tomara en cuenta los siguientes puntos:

6.8.2.1 Requerimientos de uso del control de accesos nivel usuario

Antes de continuar se toma en cuenta el tipo de funcionamiento que se solicita por parte de propietarios y encargados del hotel, esto se debe a que las personas que serán asignadas para trabajar en la parte de seguridad del hotel dispongan de un sistema amigable y no tan complejo de usar se toman en cuenta los siguientes puntos importantes que debe tener el sistema de control de acceso y de video vigilancia. Que tengan las características básicas como:

- Fácil acceso a la aplicación
- Acceso como administrador y como usuario
- Programa de fácil uso
- De preferencia que sea en idioma español

Además de poder tener acceso remoto en caso del video vigilancia debido a que permanentemente están de viaje y les gustaría contar con un sistema que se pueda acceder en cualquier parte del mundo.

6.8.2.2 Elección de la topología del control de accesos

Los sistemas de control de acceso se dividen en dos grupos los cuales presentan características distintas, como se habló anteriormente no se puede sobredimensionar las características de los equipos en cosas innecesarias para un hotel además que repercuten en el momento del costo beneficio, además de sus ventajas y desventajas que se analizaran a continuación en un breve resumen que se indica en la tabla 6.10.

<table>
<tr><th colspan="2">CONTROL DE ACCESOS</th></tr>
<tr><td colspan="2">Un control de acceso puede ser centralizado o autónomo, pero ambos requieren de los mismos componentes a excepción del software de control requerido para el sistema centralizado.</td></tr>
<tr><th>CENTRALIZADOS</th><th>AUTÓNOMO</th></tr>
<tr><td>Todos están conectados a un hardware y software especializado que transfiere información en tiempo real y lo almacena en un Pc o periférico</td><td>Funcionan previa configuración individual son capaces de almacenar la información de un número determinado de eventos que suceden en torno a el</td></tr>
<tr><th colspan="2">CARACTERÍSTICAS</th></tr>
<tr><td>• Panel de control que convierte la señal analógica de cada punto en digital
• Cuentan con sistema de monitoreo en tiempo real
• Asignación de autorización de ingreso y transferencia automática al equipo de control de acceso
• Software amigable y de fácil funcionamiento
• Hardware propio de cada marca para</td><td>• Cada equipo de control se configura con una identificación única
• Al no estar centralizado puede trabajar con un sistema de alimentación independiente como pilas o baterías
• Guarda los últimos eventos según su programación
• Para su comunicación se utiliza hardware encargado de cada marca
• Se puede restringir con una identificación de emergencia</td></tr>
</table>

la interconexión de equipos • Sistema de bloqueo en caso se quiera denegar e acceso • Sistema de emergencia para apertura de todas las puertas • Control de ingresos por horarios • Sistema autónomo en caso de desconexión del panel • Conexión de botón de apertura de salida y notificación automática	• Fácil instalación en lugares donde se necesite un control moderado • Control de ingreso por horarios • Configuración de días no hábiles para un bloqueo permanente • Conexión de botón de apertura de salida • Sistema de identificación biométrico o por tarjeta magnética o de proximidad
VENTAJAS	
• Reporte inmediato de eventos • Administración remota en caso de emergencias • Bloqueo y desbloqueo de puntos de control según necesidad • La programación de cada punto se actualiza de manera inmediata sin necesidad de interactuar con cada uno	• Cuenta con las principales características del sistema centralizado • Sencillo de usar una vez programado • Puede contar con alimentación propia • Fácil de adaptar a ambientes en donde no se puedan realizar modificaciones
DESVENTAJAS	
• Se debe planificar la construcción para la distribución del sistema antes de la implementación • En caso de fallo eléctrico el sistema queda sin sus funciones principales • Mayor mantenimiento por cuestión de cableado y energía • Mucho más costoso que un sistema tradicional	• En caso de violación del punto de acceso el sistema no puede transmitir la información • Está limitado a un destinado número de características • Puede ser afectado por fallo eléctrico • En caso se reconfigure se tiene que programar directamente el punto de control

Tabla 6.10 Comparación de sistemas de control de acceso

Elaborado por el investigador

Después de este breve análisis de los tipos de topología de control de acceso, junto con el encargado de diseño tecnológico se decidió por el control de acceso autónomo, considerando los siguientes puntos.

- Fácil administración de los puntos de control.
- Fácil adaptación en ambientes donde no se puede realizar modificaciones.
- Control de ingreso por horarios, registro de ingresos y eventos.
- Menor costo de instalación.
- Autonomía propia en caso de fallo eléctrico.
- Fácil mantenimiento y reparación.

6.8.2.3 Elección del elemento de identificación del control de accesos

En capítulos anteriores se trató el tema de elementos de identificación los cuales permiten la elección de los equipos que se encargaran del control de accesos, brevemente se realizara un resumen de las características, ventajas y desventajas de los principales tipos de identificación para la elección de la más adecuada para la implementación en el hotel Destiny.

Los principales medios de identificación son:

MEDIOS DE IDENTIFICACIÓN			
TIPO	**CARACTERÍSTICAS**	**VENTAJAS**	**DESVENTAJAS**
Pin Numérico 	• Varios niveles de codificación • Código maestro • Código de usuario	• Fácil de usar en ambientes de bajo control • Permite el control de una o varias puertas • Bajo costo	• Fácil de vulnerar • No permite asociar una clave a un usuario distinto al administrador
Tarjeta magnética	• Adopto esta tecnología de la industria bancaria • Son las tradicionales de	• Tarjetas de bajo costo • Se pueden imprimir	• Seguridad mínima aceptable

	PVC con su banda magnética • Es posible codificar una información binaria en forma magnética longitudinal en la banda	las tarjetas • Bajo costo de implementación	• Desgaste con el uso diario • Los equipos de funcionamiento fueron reemplazados por tarjetas de proximidad
Tarjeta de proximidad RFID 	• Tarjeta pasiva que no posee alimentación propia • Comunicación por radio frecuencia sin necesidad de contacto • existen de varios rangos, bajo, medio, largo alcance	• No debe pasarse por ninguna ranura lo cual aumenta su vida • Tarjetas de bajo costo y diseño al gusto del cliente • Fácil uso hasta un niño lo puede usar • Alta velocidad de lectura	• Seguridad media • El lector puede fallar por interferencia de frecuencias • No puede usarse en sistemas de distinta marca
Sensor biométrico 	• Permite el reconocimiento único de humanos basado en rasgos físicos • Varios niveles de sensibilidad de lectura • Permite almacenar los ingresos en una memoria interna	• Casi imposible de vulnerar • Varios niveles de seguridad • Se usa en la mayor parte de áreas restringidas	• Costo muy elevado, requiere un mantenimiento especial • El lector puede fallar por su mal uso • El usuario debe estar familiarizado con su uso

Tabla 6.11 Medios de identificación control de accesos

Elaborado por el investigador

Con la presente tabla podemos descartar el uso de dos medios de identificación los cuales no presentan las ventajas necesarias para su implementación que es el pin numérico porque al ser un hotel no se pueden asignar miles de pines al mes al no ser centralizado se tendría que configurar uno por uno los puntos de control, la tarjeta magnética presenta mucho desgaste en el equipo lo cual no garantiza una vida útil que este dentro de los parámetros establecidos para su funcionamiento.

Se toman en cuenta dos posibles soluciones a la propuesta de control de acceso donde se realiza una comparación adicional de sus prestaciones para poder descartar cualquier duda sobre cada sistema:

- **Tabla comparativa de sistemas biométricos:**

Lo que sigue a continuación es una tabla en la que se recogen las diferentes características de los sistemas biométricos:

	Ojo (Iris)	**Ojo (Retina)**	**Huellas dactilares**	**Geometría de la mano**	**Escritura y firma**	**Voz**	**Cara**
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Media	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta	Alta
Prevención de ataques	Alta	Muy alta	Alta	Alta	Media	Media	Media
Aceptación	Media	Media	Alta	Media	Muy alta	Baja	baja
Estabilidad	Alta	Alta	Alta	Media	Baja	Media	Media

Tabla 6.12 Comparación sistemas biométricos

Elaborado por el investigador

Actualmente la lectura biométrica de las minucias de la huella digital es, sin duda, el sistema biométrico más avanzado y seguro del mercado.

Al ser la huella dactilar y la tarjeta de proximidad la posible solución se realiza una comparación basada en medidas de seguridad para establecer la solución.

Huella dactilar vs Tarjeta de Proximidad		
Características	**Huellas**	**Proximidad**
Agilidad de marcación	Buena	Excelente
Costo del lector	Alto	Medio
Costo de la tarjeta	Sin costo	Bajo
Durabilidad	Media	Excelente
Identificación univoca	Excelente	No asegurable
Mantenimiento	Medio	No requiere
Resistente a la intemperie	Baja	Excelente
Resistente al sabotaje	Baja	Excelente
Seguridad	Excelente	media

Tabla 6.13 Huella dactilar vs tarjeta de proximidad

Elaborado por el investigador

6.8.2.4 Asignación del tipo de equipos para el control de accesos

Como conclusión y después del análisis pertinente se puede definir que la tarjeta de proximidad satisface las necesidades y requerimientos de seguridad que se plantea dentro del hotel, su fácil uso y durabilidad garantizan el funcionamiento permanente del control de acceso sin embargo se puede implementar lectores de huella en las zonas que representen mayor seguridad de acceso, para la determinación de esta decisión se tomó en cuenta:

- Al no tener un control de accesos centralizado para el acceso se debe registrar la huella en el punto de control lo cual es incómodo para el personal que se encargue de la recepción del hotel
- El sistema es costoso y no funciona en determinadas condiciones, el hotel cuenta con áreas de comida, hidromasaje, entre otros que con el pasar del tiempo causaran que los equipos dejen de responder por el uso después de que los clientes salgan de dichas áreas
- Las habitaciones presentan capacidad de hasta 5 personas, la huella es intransferible por lo cual se debería registrar a cada persona, no así con la tarjeta que puede ser usada por cualquier ocupante de la habitación.
- Al optar el uso de huella, se debe capacitar brevemente sobre el uso del sistema en el caso de niños sería imprudente dejarlos solos que manejen y estropeen los equipos de seguridad.

Una vez decidido el tipo de identificación y la topología de implementación queda la búsqueda de los diferentes tipos de equipos que existen en el mercado para eso se toma en cuenta los siguientes parámetros que son importantes al momento de comprar dispositivos tecnológicos dentro de nuestro país:

- El equipo o dispositivo tecnológico debe contar por lo menos con 2 años de garantía escrita en caso de fallo por defectos de fabricación.
- La empresa distribuidora o importadora debe contar con soporte técnico en caso de fallo de los equipos además de contar con repuestos en caso de deterioro o daño del sistema y contar con soporte telefónico.
- La empresa distribuidora o importadora debe contar con experiencia en equipos dedicados para hotelería debido a que hay muchas empresas que no prestan buen servicio en caso de daño masivo.
- Los equipos deben ser resistentes al uso diario en especial golpes, polvo, grasa, agua debido a que el uso que se da en un hotel y hay que tomar estas precauciones para alargar la vida útil de los equipos.

Como referencia es preferible indagar donde ya están instalados controles de acceso y ver si las empresas que realizaron la venta e instalación de equipos responden con los requerimientos que se presentan en caso de falla o molestias del sistema, además del uso del internet, donde las principales empresas se postulan en busca de clientes potenciales.

Después de la visita a algunos lugares que cuentan con control de acceso en la ciudad de Ambato y Quito y una pequeña revisión en internet encontramos las siguientes empresas que ofrecen servicios de control de acceso.

Entre las empresas postulantes y mejor referidas tenemos:

EMPRESA	PRINCIPALES SERVICIOS	PAGINA WEB
PROMATCO	• Sistemas de Control de Acceso • Sistemas de Control de Rondas de guardias • CCTV (Circuitos Cerrados de Televisión) • Detectores de Metales de mano y en forma de arco • Detectores de Rayos X • Dispositivos biométricos • Paneles para instalaciones contra incendios • Sistemas de Alarma contra Robo • Sistemas de Seguridad Perimetral	http://www.promatco.com.ec/acc.html#2
ACE CONTROL	• Sistema de control de accesos • Barreras de acceso • CCTV • Lectores de proximidad • Lectores biométricos • Software para administración de parqueaderos	http://www.acecontrol.com.ec/
SISTEMAS DE SEGURIDAD	• Control de accesos • CCTV • Cámaras Ip • Sistema de alarmas	http://www.sistemasdeseguridad.com.ec/
CETA	• Control de acceso para hotel • Cajas fuertes • Cajas de seguridad	http://ceta.com.ec/

	• Puertas de seguridad	
A TIEMPO	• Sistemas biométricos • Sistemas de proximidad • Control de asistencia personal • Sistemas de control de guardia • Cámaras ip	http://atiempo.com.ec/productos.html
ML CONSULTORES	• Sistemas biométricos • Control de acceso • Centrales telefónicas • Señalética y seguridad industrial • Tarjetas de proximidad	http://www.consultoresml.com/category/nosotros/

Tabla 6.14 Empresas con servicios de control de acceso

Elaborado por el investigador

Dentro de las empresas que se presentaron en la tabla 6.12 todas cuentan con servicios de seguridad mediante control de accesos, principalmente por tarjetas de proximidad la cual el punto de interés del proyecto, dentro de la amplia gama de dispositivos que se encuentran en venta, existe una gran variante por la cual se tomara la decisión de elección del sistema debido a que esto conlleva a la modificación o no de la infraestructura del Hotel, se presenta un rápido análisis de las dos distintas infraestructuras del control de accesos por tarjeta de proximidad.

Existen dos esquemas de implementación de un sistema de control de acceso por tarjeta de proximidad o biométrico.

- **Instalación de un sistema de control de acceso autónomo con todas sus características**

Fig. 6.30 Diagrama general de instalación control de accesos

Fuente: http://www.yftelperu.com/comunicacion.html

En la fig. 6.30 Se presenta un diagrama de instalación de un sistema de control de acceso con sus características técnicas soportadas como son alarma, cerradura eléctrica, botón de salida entre otros, este régimen de instalación está dirigido a empresas mas no hoteles en donde la complejidad de instalación complica la adecuación de la infraestructura, debido a que se necesita una fuente de alimentación externa y dotar al área de tuberías para la conexión de cables tanto de sensores como de cerraduras.

- **Instalación de un sistema de control autónomo con las características básicas de funcionamiento**

Como se observa en la fig. 6.31 existen cerraduras especiales que incorporan el dispositivo de control de acceso en su interior y cuentan con una protección igual o mejor a las que disponen los controles de acceso tradicionales.

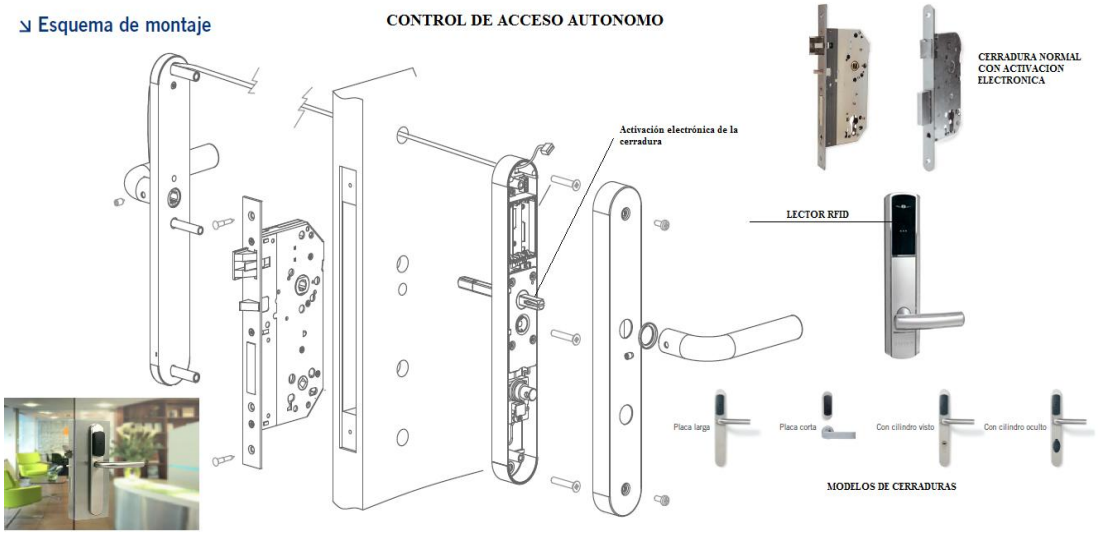


Fig. 6.31 Diagrama interno de una cerradura con control de acceso

Fuente: http://www.encryptec.com.ar/pdf/catalogo.pdf

la gran ventaja de este tipo de dispositivos es su fácil instalación en infraestructuras de todo tipo ya que cuentan con alimentación propia mediante pilas o baterías de larga duración hasta 3 años en el mejor de los casos excelentes para ambientes residenciales, hoteles, empresas medianas, una gran apuesta tecnológica al alcance de todos.

6.8.2.5 Comparación de equipos de control de acceso según sus características

Antes de la comparación de equipos se realiza la elección del tipo de infraestructura de instalación de los equipos basado en los siguientes puntos.

- Fácil instalación y reparación
- Facilidad de uso
- Autonomía propia en caso de corte eléctrico
- Lectura rápida del medio de identificación
- Durabilidad y resistencia

Como resultado de la presentación de las distintas infraestructuras de los sistemas de control de acceso, se pudo obtener como resultado que el tipo de equipos que presenta mejores prestaciones para hotel son los que traen integrado el sistema de control y permiten autonomía de larga duración.

Anteriormente se investigó las empresas que cuentan con equipos de control de acceso, se solicitó proformas de equipos de control de accesos las cuales fueron recibidas por escrito con las características de los equipos su precio de venta y instalación dentro y fuera de la ciudad de origen de las empresas.

Las empresas y equipos de control de accesos que fueron presentados se detallan a continuación:

EMPRESA	EQUIPO	CARACTERÍSTICAS
A TIEMPO	Cerradura Biometrica y proximidad Biosystem lock 13000  Cerradura biométrica de huella digital, productos exclusivo para suites, oficinas, hoteles y casas, de carcasa resistente	• Capacidad de 150 huellas registradas • 450 contraseñas • 240 numeros ID • Resolución: 500DPI • Tiempo de identificación en huellas 2seg • Tiempo de identificación en tarjetas 0.50 seg • Energía: 4 pilas AA • Transacciones: 4000 aprox. • Temperatura: 0-45 grados centígrados • Precio oferta: 680 USD c/u + IVA
ML CONSULTORES	Cerradura electrónica smartair	• El elemento de identificación puede ser una tarjeta, un llavero, brazalete, etc. • Posibilidad de incorporarse en soportes

	 La tecnología de chip sin contacto RFID de 13,56 MHz Smartair ofrece: Mayor capacidad y protección de datos. Alta velocidad de transmisión. Seguridad: la información está encriptado. La ausencia de contacto entre el chip y el lector proporciona una mayor durabilidad y bajo coste de mantenimiento. La ausencia de contacto entre el chip y el lector proporciona una mayor durabilidad y bajo coste de mantenimiento. La distancia de lectura es de 10 mm con tarjetas estándar	con otras tecnologías: tarjetas de banda magnética, proximidad de 125 kHz, chip de contacto, etc. • Gran resistencia a la intemperie, golpes, agua, polvo, temperaturas extremas. • Se instala en todo tipo de puertas con cerraduras de embutir. • No necesita cableado y se alimenta mediante 3 pilas alcalinas situadas en la parte interior. • Construido de acero inoxidable • Precio oferta: 420 USD c/u + IVA • Garantía 2 años

CETA	**Kaba generación 760**  Ya se trate de un pequeño hotel boutique o una cadena de hoteles a gran escala, la E-760 está diseñado para satisfacer las necesidades exigentes y diversos de la industria hotelera. Solución ideal para hoteles localizados frente al mar. Actualmente instalados en más de un 4 millones de habitaciones de hotel en todo el mundo, la generación de E-760 es el más vendido. Fácil de usar, segura, la E-760 es fácil de manejar y fácilmente sustituye a los seguros de las puertas mecánicas o electrónicas. Opción de cerradura con tratamiento diferenciado en sus componentes, asegurando alta resistencia contra los efectos del salitre.	• Adecuado para pequeñas y hoteles de gran escala • Control de acceso para las habitaciones, áreas comunes. • Alta seguridad y el diseño a prueba de manipulaciones • Acceso de emergencia: tarjeta de acceso de emergencia, llave mecánica y anulación electrónica • Bajo mantenimiento • Baterías duran hasta 3 años • Indicador de batería baja • Bloqueo de la programación y la auditoría no se borran durante el cambio de la batería • Firmware actualizable • Precio oferta: 240 USD c/u + IVA • Garantía 2 Años • Toda la gama de repuestos distribuidores autorizados de la marca Kaba

CETA	**Kaba generación 790 RFID**  Cerradura de última generación, opera con tres pilas AA funciona por proximidad utilizando tarjetas o pulseras MIFARE, utiliza lo último en tecnología de control de acceso para proveer los huéspedes del hotel una experiencia de acceso sin contacto, no sólo permite a los hoteles proporcionan una clase de primera experiencia al huésped, sino que también reduce significativamente los gastos de funcionamiento. Las cerraduras de la Serie 790 son la opción perfecta para los hoteles que buscan llevar a sus operaciones y sistemas de seguridad al siguiente nivel.	• Adecuado para pequeños y hoteles de gran escala • Control de acceso para las habitaciones, áreas comunes, • Alta seguridad y el diseño a prueba de manipulaciones • Acceso de emergencia: tarjeta de acceso de emergencia • Bajo mantenimiento • Funciona con un lector sin contacto completamente sellado • Baterías duran hasta 3 años • Indicador de batería baja alerta al personal • Resistente y acabado • Firmware actualizable • Precio oferta: 310 USD c/u + IVA • Garantía 2 Años • Toda la gama de repuestos distribuidores autorizados de la marca Kaba

Tabla 6.15 Equipos de control de acceso

Elaborado por el investigador

De las empresas postulantes CETA presento la alternativa más viable de equipos de control de acceso para hoteles, además que los precios están en competencia directa con las otras compañías, con años de experiencia en el campo de instalación, mantenimiento, repuestos y además de contar con técnicos especializados directamente con la empresa productora de dichas cerraduras.

Conozcamos un poco más de CETA y sus principales clientes hoteleros:

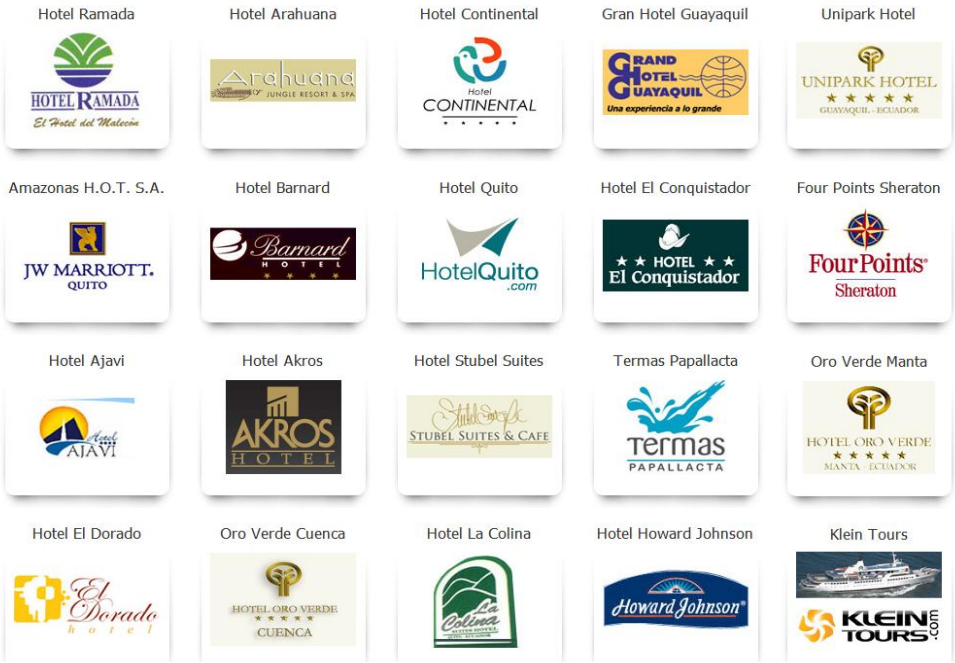


Fig. 6.32 Clientes hoteleros de control de accesos

Fuente: http://ceta.com.ec/clientes.html

En la fig. 6.32 se lista una parte de los potenciales clientes hoteleros de la empresa CETA, como podemos listar se encuentran los principales hoteles de la ciudad de Quito de alto prestigio, lo cual es el principal punto de partida para saber que se cuenta con el respaldo necesario para efectuar la compra del sistema de control de accesos, en puntos posteriores a este se presentara la propuesta económica, además de los equipos de programación del control de accesos y sus periféricos para auditar los ingresos y las principales características de los mismos.

Entre los equipos de control de acceso presentados por la empresa se listan dos el modelo que presenta mejores características de funcionamiento y comodidad de uso es el KABA 790 RFID el cual será el escogido para la implementación.

6.8.2.6 Elección del tipo de tecnología de las cámaras

Otra parte importante de la propuesta de control de accesos es las cámaras que ayudara a identificar visualmente a los infractores de la seguridad tomando en cuenta que cubrirán la mayor parte posible de zonas del hotel, para llevar un control estricto de seguridad, además de poder vigilar a que los empleados cumplan su labor acorde a su contrato y tampoco rompan las reglas de seguridad.

Una vez contabilizadas las zonas que necesitan tener video vigilancia que respalde el control de accesos, queda la elección del tipo de tecnología con la que se dotara de cámaras al hotel existen dos, de las cuales se estudiara las ventajas y desventajas para ver cuales se adaptan mejor a la situación del hotel.

Actualmente es muy común oír de Cámaras IP, cada vez se escucha hablar de esta tecnología y son muchas las dudas que surgen a la hora de decidir si es operativo seleccionar este tipo de cámaras para nuestros proyectos o no, incluso se escucha que las cámaras Análogas son una tecnología obsoleta, una tecnología que va a "desaparecer" según investigaciones esta es una afirmación bastante prematura. En la siguiente tabla se verá que las cámaras análogas nos ofrecen ciertas características que al día de hoy son inalcanzables por las cámaras IP.

Cámaras analógicas vs IP	
Hoy en día las cámaras IP pueden ofrecernos imágenes Mega Pixeles entregándonos Imágenes en Alta Definición, sin embargo las cámaras análogas continúan ofreciéndonos eficiencia, bajo costo y una alta seguridad y fiabilidad. La principal diferencia entre una cámara análoga y una IP es la forma en cómo se transmite el video y adicionalmente podríamos decir donde se comprime el video para su presentación.	
Cámaras analógicas	**Cámaras IP**
Las cámaras analógicas pueden contar con un sensor CCD que digitaliza la imagen y la procesa, pero antes de poder transmitir la imagen necesita volver a procesarla para que esta pueda	Una cámara IP se podría definir como una cámara que digitaliza y procesa imágenes análogas, las comprime internamente y luego transmite la información del video a través de una

ser recibida por un DVR, un Monitor, una Grabadora, o lo que sea. Las cámaras Análogas no integran Web Server, ni compresores, no requiere de ningún mantenimiento a parte del físico (limpieza de polvo, etc…).	conexión TCP/IP. Una Cámara IP como hemos visto anteriormente, puede montar dos tipos de Sensor, el CMOS y el CCD. Además dispone de funciones similares a las de las cámaras análogas.
CARACTERÍSTICAS	
Las cámaras Análogas operan perfectamente en diferentes condiciones de luz, transmiten el video tal cual sin compresión con lo cual las imágenes obtenidas son iguales a las captadas por la cámara sin pérdida de calidad debida a la compresión. Una cámara análoga no comprime la imagen, si no que esta función la hace el DVR, con lo cual dispone de un mejor hardware para hacer esta función incrementando tanto la calidad del video como la cantidad de frames por segundo a procesar.	Las cámaras IP nos pueden ofrecer una calidad de imagen Mega Pixel, cosa que no pueden hacer las análogas El video es comprimido antes de ser enviado al monitor, usted nunca vera la más alta calidad de las imágenes en tiempo real, ya que cuando el video le llega a usted, este ya fue Comprimido con la consiguiente pérdida de calidad. El acceso a la cámara se puede realizar mediante página web dentro de la red o con un acceso remoto debidamente configurado con los permisos necesarios.
VENTAJAS	
• Una cámara análoga puede ser conectada a cualquier DVR existente en el mercado, no existe ningún tipo de incompatibilidad de ningún tipo, salvo el sistema de video (NTSC/PAL). • Las cámaras Análogas son significativamente mucho más económicas. • No requieren de ningún otro	• Algunas Cámaras IP, tienen la capacidad de almacenar video directamente en un dispositivo de almacenamiento removible. • Una gran ventaja de las cámaras IP reside en el cableado, donde no es necesario tirar un cable desde la cámara hasta el DVR, ya que estas cámaras se conectan directamente a la Red alámbrica o inalámbrica de

periférico adicional además de la energía para transmitir video. • Las fallas que se presentan en las cámaras análogas son limitadas a esa cámara en particular, estando cada cámara aislada una de otra.	la empresa y el software en el NVR es el encargado de hacer la conexión "lógica" con la cámara. • Existe la posibilidad si la cámara lo permite de transmitir la energía por el propio cable de Red PoE.
DESVENTAJAS	
• Algunos equipos están limitados al acceso remoto para la revisión del contenido. • Las cámaras análogas son más fáciles de interceptar y ver las imágenes en caso de que se tuviera acceso al sistema de cableado. • Para hacer una cámara análoga inalámbrica debemos de recurrir a sistema de Radiofrecuencia los cuales suelen ser caros, además de que tenemos la limitante de los canales soportados por el dispositivo. • La calidad de video puede diferir por interferencias o distancia del cableado.	• Las cámaras IP tienen problemas en condiciones con baja luminosidad. • Las cámaras IP tienen los recursos limitados para hacer la compresión del video, como resultado de esto la calidad del video entregado puede diferir de la calidad que obtendríamos con una cámara análoga. • Una cámara IP puede llegar a ser hasta 3x veces más cara que una cámara análoga de las mismas características. • La instalación de cámaras IP requiere que el personal que la realiza tenga amplios conocimientos en Redes, equipos de Ruteo, etc.

Tabla 6.16 Cámaras analógicas vs cámaras IP

Elaborado por el investigador

Como conclusión podemos ver que las cámaras IP se adaptan mejor a una red ya existente y necesita de más planificación en cuanto a programación y grabación, las cámaras analogías ofrecen grandes ventajas a un bajo costo y con la integración de un DVR que fue estudiado anteriormente se digitaliza la imagen y

se la puede ver a través de redes TCP/IP, para tener las prestaciones de las cámaras IP, con esas opciones se optara por este tipo de tecnología.

6.8.2.7 Asignación de equipos para el sistema de video vigilancia

A diferencia de los equipos de control de acceso, las cámaras analógicas y DVR se encuentran fácilmente en el mercado nacional al ser un producto de uso masivo por parte de empresas grandes, medianas y pequeña, su bajo costo ayuda a tomar decisiones más fáciles en cuanto a la compra de equipos.

Para la elección de equipos se realizara una tabla de comparación de cámaras ofrecidas por empresas recomendadas dentro del país.

EMPRESA	EQUIPO	CARACTERÍSTICAS
IMPOMAX	**CÁMARA TUBO HAWELL**  Cámara ideal para exteriores con una cubierta que protege al equipo electrónico de todo tipo de condiciones climáticas. Además cuanta con un IR para trabajar en la obscuridad y un Rango efectivo sobre los 25-30 metros, además de ser compatible con cualquier tipo de DVR, cuenta con una resolución de 420 TVL.	• Sensor de imagen 1/4" Sharp ccd a color • Numero de pixeles 510 (h) x 492 (v) • Iluminación mínima 0.4 lux / F 2.0, 0 lux (ir on) • Ir led 24 unidades • Disparador electrónico 1/60(1/50) to 1/100,000(s) • Lente 3.6 mm / F 1.5 • Angulo del lente 70° • Modo iris aes • Control de ganancia auto • Consumo de corriente (±10%) 500ma • Poder de consumo (±10%) dc12v • Salida de video BNC 75Ω • Precio 75$ + IVA • Garantía 2 años

IMPOMAX	**CÁMARA TIPO DOMO HAWELL**  Cámara ideal para interiores con una cubierta que protege al equipo electrónico. Además cuanta con un IR para trabajar en la obscuridad y un Rango efectivo sobre los 10-15 metros, además de ser compatible con cualquier tipo de DVR, cuenta con una resolución de 420 TVL.	• Sensor de imagen 1/4" Sharp ccd a color • Numero de pixeles 510 (h) x 492 (v) • Iluminación mínima 0.4 lux / F 2.0, 0 lux (ir on) • Ir led 16 unidades • Disparador electrónico 1/60(1/50) to 1/100,000(s) • Lente 3.6 mm / F 1.5 • Angulo del lente 70° • Modo iris aes • Control de ganancia auto • Consumo de corriente (±10%) 500ma • Consumo (±10%) dc12v • Salida de video BNC 75Ω • Precio 50$ + IVA 2 años
SISTEMAS DE SEGURIDAD	**CÁMARA TUBO STV ST-T141**  Cámara ideal para exteriores con una cubierta que protege al equipo electrónico de todo tipo de condiciones climáticas. Además cuanta con un IR para trabajar en la obscuridad y un	• Sensor de imagen 1/4" Sony ccd a color • Numero de pixeles 510 (h) x 492 (v) • Iluminación mínima 0.4 lux / F 2.0, 0 lux (ir on) • Ir led 48 unidades • Disparador electrónico 1/60 to 1/100,000(s) • Lente 6 mm / F 2 • Angulo del lente 80° • Control de ganancia auto

	Rango efectivo sobre los 35-40 metros, además de ser compatible con cualquier tipo de DVR, cuenta con una resolución de 420 TVL.	• Consumo de corriente (±10%) 500ma • Poder de consumo (±10%) dc12v • Salida de video BNC 75Ω • Precio 88$ + IVA 2 años
SISTEMAS DE SEGURIDAD	**CÁMARA TIPO DOMO STV ST-DP110**  Cámara ideal para interiores con una cubierta que protege al equipo electrónico. Además cuanta con un IR para trabajar en la obscuridad y un Rango efectivo sobre los 10-15 metros, además de ser compatible con cualquier tipo de DVR, cuenta con una resolución de 420 TVL.	• Sensor de imagen 1/4" Sharp ccd a color • Numero de pixeles 510 (h) x 492 (v) • Iluminación mínima 0.4 lux / F 2.0, 0 lux (ir on) • Ir led 24 unidades • Disparador electrónico 1/60(1/50) to 1/100,000(s) • Lente 6 mm / F 2.0 • Angulo del lente 70° • Control de ganancia auto • Consumo de corriente (±10%) 120 mA • Poder de consumo (±10%) dc12v • Salida de video BNC 75Ω • Precio 55$ + IVA 2 años

Tabla 6.17 Propuesta cámaras analógicas

Elaborado por el investigador

En la tabla 6.15 se indica las principales cámaras de seguridad que se consideran para el diseño de video vigilancia, varias empresas enviaron proformas, se tomó en cuenta las más representativas ya que las otras presentaban los mismos productos con mayor precio, como se puede observar las cámaras cuentan con las mismas características la empresa IMPOMAX ofrece una mejor oferta económica por lo que es la elegida para la compra de estos equipos.

Para la visualización y grabación de las cámaras de seguridad se plantean dos métodos, a través de DVR en la tabla 6.16 se presentan alternativas con sus respectivas características que fueron presentadas por las mismas empresas de la tabla anterior los cuales son expuestos y analizados.

EMPRESA	EQUIPO	CARACTERÍSTICAS
IMPOMAX	**TARJETA DVR 16CH 120FPS**  La tarjeta DVR permite a los usuarios de cámaras analógicas, instalar este sistema en un PC con los recursos necesarios para poder realizar el monitoreo y grabación de las cámaras, trabaja en modo pasivo y es compatible con la mayor parte de sistemas operativos, tiene un costo económico con ranura PCI, y cables de adaptación para la conexión de cámaras.	• Número de cámaras/canales 16 • Número de frames por segundo (fps) 120 • Acceso remoto a través de internet • Grabación de video por programación • Sensor de movimiento configurable • Software incluido • 4 entradas de audio: 4 • 1 salida a TV • 6805 chipset, 10 Bits con calidad de imagen. • Bajo consumo de energía, en calor. • Baja tasa de ocupación de los recursos de CPU • Vista remota a través de teléfonos móviles • Formato de archivo de video AVI. • Precio 250 USD +IVA • 1 año de garantía

IMPOMAX	**GRABADOR DIGITAL AVTECH AVC798PV**  16CH H.264 CIF 480IPS DVD-RW El DVR AVTECH de grabación digital es lo último en tecnología para cámaras analogías, incorpora características que permiten la mejor experiencia para la grabación dedicada en hardware de video, además de permitir el acceso remoto mediante página web y compatible con la mayoría de dispositivos móviles, adaptable a todo tipo de empresas gracias a sus grandes prestaciones.	• 16 ch de video / 16 ch loops / 4 ch de audio • Compresión de grabación y transmisión: H.264 • Velocidad de Visualización y grabación en vivo: 480 ips en tiempo real • Reproduce hasta 16 cámaras al mismo tiempo • PENTAPLEX: Graba, visualiza, reproduce, transmite y back-up • Capacidad de 2 disco duro SATA de hasta 2TB c/u • Salida de video: BNC (analógica), VGA y Call Monitor BNC. • Transmisión por red LAN, WAN e internet (TCP/IP) • Posibilidad de verse a través de un Celular via GPRS 3G • Salidas: RS485 (PTZ) y conexión de alarmas • Back-up vía: DVD-RW, USB y RED • Incluye software de visualización remoto de hasta 16 cámaras simultáneamente • Precio 750 USD + IVA • 2 años de garantía

SISTEMAS DE SEGURIDAD	**TARJETA PCI DVR I-VIEW CP-5416ASE-XP0**  Tarjeta de video de 16 ch y transmisión por internet mpeg4/h.264 (120fps). Esta tarjeta cumple con estándares de video de alta compresión lo cual permite una mejor experiencia tanto en grabación como por acceso remoto, se instala en cualquier tipo de computador adecuado para la grabación permanente de video. Además de tener un sistema pasivo de trabajo mientras graba permite el acceso a las prestaciones del computador.	• Visualización y grabación de 16 ch a 120 fps • Visualización multipantalla: 1, 4, 6, 8, 9, 10, 13 y 16 • Compresión: Wavelet, M-JPEG y MPEG-4, • Modos de grabación: continua, alarma, detección de movimiento, horarios • Almacenamiento: graba automáticamente nuevos videos sobre los más antiguos • Backup: HDD, CD-RW, DVR-RW, etc • Función de PRE-alarma • Perdida de video notificado automáticamente • Notificación de alarmas vía teléfono, email o imagen en vivo • Password de protección con múltiples niveles desde administrador a usuario • Solución IP dinámico no requiere IP fijos. • Acceso vía página WEB IE, desde cualquier parte del mundo • Precio 590 USD +IVA • 1 año de garantía

SISTEMAS DE SEGURIDAD	**GRABADOR DIGITAL STV ST-7216HVI-ST/SN**   GRABADOR DIGITAL X 16CH H.264 CIF 120IPS El DVR AVTECH de grabación digital es lo último en tecnología para cámaras analogías, incorpora características que permiten la mejor experiencia para la grabación dedicada en hardware de video, además de permitir el acceso remoto mediante página web y compatible con la mayoría de dispositivos móviles, adaptable a todo tipo de empresas gracias a sus grandes prestaciones.	• 16ch de video / 1ch de audio • Compresión de grabación y transmisión: H.264 • 2 stream de video independientes para grabar y transmitir a diferente velocidad y resolución • Velocidad de Visualización en vivo: 120ips (tiempo real) • Velocidad de Grabación: 480ips (tiempo real) • Graba, visualiza, reproduce, transmite y back-up • Capacidad de 1 disco duro SATA de hasta 2TB • Salida de video: BNC (analógica), VGA. • Transmisión por red LAN, WAN e internet TCP/IP • Posibilidad de verse a través de un Celular via GPRS 3G • Dual Stream • Salidas: RS485 (PTZ) • Back-up vía: USB y RED • Incluye software de visualización remoto de hasta 64 cámaras • Precio 550 USD + IVA • 1 año de garantía

Tabla 6.18 Equipos de grabación digital de cámaras analógicas

Elaborado por el investigador

En la tabla 6.16 se presentan opciones de equipos propuestos por estas dos diferentes empresas, se seleccionaron los que pueden satisfacer las necesidades mínimas para el sistema de video vigilancia, entre los puntos que se tomaran en cuenta para la elección se encuentran:

- Largos periodos de grabación
- Acceso remoto en la red interna
- Acceso remoto mediante internet
- Configuración de grabación mediante movimiento
- Calidad de compresión a la hora de la grabación
- Interface de uso agradable
- Costo beneficio
- Capacidad de grabación
- Visualización simultanea de cámaras

Después de analizar los equipos presentados podemos tomar la conclusión de que el indicado para el sistema de video vigilancia es el DVR AVTECH siendo el que más prestaciones ofrece al momento de interactuar con el dispositivo, además de que es compatible con la mayor parte de dispositivos móviles lo cual creara un entorno de revisión agradable por parte de los propietarios así como de la persona encargada del monitoreo, se descartó la posibilidad de incorporar tarjetas de grabación a un computador debido a que dependen más del hardware del PC para cumplir con sus características principales lo cual repercute en el costo beneficio porque primero de debe adecuar un PC que soporte todo el tiempo prendido en este caso un servidor, el cual sería muy costoso y requiere más mantenimiento, no así el hardware dedicado de video para la grabación y reproducción de cámaras.

En la fig. 6.34 se presenta el sistema que se usara en el Hotel Destiny.

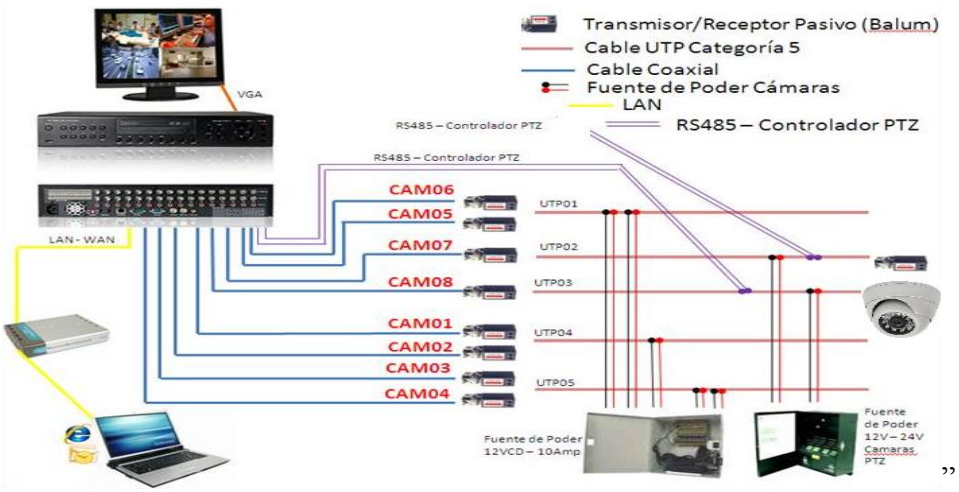


Fig. 6.33 Esquema de conexión de sistema de video vigilancia CCTV

Elaborado por el investigador

6.8.3 Diseño e implementación

Una vez definidos los equipos y el tipo de infraestructura que ocupa cada uno, queda establecer la ubicación exacta de cada uno de ellos, además de la configuración y prueba de funcionamiento y su zona de cobertura, a continuación se describe los planos y la ubicación de equipos de control de acceso y video vigilancia para cumplir los objetivos planteados de la propuesta la ubicación se planteara por zonas y tomando en cuenta la tabla 6.8 realizada con el objetivo de identificar las zonas y sus requerimientos.

Para el diseño de la video vigilancia se usa la característica principal de las cámaras las cuales son el ángulo de visión que se considera en 70 grados y la distancia efectiva de 10 metros, a partir de ahí la ubicación de cada cámara se realiza con las respectiva identificación numérica que se describirá después de cada plano.

Para el control de acceso se toma en cuenta la tabla 6.6 en donde se indica las zonas que necesitan el control, cabe recalcar que se usara la cerradura Kaba 790 que trabaja de forma autónoma y sin conexión de igual forma cuenta con su numeración por cada piso para la configuración e identificación.

Para el diseño se considera la siguiente simbología para la fácil identificación de equipos tanto de control de accesos como de video vigilancia.

Simbología AutoCAD:

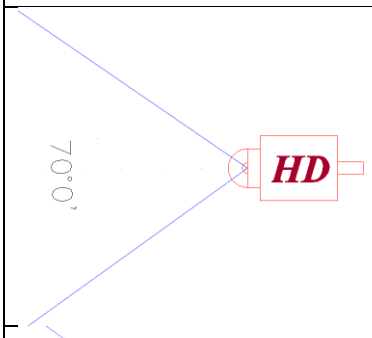
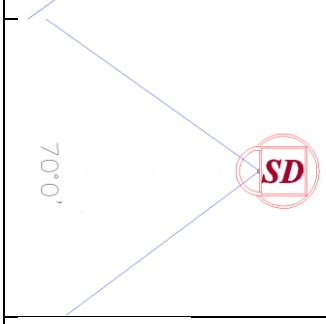
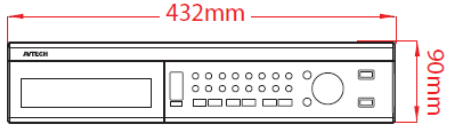
Símbolo	Descripción
	Cámara HAWELL de alta definición tipo tubo con ángulo de visión de 70 grados y distancia efectiva de 10 metros
	Cámara HAWELL de definición estándar tipo domo con ángulo de visión de 70 grados y distancia efectiva de 10 metros
	Cerradura Autónoma Hotelera Kaba 790 con lectora de proximidad RFID para dormitorios y áreas restringidas
	Lector de proximidad RFID Kaba exos para ascensor
	DVR Avtech de 16 canales para grabación y visualización de cámaras
	Computadora compacta Kaba con sistema Atlas para programación de tarjetas y cerraduras

Tabla 6.19 Simbología de equipos

Elaborado por el investigador

6.8.3.1 Diseño de planos y distribución de equipos

Para la propuesta de diseño se realiza la presentación de planos con la distribución y numeración de equipos que se realizó en conjunto con el representante del hotel:

- **ESTACIONAMIENTO**

Numero de dispositivo	**Descripción**
Cámara HD 0.1	Cubre la zona de entrada principal del estacionamiento
Cámara SD 0.2	Cubre la zona de entrada, circulación y el parqueadero
Cámara SD 0.3	Cubre la zona de entrada, circulación y el parqueadero
Cámara SD 0.4	Cubre la zona del cuarto de máquinas y parqueadero
Cámara SD 0.5	Cubre la zona de ingreso al ascensor y parqueadero
Control de acceso 0.1 A	Control de acceso al ascensor

Tabla 6.20 Distribución de equipos estacionamiento

Elaborado por el investigador

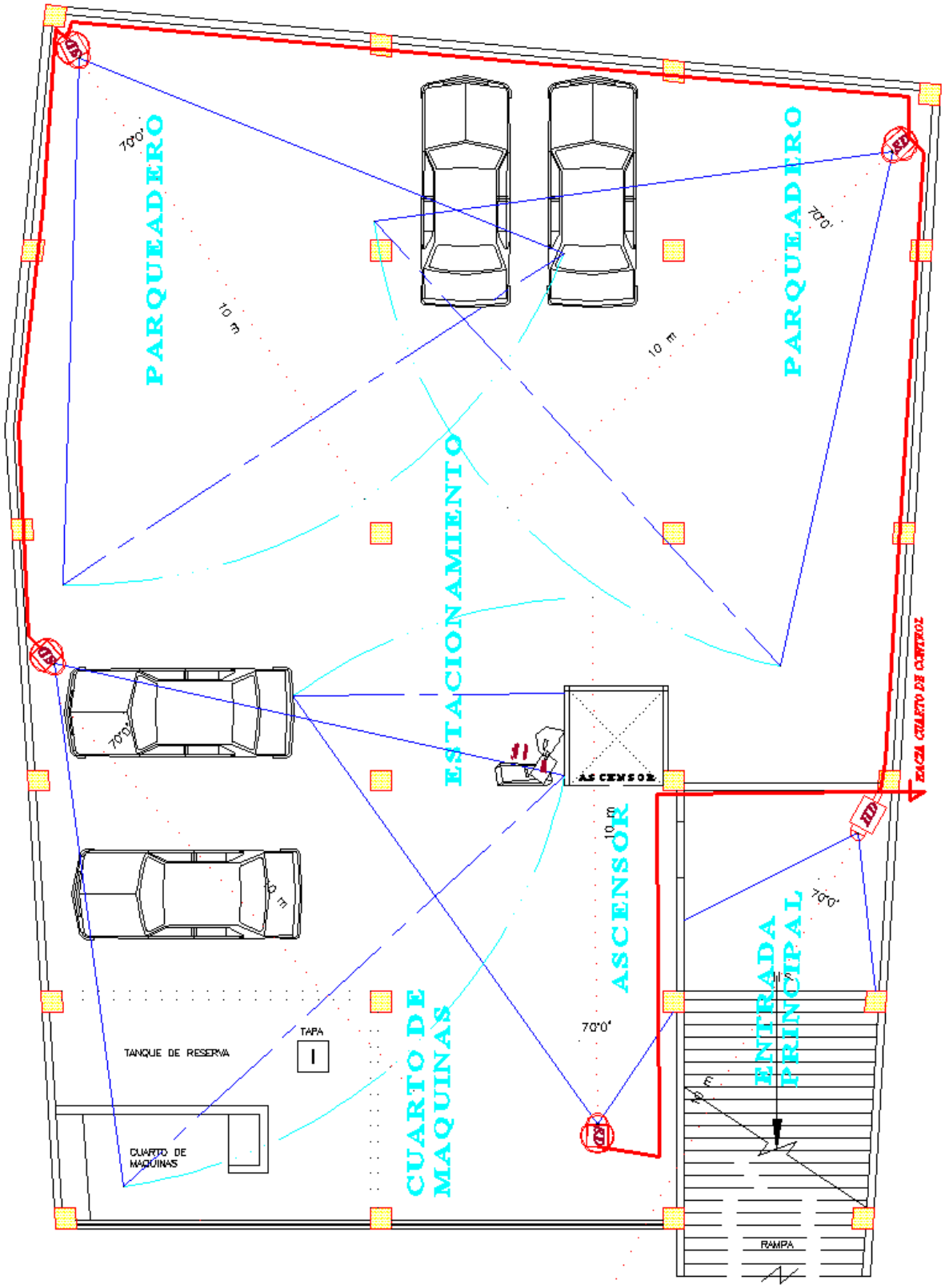


Fig. 6.34 Propuesta estacionamiento

Elaborado por el investigador

- **PLANTA BAJA**

Numero de dispositivo	Descripción
Cámara HD 1.1	Cubre la zona de entrada principal al hotel y la recepción
Cámara SD 1.2	Cubre la zona de entrada, circulación externa
Cámara SD 1.3	Cubre la zona del restaurante e ingreso de escaleras al bar
Cámara SD 1.4	Cubre la zona de la administración e ingreso al cuarto de equipos
Cámara SD 1.5	Cubre la zona del pasillo, ingreso cocina, habitaciones, administración
Cámara SD 1.6	Cubre la zona de la cocina
Control de acceso 1.0 A	Control de acceso al ascensor
Control de acceso 1.1 H	Control de acceso habitación 01
Control de acceso 1.2 H	Control de acceso habitación 02
Control de acceso 1.3 E	Control de acceso cuarto de equipos
Control de acceso 1.4 B	Control de acceso bodega restaurante

Tabla 6.21 Distribución de equipos planta baja

Elaborado por el investigador

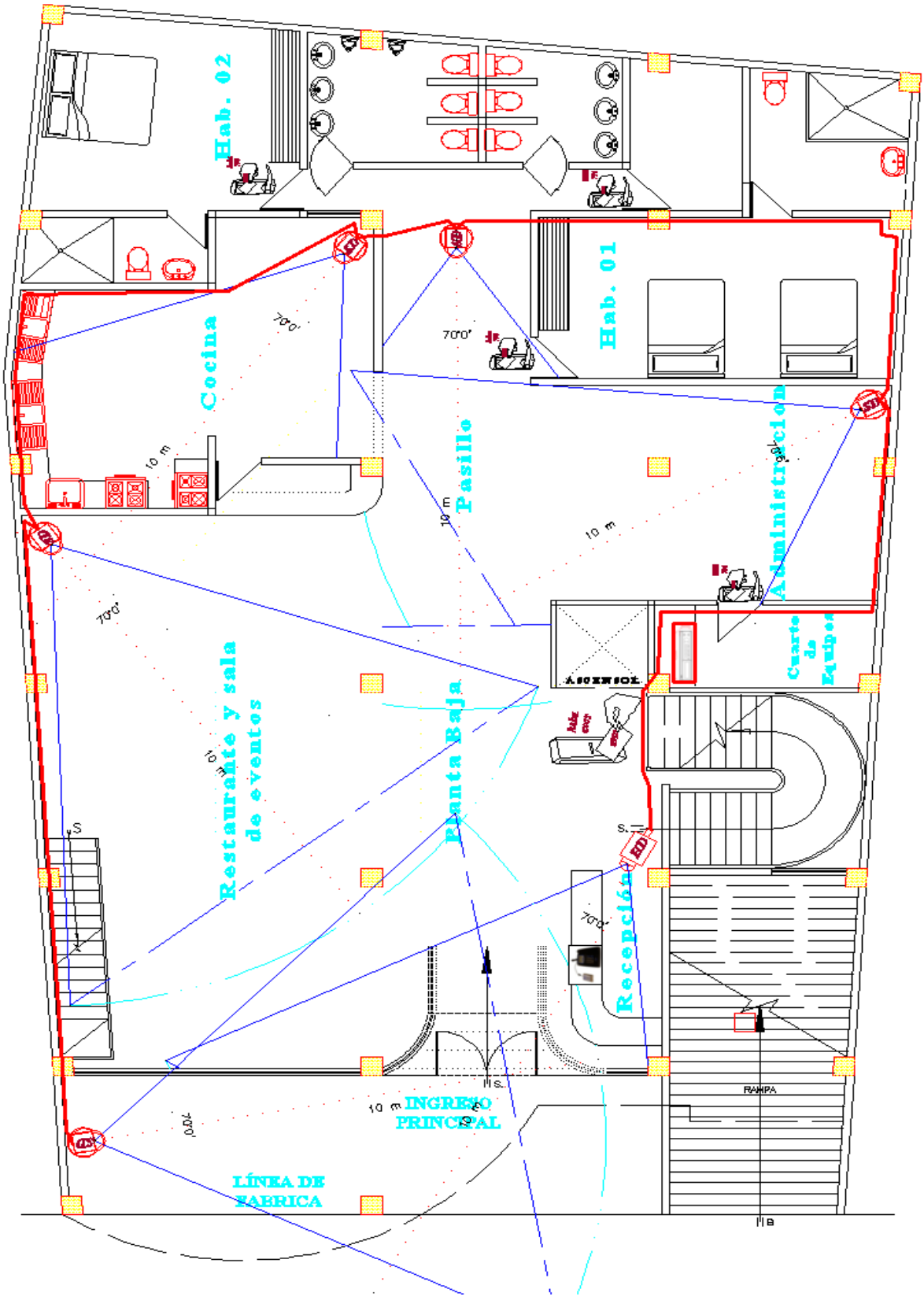


Fig. 6.35 Propuesta planta baja

Elaborado por el investigador

- **PRIMERA PLANTA**

Numero de dispositivo	Descripción
Cámara HD 2.1	Cubre la zona del bar, barra de pagos
Cámara SD 2.2	Cubre la zona del bar
Cámara SD 2.3	Cubre la zona de ingreso al piso, ascensor y habitación
Cámara SD 2.4	Cubre la bodega de Licores
Cámara SD 2.5	Cubre la bodega de Pertenencias
Cámara SD 2.6	Cubre la zona del pasillo ,entrada a habitaciones y bodegas
Control de acceso 2.0 A	Control de acceso al ascensor
Control de acceso 2.1 H	Control de acceso habitación 03
Control de acceso 2.2 H	Control de acceso habitación 04
Control de acceso 2.3 H	Control de acceso habitación 05
Control de acceso 2.4 H	Control de acceso habitación 06
Control de acceso 2.5 H	Control de acceso habitación 07
Control de acceso 2.6 H	Control de acceso habitación 08
Control de acceso 2.7 H	Control de acceso habitación 09
Control de acceso 2.1 B	Control de acceso bodega de licores
Control de acceso 2.2 B	Control de acceso bodega de pertenencias

Tabla 6.22 Distribución de equipos primera planta

Elaborado por el investigador

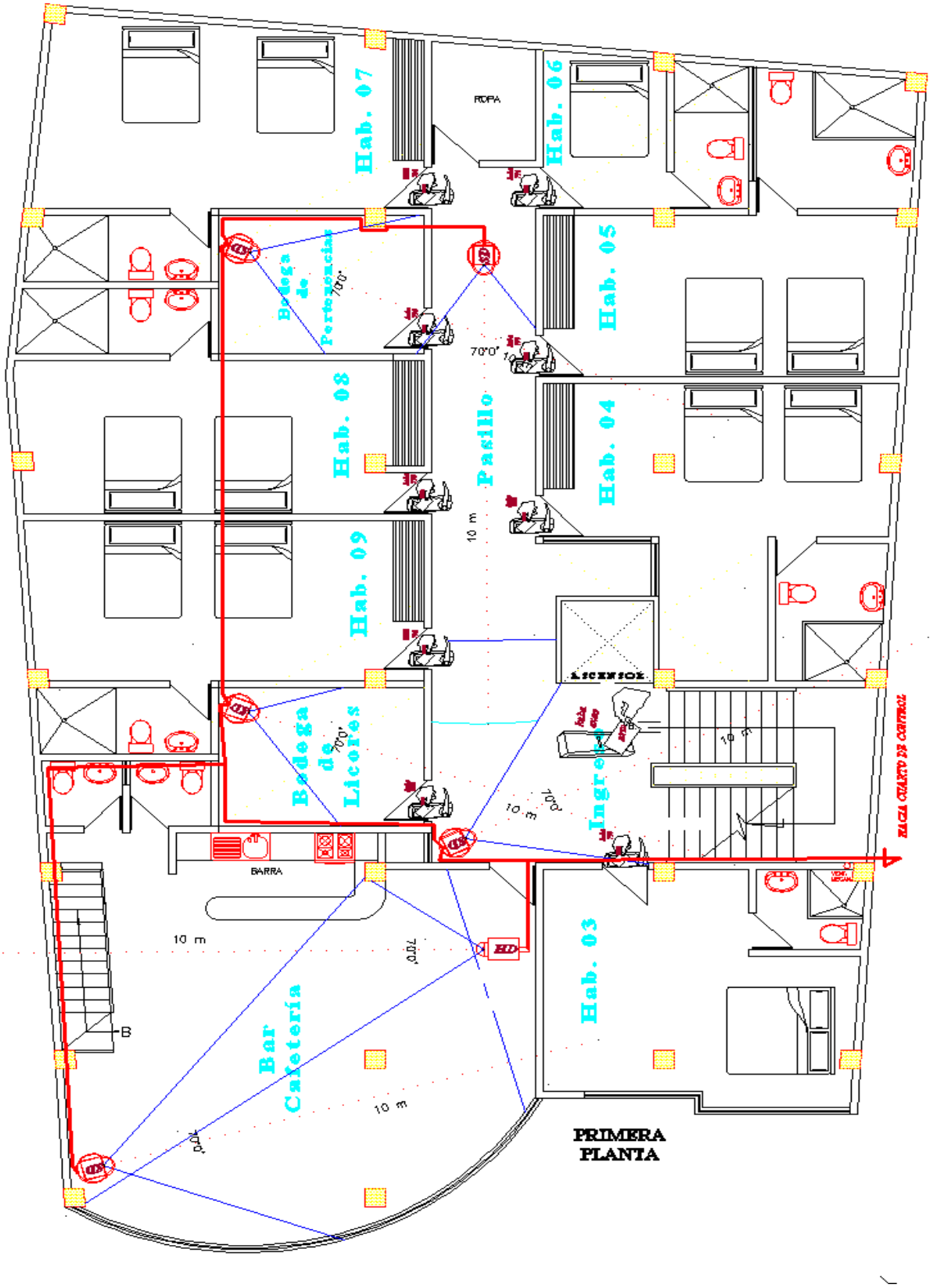


Fig. 6.36 Propuesta primera planta

Elaborado por el investigador

- **SEGUNDA PLANTA**

Numero de dispositivo	Descripción
Cámara SD 3.1	Cubre la zona de ingreso al piso, ascensor y habitación
Cámara SD 3.2	Cubre el cuarto de Computación
Cámara SD 3.3	Cubre la cuarto de Juegos
Cámara SD 3.4	Cubre la zona del pasillo ,entrada a habitaciones y bodegas
Cámara SD 2.5	Cubre el cuarto de Recreación
Control de acceso 3.0 A	Control de acceso al ascensor
Control de acceso 3.1 H	Control de acceso habitación 10
Control de acceso 3.2 H	Control de acceso habitación 11
Control de acceso 3.3 H	Control de acceso habitación 12
Control de acceso 3.4 H	Control de acceso habitación 13
Control de acceso 3.5 H	Control de acceso habitación 14
Control de acceso 3.6 H	Control de acceso habitación 15
Control de acceso 3.1 S	Control de acceso Suite 01
Control de acceso 3.1 B	Control de acceso cuarto de Computación
Control de acceso 3.2 B	Control de acceso cuarto de Juegos
Control de acceso 3.3 B	Control de acceso cuarto de Recreación

Tabla 6.23 Distribución de equipos segunda planta

Elaborado por el investigador

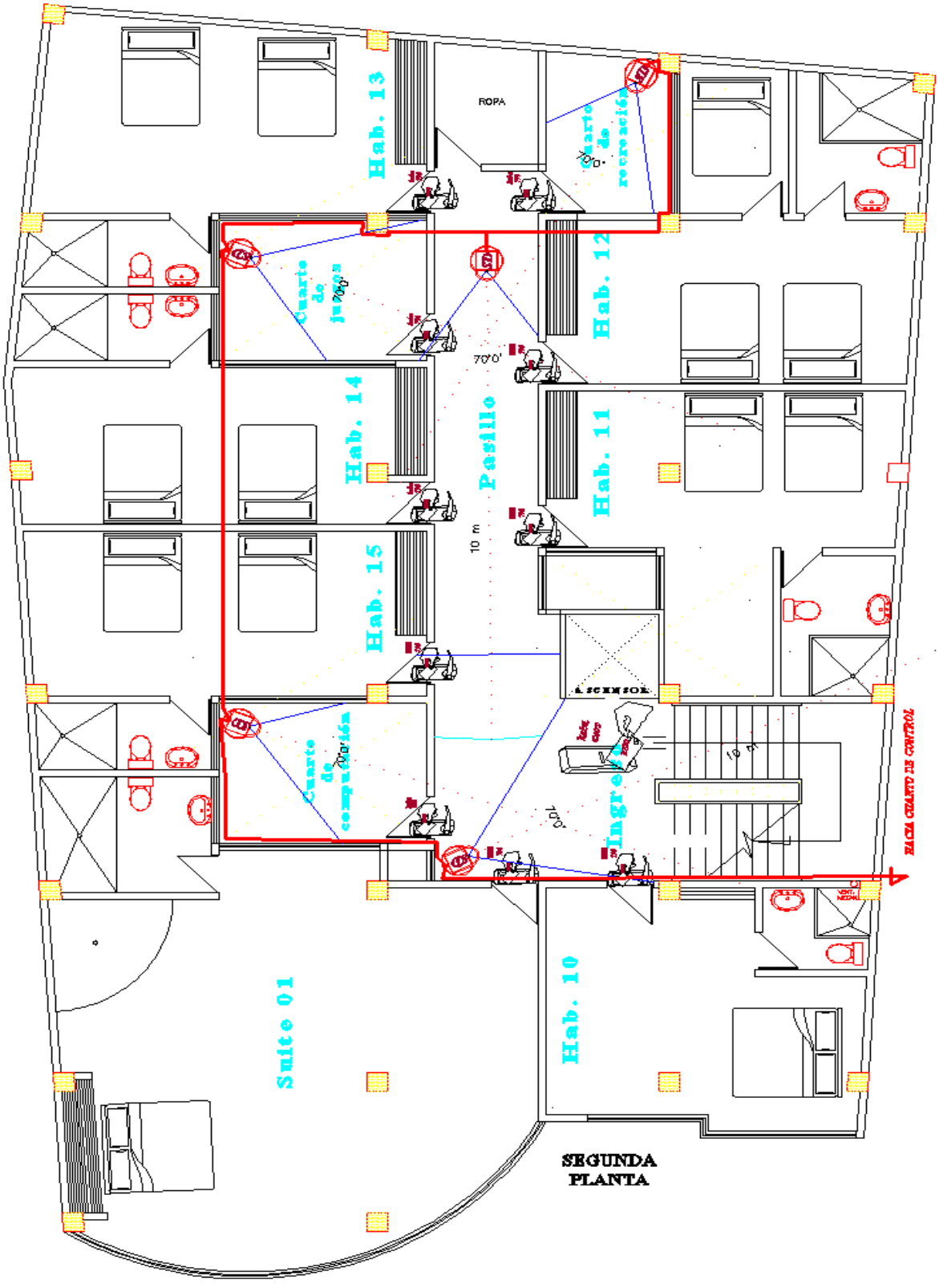


Fig. 6.37 Propuesta segunda planta

Elaborado por el investigador

- **TERCERA PLANTA**

Numero de dispositivo	Descripción
Cámara SD 4.1	Cubre la zona de ingreso al piso, ascensor y habitación
Cámara SD 4.2	Cubre la zona del pasillo ,entrada a habitaciones
Control de acceso 4.0 A	Control de acceso al ascensor
Control de acceso 4.1 H	Control de acceso habitación 16
Control de acceso 4.2 H	Control de acceso habitación 17
Control de acceso 4.3 H	Control de acceso habitación 18
Control de acceso 4.4 H	Control de acceso habitación 19
Control de acceso 4.5 H	Control de acceso habitación 20
Control de acceso 4.6 H	Control de acceso habitación 21
Control de acceso 4.1 S	Control de acceso Suite 02

Tabla 6.24 Distribución de equipos tercera planta

Elaborado por el investigador

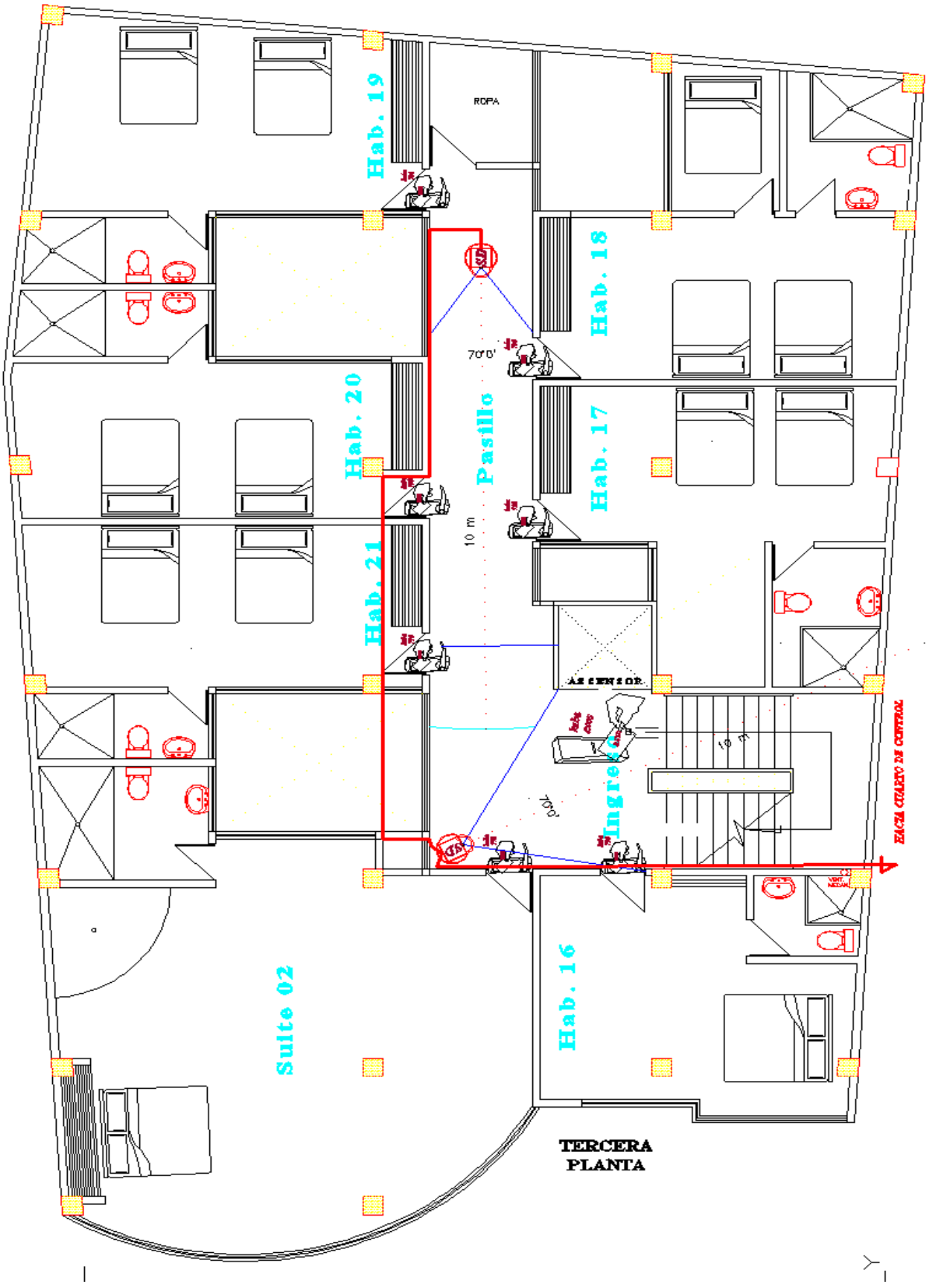


Fig. 6.38 Propuesta tercera planta

Elaborado por el investigador

- **CUARTA PLANTA**

Numero de dispositivo	Descripción
Cámara SD 5.1	Cubre la zona de ingreso al piso, ascensor y habitación
Cámara SD 5.2	Cubre la zona del pasillo ,entrada a habitaciones
Control de acceso 5.0 A	Control de acceso al ascensor
Control de acceso 5.1 H	Control de acceso habitación 22
Control de acceso 5.2 H	Control de acceso habitación 23
Control de acceso 5.3 H	Control de acceso habitación 24
Control de acceso 5.4 H	Control de acceso habitación 25
Control de acceso 5.5 H	Control de acceso habitación 26
Control de acceso 5.6 H	Control de acceso habitación 27
Control de acceso 5.1 S	Control de acceso Suite 03

Tabla 6.25 Distribución de equipos cuarta planta

Elaborado por el investigador

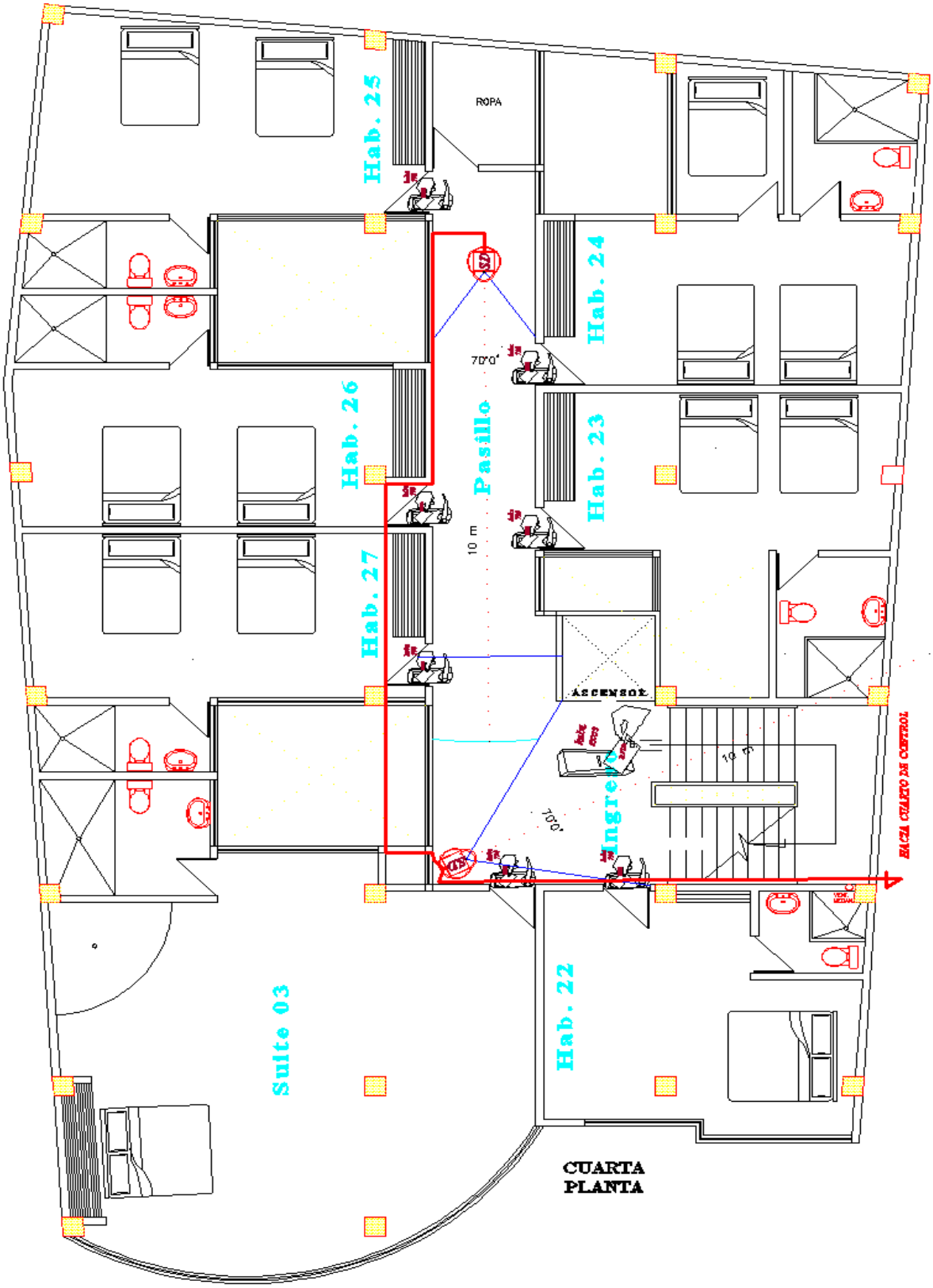


Fig. 6.39 Propuesta cuarta planta

Elaborado por el investigador

- **TERRAZA**

Numero de dispositivo	Descripción
Cámara SD 6.1	Cubre la zona de ingreso cuarto de descanso, pasillo de circulación y ingreso al turco
Cámara SD 6.2	Cubre el cuarto del sistema solar
Cámara SD 6.3	Cubre la lavandería
Control de acceso 6.1 H	Control de acceso Cuarto de descanso

Tabla 6.26 Distribución de equipos terraza

Elaborado por el investigador

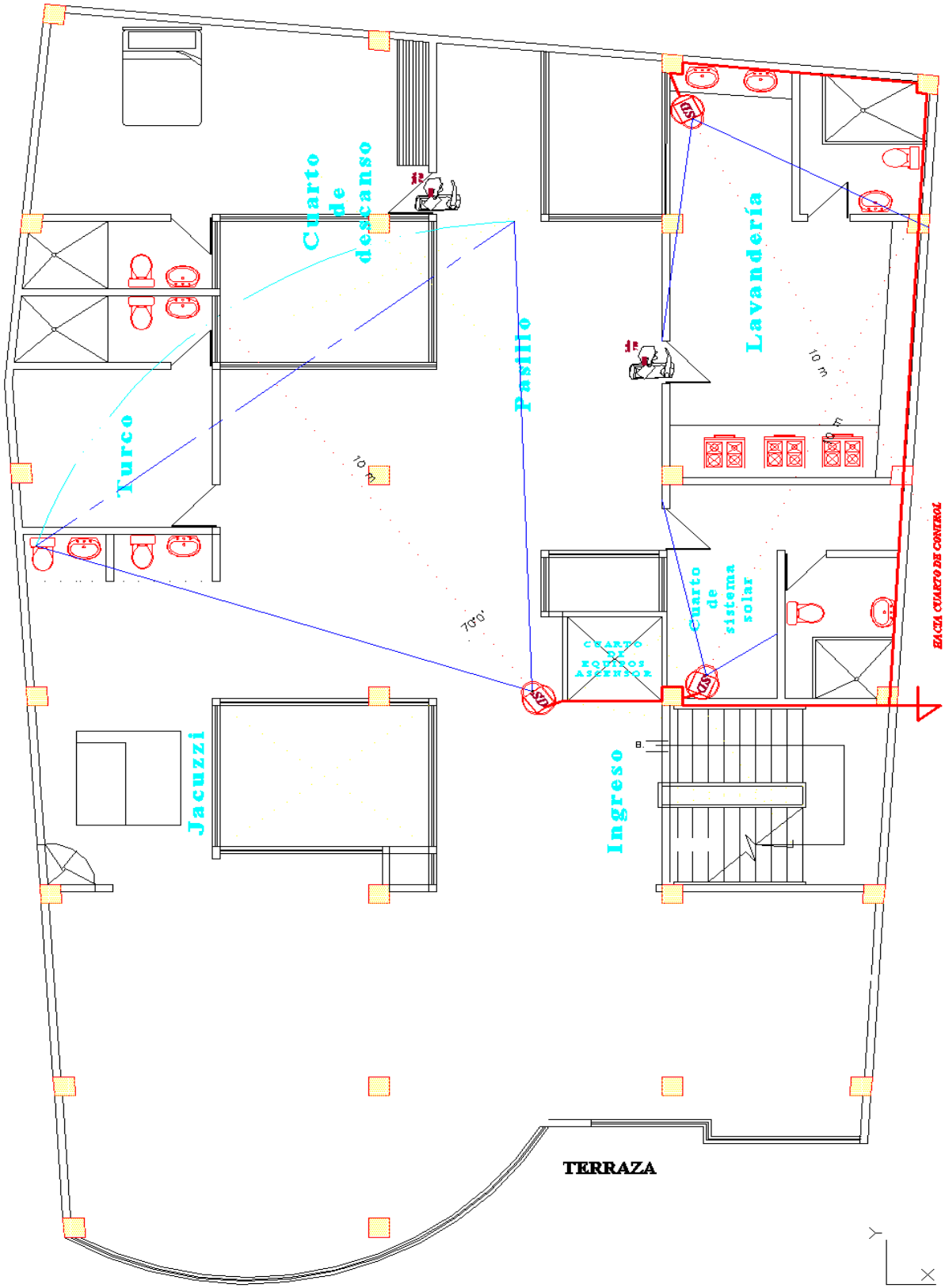


Fig. 6.40 Propuesta terraza

Elaborado por el investigador

Una vez lista la distribución de equipos se realiza un resumen para la configuración de dispositivos la cual se lo realiza independientemente por cada uno tanto de control de acceso como de video vigilancia fig. 40.

Fig. 6.41 Control de accesos y cctv

Elaborado por el investigador

6.8.3.2 Presentación de equipos del control de acceso

Una vez listo el diseño del control de acceso en el Hotel Destiny y la compra de los mismos, lo cual tiene 3 meses de demora por la importación de todos los equipos, queda la puesta en marcha tanto del funcionamiento como de la instalación que se realiza en cooperación de la empresa CETA.

Antes de continuar con la configuración se realiza un análisis en detalle de todos los dispositivos que conforman el control de accesos.

Soluciones de Control de Acceso para Hoteles

- **Cerradura Kaba generación E790 RFID**

Fig. 6.42 Cerradura electrónica de proximidad 790

Fuente: http://ceta.com.ec/serraduras.html

Diseñada para cubrir tanto las necesidades de los huéspedes como las delos hoteleros, la cerradura 790 cumplirá plenamente con tus expectativas de seguridad, sin importar la organización o la estructura física del hotel.

Para entrar, los huéspedes solo necesitan colocar su tarjeta frente a la cerradura. Aunado a esto, usando la tecnología de sellos y tarjetas de proximidad, es posible rastrear los movimientos de los empleados auditando sus tarjetas; de igual forma el personal de seguridad solo necesitará una tarjeta de auditoría para extraer los registros de una cerradura, con la gran ventaja de que las tarjetas no se desmagnetizan.

Todas las piezas electrónicas y las baterías están en la parte frontal de la cerradura, por lo cual no será necesario molestar a los huéspedes para hacer el mantenimiento. Las actualizaciones del software se hacen en sitio, eliminando los retrasos.

Seguridad Total y Confort	Ingeniería de Calidad	Compatibilidad y Certificación
• Lector diseñado ergonómicamente. Los huéspedes solo tienen que colocar la tarjeta frente a la cerradura • Apoyo auditivo y visual para el usuario. Los LEDs están colocados en el lector • Cancelación automática de la tarjeta de un huésped anterior para brindar seguridad y privacidad • Tecnología de lectura y escritura – las tarjetas del personal llevan consigo la información • Las cerraduras se pueden auditar utilizando la Tarjeta de Auditoria	• Completamente metálica, mortise y mecanismos de alta resistencia • Cerrojo de una pulgada para dar mayor protección y privacidad (disponible en automático) • Vínculo de comunicación infrarrojo (IR) para programación y auditorías • Sistema de drenado interno diseñado para prevenir la acumulación de condensación interna • Utiliza credenciales Mini MIFARE, así como tarjetas para los huéspedes de gran costo-beneficio	• Disponible en versiones compatibles con el Sabbat • Manijas ADA • Cumple con las normas UL 10C y ULC S-104, en puertas resistentes al fuego hasta por tres horas • Certificación ANSI/BHMA A156.13 para cerraduras con mortise Grado 1 y A156.13 para cerraduras electrificadas • Piezas electrónicas conforme a la norma FCC Parte 15 Clase A y la directiva CE 89/336/ECC • Compatible con RoHS
Mantenimiento sin preocuparse	**Sencillez**	**Seguridad para cada puerta**
• Funciona con tres baterías AA colocadas en frente de la cerradura (sin utilizar paquetes). Las baterías se pueden cambiar sin molestar a los huéspedes y sin tener que reprogramar las cerraduras • La vida de las baterías es suficiente hasta por 120,000 aperturas (de 2 a 3 años)	• Interfaz lista para usarse con un PMS • Se utiliza con un FDU o con ATLAS • Combinación de soluciones: Cerraduras electrónicas de proximidad y de banda magnética juntas • Variedad de tarjetas, brazaletes y sellos	• Diferentes opciones: mortise (Americana y Europea), pestillo cilíndrico, dispositivo de salida y RAC • Cilindro de emergencia • La cerradura se puede integrar a un sistema de llave maestra

Fig. 6.43 Detalles cerradura Kaba 790

Fuente: http://ceta.com.ec/serraduras.html

- **Controlador Remoto de Acceso Exos**

Fig. 6.44 Exos lectora de proximidad autónoma

Fuente: http://ceta.com.ec/serraduras.html

Los controladores remotos de acceso se usan para regular el acceso en áreas restringidas, incluyendo pisos ejecutivos, spas, clubs de salud o áreas de estacionamiento donde es impráctico colocar una cerradura electrónica común. También hay lectores de proximidad disponibles para estas áreas. También puedes utilizar la tecnología de proximidad para las puertas traseras, estacionamientos o accesos a escaleras, ascensores.

- **Opciones de credencial RFID**

Fig. 6.45 Credenciales RFID

Fuente: http://ceta.com.ec/serraduras.html

MIFARE Mini: Una solución efectiva para las tarjetas de los huéspedes. Disponibles con impresión genérica, logotipos de diferentes cadenas hoteleras o personalizadas a gusto del cliente.

MIFARE 1K: Con memoria para 100 eventos, son ideales para el personal. Disponibles como sellos (para huéspedes frecuentes o el personal) o brazaletes (para huéspedes en resorts y parques acuáticos).

MIFARE 4K: Tiene, memoria para 300 eventos, así que son ideales como tarjetas de auditoría e interrogar a las cerraduras.

- **FDU 780 de última generación**

Sencillo pero poderoso, el FDU (Front Desk Unit) de Última Generación es ideal para los hoteles que tienen la necesidad de tener un sistema de control de acceso exhaustivo sin las molestias de una infraestructura centralizada IT.

Solo o interactuando con un PMS, el FDU de Última Generación hace todo, es ideal para los pequeños hoteles en la necesidad de un sistema de control de acceso completa con estaciones de trabajo individuales o múltiples.

Fig. 6.46 FDU (Front Desk Unit)

Fuente: http://www.kaba-ilco.com/lodging-systems/en/Products-Solutions/Access-Control-Systems/294430/frontsk-unit.html

- Codifica, lee y verifica tarjetas magnéticas
- Los programas, auditorías y mantiene bloqueos de hoteles
- Permite 15 niveles de acceso tarjeta de acceso
- Incluye 5 niveles de autorización
- Codifica 10 tarjetas magnéticas para usos especiales
- Almacena una auditoría de las últimas 4000 transacciones
- Mantiene la hora del sistema
- Permite bloquear / FDU auditoría visualización e impresión

- Soporta 8 invitados y personal de 16 áreas comunes
- Con capacidad para 16.000 habitaciones
- Controla la información obtenida del sistema de rastreo
- Programa las cerraduras
- Administra y audita las cerraduras
- Imprime informes de acceso
- Puertos USB
- Un puerto de comunicación serial (DB9 macho), impresoras
- POS compatible
- PMS / interfaz ordenador permite leer datos de los huéspedes check-in para ser transferidos a la FDU

Gracias a sus puertos USB, se puede conectar el FDU a un ordenador externo impresora o sistema PMS para compartir el registro de entrada de datos y presentar auditorías e informes que miden la eficiencia operativa. Implementar actualizaciones y cambios de configuración inmediatamente, eliminando los retrasos y los costes de envío. Se puede actualizar y reconfigurar el FDU de Última Generación instantáneamente en el lugar donde se encuentre, además, es posible exportar las auditorías en archivos de texto a una memoria USB.

Presenta una interfaz intuitiva con menús para el, permite que el personal de la recepción maneje el FDU de Última Generación de una forma sencilla con muy poco entrenamiento, dejándoles más tiempo para buscar nuevos huéspedes.

- **RFID ENCODER 790 LOCK**

Fig. 6.47 Codificador Kaba de tarjetas RFID

Fuente: http://www.kaba-ilco.com/lodging-systems

Incluido con el DFU Kaba encontramos el codificador de tarjetas RFID, que además permite la lectura de tarjetas de auditoria mediante comunicación USB.

- **PROGRAM UNIT ADAPTOR ASSY 790**

Fig. 6.48 Cable de Programación cerraduras Kaba 790

Fuente: http://www.kaba-ilco.com/lodging-systems

El cable de programación Kaba 790 cuenta con conexión serial al FDU que permite la programación de las cerraduras además de otras características.

- **Cilindros y llaves de seguridad**

Fig. 6.49 Llaves y cilindro de seguridad

Elaborado por el investigador

En caso de emergencia o fallo electrónico las cerraduras Kaba cuentan con el sistema de seguridad que permite la apertura de la cerradura en cualquier instante el cilindro es genérico para todo el sistema y codificado por cada hotel.

6.8.3.3 Instalación y programación de cerraduras Kaba

Una vez que ya se cuenta con los equipos de control de acceso se procede con la instalación y configuración de cada uno a excepción de los lectores que corresponden al ascensor debido a que el mismo se encuentra en estado de instalación con una demora de 2 meses.

6.8.3.4 Pasos de instalación de cerraduras Kaba E790

Para la instalación de las cerraduras se cuanta con un diagrama físico de ubicación de cada una que fue presentado en los planos de cada zona y piso del hotel.

Para la instalación física de cada cerradura se necesitan lo siguiente.

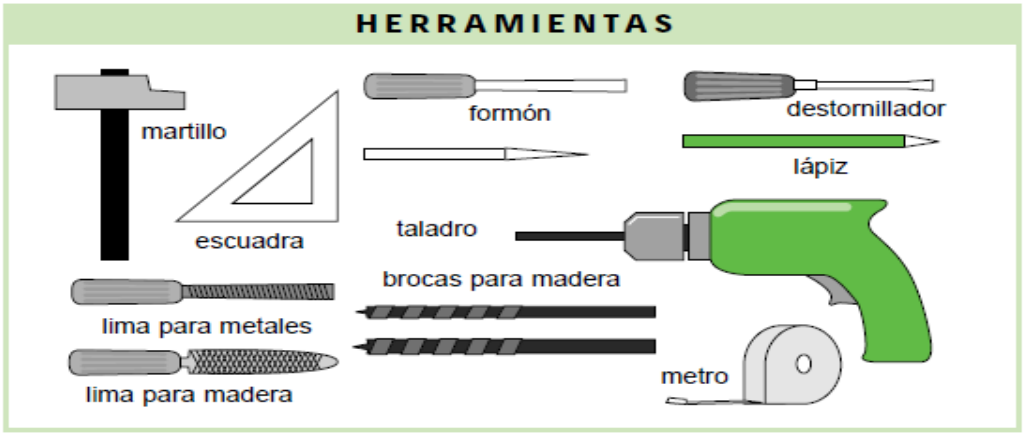


Fig. 6.50 Herramientas de instalación de cerraduras

Fuente: http://grupos.emagister.com/documento/instalacion_de_cerraduras_multipunto/

Una vez que se tienen las herramientas hay que comprobar el sentido de apertura de la puerta.

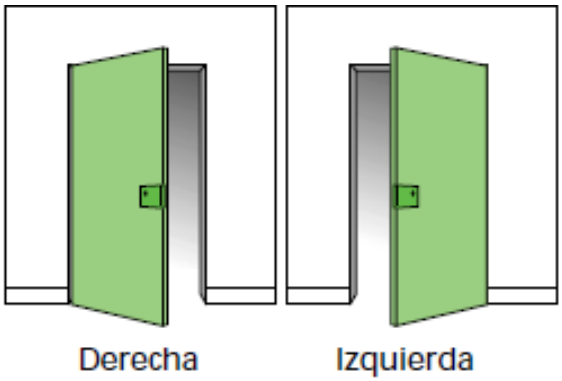


Fig. 6.51 Sentido de apertura en una puerta

Fuente: http://grupos.emagister.com/documento/instalacion_de_cerraduras_multipunto/

Una vez fijado el sentido de la cerradura y con materiales procedemos con la apertura de la caja de la cerradura y la descripción de sus componentes.

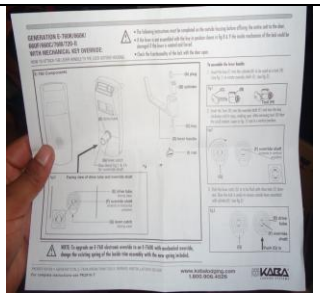
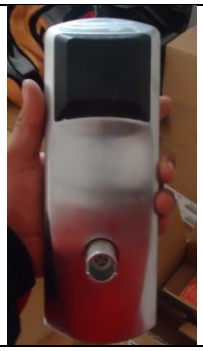
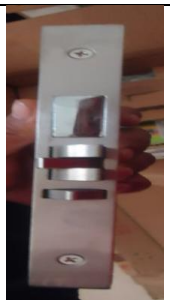
		
Cerraduras Kaba 790	Apertura de la caja	Manual de la cerradura
		
Parte frontal lector RFID	Cerradura parte lateral	Cerradura parte frontal
		
Pilas AA de alimentación	Protección cilindro	Tornillos y engranes
		
Parte trasera	Cilindro de emergencia	Todo el contenido

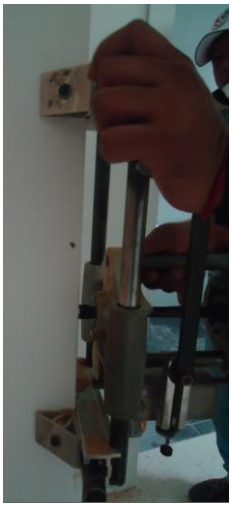
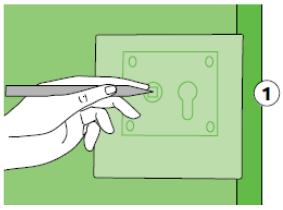
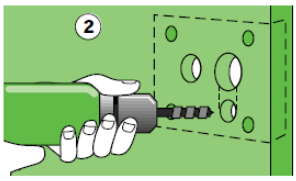
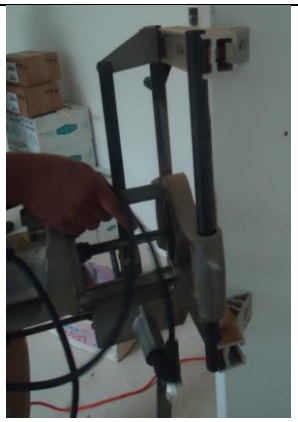
Tabla 6.27 Contenido de la caja cerradura 790

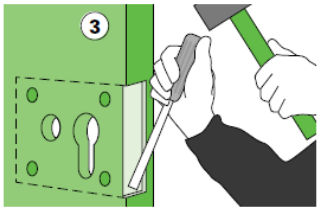
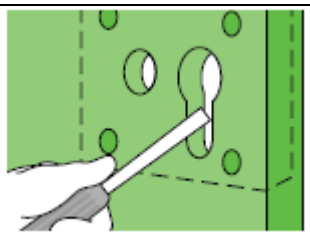
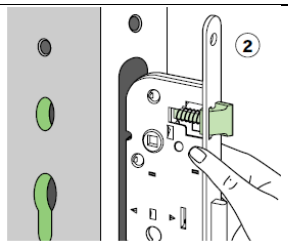
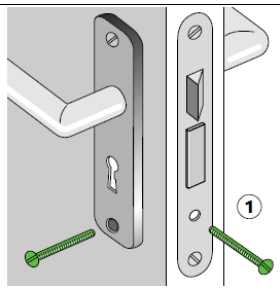
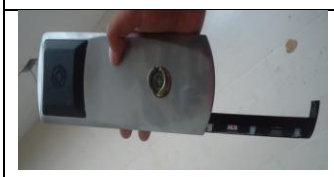
Elaborado por el investigador

Una vez desempaquetado el producto procedemos con la colocación de las pilas AA en el frente de la cerradura, probamos que la cerradura encienda en modo pasivo, una vez listo empezamos con el proceso de instalación.

Cabe recalcar que el proceso de instalación es igual o similar a cerraduras normales, debido a esto se contó con la presencia de un técnico de la empresa CETA que fue el encargado de perforación, alineación, prueba de cada una.

Con herramientas en mano empezamos con los siguientes pasos que se detallan a continuación:

<table>
<tr><td>Colocar la plantilla de la cerradura con cinta adhesiva en el desplazamiento elegido, y marcar los agujeros, la manilla debe colocarse a 1.05 m del suelo y marcar los ejes</td><td>A continuación taladrar el paso de los tornillos y el paso de los ejes de la manilla, todo esto con las brocas adecuadas para cada uno y llevar la mayor precisión en la perforación. Para evitar que la puerta se parta aseguramos con escuadras de sujeción.</td><td>Fotos reales de la instalación
  </td></tr>
<tr><td>  </td><td>  </td><td>  </td></tr>
<tr><td>A continuación o posterior a esto realizamos la perforación en la cara lateral de la puerta en donde va la cerradura para esto usamos un taladro patentado de la marca de la cerradura</td><td>Realizamos la perforación en el lateral según especificaciones con una medida de 30 cm y 2 cm para embonar la cerradura. Después de eso con un formón y lima corregimos los pequeños errores para que ingrese fácilmente</td><td>  </td></tr>
</table>

		
Rebajar el emplazamiento del frente en el canto de la puerta con el formón, Una vez corregidos los errores ingresamos la cerradura	Colocar los 4 tornillos incluidos en el embalaje. Procedemos a ajustar con los tornillos adecuados y colocar los ejes de giro de la manilla.	
		
Colocamos el cilindro de apertura de emergencia en la parte frontal de la cerradura, además de las pilas para poder abrir la puerta	Una vez con el cilindro colocamos la manilla correspondiente de orientación de la puerta derecha o izquierda.	
		

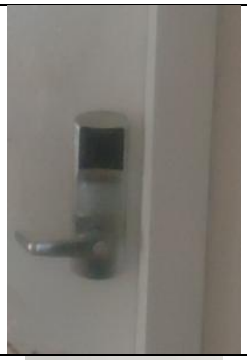
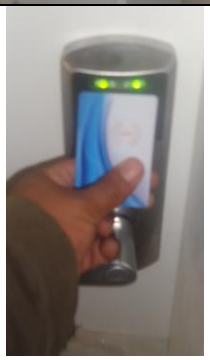
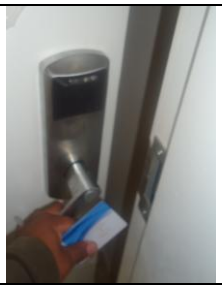
Sobre los ejes montamos la parte frontal y posterior de la cerradura, ajustamos los tornillos para asegurar que no sufra una caída.	Probamos el giro de los ejes y cerramos la puerta para proceder con la a marcar los puntos de fijación de la hembra de la cerradura.	
		
Una vez marcado la parte de instalacion de la hembra de la cerradura se procede a perforar y instalar la hembra.	Probamos que cierre la puerta y no tenga incombenientes en abrir con una tarjeta de prueba y quedar bien segura en caso contrario ajustamos según convenga.	
		

Tabla 6.28 Proceso de instalación cerradura Kaba 790

Elaborado por el investigador

Una vez terminada la instalación probamos con una tarjeta de prueba del sistema esto lo hacemos para todas las cerraduras instaladas, después de eso el carpintero corrige las fallas de instalación en estética y cogiendo fallas, una vez instaladas procedemos con la configuración de cada una de ellas.

6.8.3.5 Programación del sistema de Control de acceso

Con todo listo para el funcionamiento del control de accesos, procedemos con la configuración de las cerraduras para asignarles una identificación, zona, tipo, para lo cual necesitamos lo siguiente:

- Distribución de zonas
- Cable de programación DFU
- DFU (Puesto de recepción)

DISTRIBUCIÓN DE ZONAS PARA LA CONFIGURACIÓN			
Zona / área		**Numero**	**Nivel de acceso**
HABITACIONES Y SUITES			
1	Habitación 01	101	Huéspedes, personal, administrador
1	Habitación 02	102	Huéspedes, personal, administrador
2	Habitación 03	201	Huéspedes, personal, administrador
2	Habitación 04	202	Huéspedes, personal, administrador
2	Habitación 05	203	Huéspedes, personal, administrador
2	Habitación 06	204	Huéspedes, personal, administrador
2	Habitación 07	205	Huéspedes, personal, administrador
2	Habitación 08	206	Huéspedes, personal, administrador
2	Habitación 09	207	Huéspedes, personal, administrador
3	Habitación 10	301	Huéspedes, personal, administrador
3	Habitación 11	302	Huéspedes, personal, administrador
3	Habitación 12	303	Huéspedes, personal, administrador
3	Habitación 13	304	Huéspedes, personal, administrador
3	Habitación 14	305	Huéspedes, personal, administrador
3	Habitación 15	306	Huéspedes, personal, administrador
4	Habitación 16	401	Huéspedes, personal, administrador
4	Habitación 17	402	Huéspedes, personal, administrador
4	Habitación 18	403	Huéspedes, personal, administrador
4	Habitación 19	404	Huéspedes, personal, administrador
4	Habitación 20	405	Huéspedes, personal, administrador
4	Habitación 21	406	Huéspedes, personal, administrador
5	Habitación 22	501	Huéspedes, personal, administrador
5	Habitación 23	502	Huéspedes, personal, administrador
5	Habitación 24	503	Huéspedes, personal, administrador
5	Habitación 25	504	Huéspedes, personal, administrador
5	Habitación 26	505	Huéspedes, personal, administrador
5	Habitación 27	506	Huéspedes, personal, administrador
6	Suite 01	307	Huéspedes, personal, administrador
6	Suite 02	407	Huéspedes, personal, administrador
6	Suite 03	507	Huéspedes, personal, administrador
ASCENSOR			
7	Planta 0	001	Huéspedes, personal, administrador
7	Planta 1	103	Huéspedes, personal, administrador
7	Planta 2	208	Huéspedes, personal, administrador
7	Planta 3	308	Huéspedes, personal, administrador
7	Planta 4	408	Huéspedes, personal, administrador
7	Planta 5	508	Huéspedes, personal, administrador
Cuartos para distracción de huéspedes			
7	Cuarto Pc	309	Huéspedes, personal, administrador

7	Cuarto Juegos	310	Huéspedes, personal, administrador
7	Cuarto Recreación	311	Huéspedes, personal, administrador
Cuartos de acceso permanente solo personal autorizado			
8	Bodega restaurante	701	Personal, administrador
8	Bodega licores	702	Personal, administrador
8	Bodega pertenencias	703	Personal, administrador
9	Lavandería	704	Personal, administrador
10	Cuarto de equipos	705	Administrador

Tabla 6.29 Tabla de configuración de numero de cerraduras

Elaborado por el investigador

- **Programación de cerraduras mediante FDU**

Se hace referencia al manual de programación que viene con el equipo, en donde aplica de una en una en este ejemplo se realiza para el Hotel Destiny en donde se siguen los siguientes pasos para una configuración basica.

- Encendemos el DFU, una vez con carga completa trabaja de forma autónoma, ingresamos la hora y fecha exactas para que se envié a la programación de las cerraduras.
- Conectamos el cable de programación al puerto serial DB9.
- Procedemos a poner sobre la cerradura el cable de programación como se indica en la fig. 6.52.

Fig. 6.52 Programación cerradura Kaba

Elaborado por el investigador

- El DFU cuenta con una tarjeta de acceso o un código que se puede activar mediante su menú.
- Antes de la programación hay que tomar en cuenta que si es la primera vez que lo hacemos, debemos asegurarnos que las baterías de la cerradura deben estar en perfectas condiciones, en caso se interrumpa

la programación, reemplazarlas y volver a inicializar la cerradura como indica el manual.

- Activar el menú del FDU
- Presionar 8 seleccionar programación
- Presionar 1 seleccionar una cerradura
- Presionar 1 seleccionar programar direcciones
- Escribir el número de habitación, suite, bodega, ejemplo 101, sección 01, piso 1, grupo 1, zona 1, área 1, toda esta información según el cuadro de planificación del hotel, presionar enter y esperar que se realice el proceso de programación de la cerradura.
- Una vez terminado se presenta el mensaje "la comunicación se a realizado satisfactoriamente"
- Este proceso se lo realiza para todas las cerraduras que sean de huéspedes, existe otro proceso de programación de áreas comunes.

- **Programación de áreas comunes**

Las áreas comunes representan las zonas en donde el huésped puede ingresar además de su habitación durante su hospedaje estas áreas son.

- Ascensor
- Cuarto de computación
- Cuarto de juegos
- Cuarto de recreación

Programación

- Ingresamos al menú
- Presionamos 8 seleccionamos programación
- Presionamos 1 seleccionamos una cerradura
- Presionamos 4 seleccionamos programación áreas comunes
- Presionamos > seleccionamos área huésped
- Presionamos ∨ seleccionamos área
- Ingresamos

- Seleccionamos el área configurada en la programación de cada cerradura
- Además podemos asignar un tiempo de uso de cada área
- Una vez configurado presionamos enter y esperar que se realice el proceso de programación de la cerradura.
- Una vez terminado se presenta el mensaje "la comunicación se a realizado satisfactoriamente"

- **Programación de áreas restringidas**

Las áreas restringidas representan las ubicaciones que solo pueden ser utilizadas por personas autorizadas como empleados o el administrador del sistema, estas áreas son:

- Bodega restaurante
- Bodega licores
- Bodega pertenencias
- Lavandería
- Cuarto de equipos

Programación

- Ingresamos al menú
- Presionamos 8 seleccionamos programación
- Presionamos 1 seleccionamos una cerradura
- Presionamos 5 seleccionamos Programación áreas Restringidas
- Presionamos el número asignado al área ejemplo 10 del cuarto de equipos, el rango va de 1 a 200.
- Además podemos asignar un tiempo de uso de cada área
- Una vez configurado presionamos enter y esperar que se realice el proceso de programación de la cerradura.
- Una vez terminado se presenta el mensaje "la comunicación se a realizado satisfactoriamente"
- Ahora esta cerradura corresponde al área restringida numero 10

Una vez terminada la configuración de todas las cerraduras con la información de número de habitaciones, áreas comunes y las áreas restringidas, se termina el proceso de programación de cerraduras, cabe recalcar que se pueden incrementar a futuro muchas más cerraduras de igual manera se podrán programar.

La programación tiene muchas más opciones que se pueden adaptar a todo tipo de situaciones como sea el caso, se adjunta el manual de programación en anexos en donde se puede revisar todas las posibilidades que representa el control de acceso.

- **Codificación de tarjetas de acceso mediante FDU**

Las tarjetas son el medio de acceso, que permiten la autorización de apertura de cerraduras y áreas comunes, existen mucha formas de configuración de tarjetas solo se tomaran las principales de uso para el hotel Destiny las demás se presentan en anexos las cuales pueden ser adaptadas a cualquier tipo de usos.

La codificación se realiza con el DFU y se graba o codifica mediante el codificador RFID 790 que se indicó con anterioridad.

A continuación se presenta la codificación de algunos tipos de tarjetas de acceso:

- **Codificación tarjeta llave de Huésped**

La tarjeta de huésped contiene la numeración de la habitación o suite, el tiempo de creación, el tiempo de expiración y otras opciones disponibles, como áreas comunes las cuales están a disposición del huésped del Hotel.

Programación

- Ingresamos al menú
- Presionamos 1 para seleccionar tarjeta huésped
- Presionamos 1 seleccionamos huésped
- ingresamos el número asignado de habitación ejemplo 101
- El número de noches de hospedaje
- La fecha de ingreso
- La hora de expedición de la tarjeta
- Asignamos como tarjeta nueva

- Asignamos la cantidad de tarjetas en caso necesiten más de una
- Asignamos las áreas comunes para el uso de la tarjeta
- Una vez configurado presionamos enter y esperar que se realice el proceso de codificación de la tarjeta
- Insertamos o montamos la tarjeta en el codificador
- Una vez terminado se presenta el mensaje " Su tarjeta de huésped ha sido creada para la habitación 101 satisfactoriamente"
- Ahora esta tarjeta únicamente corresponde a la habitación 101 y áreas comunes del hotel
- Una vez pasada la hora de expiración la tarjeta queda anulada
- La tarjeta llevara impresa una forma de presentación del hotel, la cual será obsequiada como medio de información y publicidad

- **Codificación tarjeta Huésped pre-registro**

Puede ser elaborada 10 días antes de que comience el registro del huésped, encaso se realicen reservaciones vía telefónica o internet.

Programación

- Ingresamos al menú
- Presionamos 1 para seleccionar tarjeta huésped
- Presionamos 1 seleccionamos huésped pre- registro
- Ingresamos el número asignado de habitación ejemplo 101
- Presione la flecha derecha para acceder al menú Fecha e indicar cuándo será utilizada en la cerradura. Nota: Se podrá hacer las tarjetas de Pre-Registro solo con 10 días de anticipación. Presione cuando haya seleccionado la Fecha.
- Puede cambiar otras opciones como la cantidad de Noches, la Hora de Expiración, Tarjeta Nueva o Duplicada y cualquier otra opción habilitada en el FDU. Utilice el botón de flecha abajo para cambiar las opciones.
- Asignamos las áreas comunes para el uso de la tarjeta

- Una vez configurado presionamos enter y esperar que se realice el proceso de codificación de la tarjeta
- Insertamos o montamos la tarjeta en el codificador
- Una vez terminado se presenta el mensaje " Su tarjeta de pre-registro huésped ha sido creada para la habitación 101 satisfactoriamente"
- Ahora esta tarjeta únicamente corresponde a la habitación 101 y áreas comunes del hotel
- Una vez pasada la hora de expiración la tarjeta queda anulada

- **Para verificar las Tarjetas de los Huéspedes**

Puede verificar una Tarjeta Huésped utilizando la función "Leer/Verificar" y saber el número de Tarjeta del Huésped mediante esta función, a menos de que el FDU esté configurado para no hacerlo.

- Deslice su tarjeta de Autorización válida para el FDU o teclee su NIP.
- Para la Cerradura de proximidad 790, presente su tarjeta de Autorización válida para el FDU sobre el codificador de proximidad externo.
- Si el nivel de usuario es FDA, presione el botón para ir a la pantalla principal.
- Presione 2 para seleccionar "Leer/Verificar".
- Deslice la Tarjeta del Huésped para que sea leída.
- Para la cerradura 790 de proximidad presente la tarjeta en el codificador de tarjetas de proximidad externo.
- Si la tarjeta no es una Tarjeta de Huésped, el FDU desplegará un mensaje de error de "Tipo inválido de tarjeta" y regresará al menú anterior. De otro modo, en caso necesario se le pedirá al usuario su número de habitación.
- Ingrese el número de habitación de la tarjeta verificada, después presione Para una habitación que pertenece a una Suite de Puerta Común ingrese el número de la Puerta Común.

- Si la tarjeta no corresponde al número ingresado, el FDU desplegará el mensaje de error "Tipo de tarjeta inválida" y regresará al menú anterior.
- Si la tarjeta corresponde al número de habitación ingresado los detalles de la tarjeta se desplegarán en la pantalla.
- Para ver la información restante de la tarjeta, utilice la flecha abajo. Si el FDU tiene un sistema de track 3 que permite los números de folio y la tarjeta no tiene un folio definido, se dejará el campo en blanco.
- Presione cualquier botón para regresar al Menú principal.

- **Codificación tarjeta llave de áreas restringidas**

La tarjeta de áreas restringidas permite solo al administrador o encargado de mantenimiento ingresar a la zona.

Programación

- Ingresamos al menú
- Presionamos 6 para seleccionar tarjeta personal
- Presionamos 3 seleccionamos área restringida
- Ingresamos el número asignado del área por ejemplo 10
- Asignamos como tarjeta nueva
- Asignamos la cantidad de tarjetas en caso necesiten más de una
- Una vez configurado presionamos enter y esperar que se realice el proceso de codificación de la tarjeta
- Insertamos o montamos la tarjeta en el codificador
- Una vez terminado se presenta el mensaje " Su tarjeta área restringida ha sido creada para la área 10 satisfactoriamente"
- Ahora esta tarjeta únicamente corresponde al área 10
- La tarjeta asignada será identifica por cada empleado o administrador para las auditorias pertinentes

- **Codificación tarjeta llave de Botones**

Utilizado para hacer la tarjeta maestra del botones la cual abre todas las habitaciones de la propiedad exceptuando las áreas restringidas o las habitaciones que han sido cerradas utilizando el pestillo o seguro de privacidad, una tarjeta de cierre de habitación o una tarjeta de cierre del hotel. La tarjeta maestra de botones opera únicamente en los niveles de habitaciones y suites. No hay husos horarios con esta tarjeta debido a que el momento de expiración debe ser establecido en el menú de expiración. Utilizado para hacer la tarjeta maestra del botones.

- Ingresamos al menú
- Presionamos 6 para seleccionar tarjeta personal
- Presionamos 2 seleccionamos Autorización FDU
- Presione la flecha derecha para seleccionar "Botones".
- Utilice la flecha abajo para ingresar la Autorización # (cada tarjeta debe ser hecha por separado y debe tener un # individual ente 121-160).
- Ingrese el número de Autorización 121 (ejemplo). Presione enter.
- Utilice la flecha abajo para habilitar el NIP de Autorización #. (Este será desplegado si la opción de NIP está habilitada).
- Utilice la flecha abajo para ingresar el NIP# 1234 (ejemplo) (Cada tarjeta debe tener un #NIP separado). Presione enter
- Inserte y deslice una tarjeta en blanco y/o presente la tarjeta al codificador de proximidad (para las cerraduras 790).
- Su tarjeta de Autorización del botones #121 ha sido creada.
- El NIP#5678 puede remplazar la tarjeta BA#121 para acceder al FDU.
- Ingresamos el número asignado del área por ejemplo 10
- Asignamos como tarjeta nueva
- Asignamos la cantidad de tarjetas en caso necesiten más de una
- Una vez configurado presionamos enter y esperar que se realice el proceso de codificación de la tarjeta
- Insertamos o montamos la tarjeta en el codificador

- **Para resumir se puede codificar las siguientes tarjetas:**

Tarjeta de Huésped por Una Vez	Recepción (FDA)
Suites adjuntas	Programador (PA)
Suites de Puerta Común	Maestra (MA)
Tarjeta de prueba de la batería	Gerente General (GMA)
Tarjetas de programación	Gran Maestra
Tarjetas de Inicialización	Emergencia
Tarjetas de Prueba de la Cerradura	Reinicio del hotel Reinicio de tarjetas de huésped
Tarjetas de Paso Libre	Reinicio de área de acceso
Acceso del huésped a área común	restringido
Tarjetas de Bloqueo/Desbloqueo	Reinicio de tarjetas del personal
Cierre del hotel	Reinicio de Área Restringida
Auditoría de la cerradura	Reinicio de Botones
Tarjeta de Piso	Reinicio de tarjeta Gran Maestra
Tarjeta de Zona	Reinicio Emergencia
Tarjeta de Área	Tarjeta de auditoria

- **Horarios fijos**

Hay seis zonas horarias fijadas que se pueden utilizar para limitar el acceso del personal a cualquier cerradura en el sistema

  - Deslice una tarjeta autorizada GMA o MA.
  - Para la cerradura de proximidad 790, presente una tarjeta de Autorización válida para el FDU sobre el codificador de proximidad externo.
  - Presione 7 para seleccionar la opción “configuración FDU”.
  - Presione 2 para seleccionar la opción “características FDU”.
  - Presione 2 para seleccionar la opción “opciones de tarjeta”.
  - Presione 2 para seleccionar la opción “tarjeta personal”.
  - Presione 3 para seleccionar “Horarios Fijos”.
  - Presione la flecha derecha para habilitar/deshabilitar los horarios fijos.
  - La disposición del horario fijo es la siguiente: Timezone-1 12 am a 4 am, Timezone-2 4 am a 8 am, Timezone-3 8 am a 12 pm, Timezone-4 12 pm a 4 pm, Timezone-5 4 pm a 8 P.M., Timezone-6 8 pm a 12 am.
  - Utilice la flecha abajo para cambiar a cada horario fijo.
  - Los horarios fijos son a partir 1 a 6. Las opciones son:

- Sí= cuando la tarjeta de personal se hace en cuestión de los avisos del FDU de sí/no a permitir/rechazar el acceso a las habitaciones del huésped para el horario fijo específico seleccionado.
- No= no será codificado el horario fijo específico en la tarjeta, y no tendrá ningún acceso.
- Auto= no será solicitado el horario fijo específico al codificar la tarjeta de personal.
- El FDU dará el acceso automático al horario fijo específico.
- Una vez establecidas todas las opciones, presione Se han registrado los ajustes

- **Auditoría de cerradura**

La auditoría de la cerradura se puede consultar en caso de acceso restringido para determinar qué tarjeta fue utilizada, cuando ocurrió la entrada, y la identidad del operador que utilizó la tarjeta. El registro de auditoría de la cerradura también registra el uso de tarjetas especiales tales como uso del reajuste (Reinicio), de salida, de la programación, de la inicialización y del pestillo. El cable de FDU y de la comunicación se utiliza para leer la auditoría almacenada en la cerradura o alternativamente una sola tarjeta de auditoría para la cerradura 790 de proximidad.

Auditar cerradura

- Presione 9 para seleccionar el menú “auditoria/reporte”.
- Presione 1 para seleccionar el menú “auditoria de cerradura”.
- Presione 1 para seleccionar el menú “auditar cerradura.”
- Nota: El FDU puede almacenar hasta 10 intervenciones en la memoria de la cerradura.
- Si ya existen intervenciones almacenadas en la memoria del FDU, FDU mostrará: “borrar intervenciones de la memoria?” 1=Si para borrar todas las intervenciones No= guardar todas las intervenciones.
- El FDU mostrará: “configurado para audit lock strike a key”.
- Deslice una tarjeta programada en la cerradura (o presente la tarjeta en el lector, para la cerradura 790 de proximidad). El L.E.D. verde sólido entrará en modo de programa para activar la cerradura.

- Conecte el cable de la comunicación del FDU, firmemente en la cerradura y presione en el FDU. Se observa el siguiente mensaje: “La comunicación se realizó con éxito. Presione cualquier tecla para continuar.”
- La auditoría ha sido almacenada en la unidad FDU.

- **Crear una tarjeta de auditoría**
  - Presione 4 para seleccionar el menú “activación de la tarjeta”.
  - Presione 6 para seleccionar la “auditoría de la cerradura.”
  - Ingrese la cantidad de tarjetas que se fabricarán.
  - Cuando establezca la cantidad, presione para codificar la tarjeta(s).
  - Presente la tarjeta(s) al codificador de proximidad (para la cerradura 790).
  - Se ha creado la tarjeta de auditoría de la cerradura.

- **Crear reporte a través de la tarjeta de auditoria**
  - Presione 9 para seleccionar el menú “auditoria/reporte”.
  - Presione 1 para seleccionar el menú “auditoría de la cerradura”.
  - Presione 1 para seleccionar “auditar cerradura”
  - Presentar la tarjeta de auditoría de la cerradura al lector de proximidad. La auditoría ha sido almacenada en la unidad FDU.

- **Auditando la tarjeta personal**
  - Presente la tarjeta autorizada al codificador FDU de proximidad externo.
  - Presione 9 para seleccionar el menú “auditoria/reporte”.
  - Presione 3 para seleccionar el menú “auditoria personal”.
  - Presione 1 para seleccionar el menú “auditar personal”.
  - Presente una tarjeta personal (sección, piso, grupo, zona, área, bell Man’s master o grand master) al lector de proximidad.
  - La auditoría se ha almacenado en la unidad FDU. Conservé la identificación proporcionada
  - de la auditoría para futuras operaciones

- **Reporte de cerradura para imprimir**

Conecte el impresor serial al puerto serial del FDU, o un impresor USB al puerto USB. Referencias en el 9.1.4. Que se encuentra en anexos. En el paso 6 seleccione

el tipo de medio de impresión que ha sido conectado a la unidad FDU. Ahora continúe con los siguientes pasos.

- **Reporte de cerradura al dispositivo de memoria USB**

Conecte un dispositivo de memoria USB al puerto USB. Referencias en el 9.1.5. En el paso 6 seleccione el medio "dispositivo USB" que ha sido conectado a la unidad FDU. Ahora continúe con los siguientes pasos.

Con esto se finaliza la parte de control de accesos que se implementó en el Hotel.

6.8.3.6 Instalación y programación del sistema de video vigilancia

Los equipos seleccionados para video vigilancia se expusieron con anterioridad en la tabla 6.15 los cuales fueron adquiridos y entregados a los propietarios del hotel, el sistema de cableado para las cámaras se encuentra listo para la instalación de las mismas, las cuales no son instaladas por motivos de acabados en el interior del hotel, postergando la instalación para un mes antes de la apertura.

Antes de continuar con la configuración se realiza un análisis del DVR que es el medio de grabación y de la configuración según requerimientos por zonas en el hotel, las cuales son presentadas a continuación.

- **Consideraciones previas a la instalación:**

Para la instalación del sistema de video vigilancia se tomó en cuenta lo siguiente:

- Determinar la finalidad del sistema de C.C.T.V., y determinar la misión de cada cámara en el sistema.
- Definir las áreas que cada cámara visualizara.
- Elegir el tipo de cámara adecuada según su utilidad
- Determinar donde se localizara el monitor o monitores para visualizar el sistema.
- Determinar el mejor método para transmitir la señal de vídeo de la cámara al monitor.
- Diseñar el área de control.
- Definir el tipo de cable directo con BNC, o mediante adaptadores BALUM

- Elegir el equipo de videograbación DVR

- **Tipo de cable para la instalación**

Para la instalación se utilizó cable UTP cat6 de las siguientes especificaciones.

El cable UTP Cat6 usa al máximo el ancho de banda, proporcionando un desempeño excepcional. Funciona conforme a los requisitos de la norma ANSI/TIA/EIA-568 B.2-1, Categoría 6 e ISO/IEC-11801.

Especificaciones:

- Número de Pares: 4
- Conductores: 8
- AWG: 23
- Tipo: Sólido CM
- Alambre de Cobre

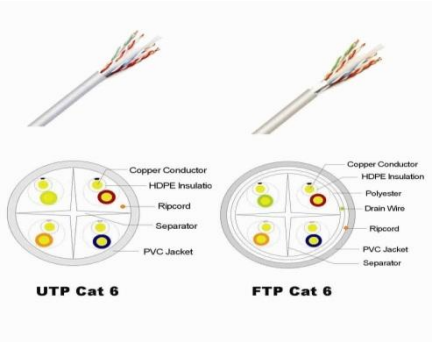


Fig. 6.53 Cable Cat 6

Fuente: www.lolap.wordpress.com

Ventajas en CCTV

- Se pueden usar cables multipares existentes compartidos con otros servicios como alarmas, telefonía y datos.
- Costo menor que el del coaxial.
- Cableados discretos en interiores
- Empalmes rápidos y económicos
- Menor volumen. Por un solo cable UTP se pueden mandar hasta 4 cámaras (4 pares)
- Menores pérdidas y mayor alcance sin amplificadores
- Menores interferencias
- Con este cable se puede transmitir video a más de 600 metros sin amplificador

En el hotel se estima que la cámara de mayor extensión de cableado se encuentra en la terraza con una longitud de cable de 30 a 60 metros.

- **Balun adaptador de CCTV**

La palabra "balun" es una contracción de "BALanced to UNbalanced transformer", es decir, "transformador de balanceado a desbalanceado". Entonces lo mejor es partir por comprender a qué se refiere exactamente este concepto del balance. En el caso de nuestro proyecto usamos Balum de modo pasivo, a diferencia de los activos que necesitan de energía para ayudar con la amplificación de transmisión para alcanzar mayores distancias.

El Balum es el encargado de transformar la resistencia e impedancia del cable UTP a 75Ω de conectores BNC que son por defecto de entradas y salidas de cámaras y del DVR encargado de la transmisión, existen Balum que permiten transmitir audio video y energía para ahorrar espacio.

En el caso práctico de nuestro proyecto se usara un par por conexión de cámara, lo cual ahorrara espacio y dinero.

Fig. 6.54 Adaptador de video Balun

Elaborado por el investigador

El voltaje que se usara en las cámaras es de 12v a 2 amperios cada una, se instala dentro de una caja de conexión junto a cada cámara lo cual está listo en la infraestructura del hotel, además en cada piso existe una caja de control en donde están las conexión de cámaras, internet y línea telefónica en caso de fallos de visualización se puede revisar libremente cada cámara.

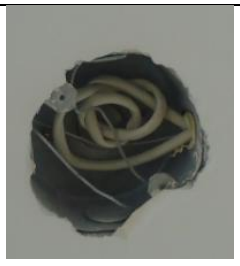


Tabla 6.30 Imágenes físicas para la instalación de cámaras

Elaborado por el investigador

Distribución y requerimientos del sistema de video vigilancia:

DISTRIBUCIÓN DE ZONAS PARA LA CONFIGURACIÓN			
DVR / área		**Numero**	**Requerimiento**
ESTACIONAMIENTO			
DVR 1	Ingreso	01	Cámara HD, Grabación permanente
DVR 1	Parqueadero	02	Cámara SD, Grabación por detección de movimiento
DVR 1	Parqueadero	03	Cámara SD, Grabación por detección de movimiento
DVR 1	Cuarto de maquinas	04	Cámara SD, Grabación por detección de movimiento
DVR 1	Ascensor	05	Cámara HD, Grabación permanente
PLANTA BAJA			
DVR 1	Ingreso	06	Cámara HD, Grabación permanente
DVR 1	Ingreso	07	Cámara SD, Grabación permanente
DVR 1	Restaurante	08	Cámara SD, Grabación permanente
DVR 1	Administración	09	Cámara SD, Grabación permanente
DVR 1	Pasillo	10	Cámara SD, Grabación permanente
DVR 1	Cocina	11	Cámara SD, Grabación permanente
PRIMERA PLANTA			
DVR 1	Bar cafetería	12	Cámara HD, Grabación permanente
DVR 1	Ingreso bar	13	Cámara SD, Grabación permanente
DVR 1	Ingreso piso 1	14	Cámara SD, Grabación permanente
DVR 1	Bodega licores	15	Cámara SD, Grabación por detección de movimiento
DVR 1	Bodega pertenencias	16	Cámara SD, Grabación por detección de movimiento
DVR 2	Pasillo	01	Cámara SD, Grabación permanente
SEGUNDA PLANTA			
DVR 2	Ingreso piso 2	02	Cámara SD, Grabación permanente
DVR 2	Computadores	03	Cámara SD, Grabación por detección de movimiento
DVR 2	Juegos	04	Cámara SD, Grabación por detección de movimiento
DVR 2	Recreación	05	Cámara SD, Grabación por detección de movimiento
DVR 2	Pasillo	06	Cámara SD, Grabación permanente
TERCERA PLANTA			
DVR 2	Ingreso piso 3	07	Cámara SD, Grabación permanente
DVR 2	Pasillo	08	Cámara SD, Grabación por detección de movimiento
CUARTA PLANTA			
DVR 2	Ingreso piso 4	09	Cámara SD, Grabación permanente
DVR 2	Pasillo	10	Cámara SD, Grabación por detección de movimiento
TERRAZA			
DVR 2	Ingreso terraza	11	Cámara SD, Grabación permanente
DVR 2	Sistema Solar	12	Cámara SD, Grabación por detección de movimiento
DVR 2	Lavandería	13	Cámara SD, Grabación por detección de movimiento

Tabla 6.31 Tabla de configuración de requerimientos de video vigilancia

Elaborado por el investigador

- **Consideraciones para la instalación**

Nunca pasar un cable a no menos de 20 cm. de una línea de corriente alterna, produce interferencias. Usar en lo posible los cables en un solo tramo, los empalmes traen pérdidas en la señal, en caso de tener que hacerlo usar conectores o soldar y aislar.

Evitar en la medida de las posibilidades los tendidos aéreos, el cable suele atraer descargas atmosféricas, que pueden quemar el integrado de vídeo de la cámara. Hay también otro tipo de cable que se utiliza en las instalaciones de los kits de observación, 4 conductores y una malla, en este tipo de cable se envía la información de vídeo, audio y alimentación.

- **Esquema del sistema de video vigilancia:**

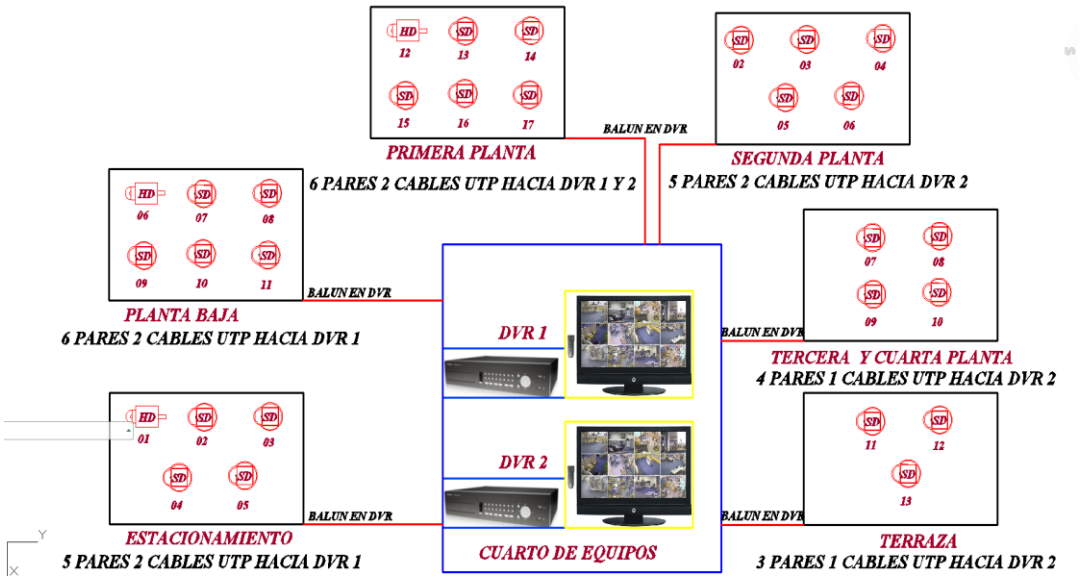


Fig. 6.55 Diagrama físico del sistema de video vigilancia

Elaborado por el investigador

- **Configuración del sistema de video vigilancia**

Una vez que se instale físicamente todo el cableado y cámaras, se procede con la configuración de equipos de grabación según la tabla indicada anteriormente, la cual realiza una distribución por zonas, se presenta la siguiente programación básica para iniciar y poner en funcionamiento los DVR adquiridos por el hotel.

- **Presentación y configuración DVR AVTECH AVC798PV**

Este dispositivo debe utilizarse únicamente con el tipo de fuente de alimentación indicado en la etiqueta del fabricante. Conecte el cable de alimentación AC indicado en el adaptador de alimentación, y enchúfelo en una toma eléctrica. Se iluminará la luz LED de encendido.

Antes de encender el DVR, asegúrese de que las cámaras están conectadas y que alimentadas por su correspondiente fuente de alimentación para que el sistema de vídeo por cámaras las detecte adecuadamente. Así mismo, asegúrese de que el monitor (LCD o CRT) esté conectado al DVR antes de encender el DVR para que se detecte correctamente la salida de vídeo.

Para asegurar que su DVR funcione constante y apropiadamente, se recomienda el uso de UPS (Suministrador de energía ininterrumpida, opcional) para un funcionamiento continuado.

Pasos para empezar

Para empezar se realizaran varios pasos de configuración inicial, no se los presenta en detalle, solo un breve resumen lo demás se puede consultar en el manual de referencia del equipo.

- Conexión de discos duros para el almacenamiento
- Configuración de fecha y hora
- Eliminar el disco duro
- Configuración de contraseña
- Conexión del ratón USB
- Barra de Menú Rápido

- **Funcionamiento básico**

El funcionamiento básico del equipo está dado por un sinnúmero de posibilidades las cuales no necesitan del mayor conocimiento para su uso, el cual presenta opciones de fácil reconocimiento como se muestra en la fig. 6.56

Icono	Función	Icono	Función	Icono	Función
	Canal de audio directo (1 ~ 4)		Canal de audio de reproducción (1 ~ 4)		Canal de audio desactivado
	Zoom Digital activado		Zoom Digital desactivado		Grabación temporizada
	Red desconectada		Internet conectado		LAN conectada
	Ratón USB conectado		Unidad / Dispositivo flash USB conectado		No se ha conectado el dispositivo USB
	Bloqueo de teclado		Modo PTZ activado		Sobrescribir el disco duro
	Administrador		Operador		Secuencia
	Movimiento		Grabando		Alarma

Fig. 6.56 Presentación básica del entorno DVR

Fuente: Manual DVR AVTECH

- **Grabación manual**

  De forma predeterminada, la grabación manual está activada ( ) cuando se enciende el DVR y se ha instalado un HDD.

- **Grabación de evento**

  Cuando la detección de movimiento o la alarma se activa, se muestra en la pantalla el icono de movimiento ( ) o el icono de alarma ( ) para informar del evento de movimiento o alarma.

- **Grabación temporizada**

  Cuando la grabación por temporizador está activada, verá el icono en la pantalla.

- **Sobre escritura del HDD**

  De forma predeterminada, la función de sobre escritura del disco duro está ENC. y se mostrará en la pantalla.

- **Control de reproducción**

  Debe haber al menos 8192 imágenes de datos grabadas para que la reproducción funcione correctamente. De no ser así, el dispositivo detendrá la reproducción. Por ejemplo, si el IPS está configurado a 30, el tiempo de grabación debe ser de al menos 273 segundos (8192 imágenes / 30 IPS) para que la reproducción funcione correctamente.

	Reproducción Rápida	Aumenta la velocidad del REPRODUCCION RÁPIDA. Haga clic una vez para conseguir una velocidad de avance de 4X y haga clic dos veces para una velocidad de 8X, etc., siendo la máxima velocidad de 32X.
	Rebobinado	Aumenta la velocidad del rebobinado. Haga clic una vez para conseguir una velocidad de rebobinado de 4X y haga clic dos veces para una velocidad de 8X, etc., siendo la máxima velocidad de 32X.
/	Despliegue / Pausa	Haga clic para reproducir el último clip de vídeo inmediatamente y haga clic de nuevo para pausarlo. En el modo pausa, haga clic un vez en para avanzar un fotograma y haga clic en para rebobinar un fotograma.
	Paro	Haga clic para detener la reproducción de vídeo.
	Reproducción lenta	Haga clic un vez para obtener una velocidad de reproducción de 1/4X y haga clic dos veces para una velocidad de 1/8X.
/	Hora anterior / siguiente	Haga clic para saltar el intervalo de una hora siguiente / anterior, por ejemplo: 11:00 ~ 12:00 o 14:00 ~ 15:00, y comience a reproducir el clip de vídeo del evento más cercano grabado durante toda esa hora.

Fig. 6.57 Control de grabación

Fuente: Manual DVR AVTECH

- **Configuración de grabación**

Cada DVR cuenta con dos discos duros de 1 tb, lo cual permite varios días de grabación, es difícil saber el tiempo exacto de grabación que permitirá el dispositivo, para esto nos basamos en un cálculo que lo podemos realizar manualmente de la siguiente manera.

El equipo recomienda el siguiente formato de grabación el cual será el escojido para la configuración ya que ofrece calidad y menor tamaño en espacio del disco.

- **Cálculo en H.264**

Velocidad binaria aprox./8 (bits en un byte) x 3.600s = KB por hora/1.000 = MB por hora MB por hora x horas de funcionamiento diarias/1.000 = GB por día GB por día x periodo de almacenamiento solicitado = Necesidades de almacenamiento

Cámara	Resolución	Velocidad binaria aprox. (kbps)	Imágenes por segundo	MB/hora	Horas de funciona-miento	GB/día
No. 1	CIF	110	5	49.5	8	0.4
No. 2	CIF	250	15	112.5	8	0.9
No. 3	4CIF	600	15	270	12	3.2
Capacidad total para las 3 cámaras y 30 días de almacenamiento = 135 GB						

Las cifras anteriores están basadas en muchos movimientos en una escena. Con algunos cambios en una escena, las cifras pueden ser un 20% inferiores. La cantidad de movimiento de una escena puede tener un gran impacto en el almacenamiento requerido.

Fig. 6.58 Cálculo de grabación formato H.264

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

En nuestro caso manejaremos un máximo de 16 cámaras por DVR cada uno tiene la capacidad de 2000 GB, en la web existen una página en donde podemos ingresar los datos para obtener un estimado del tiempo de grabación.

- Ingresamos al link www.i3international.com/es/storagecalculator.html
- Ingresamos los datos de nuestro proyecto
- Compresión = H.264
- Calidad = alta
- Resolución = 4CIF (740*480)
- Velocidad de imagen = 10 fps
- Canales = 16
- Horas de grabación = 24
- Días de grabación = 30

Como resultado obtenemos 2202.48 Gb que están dentro de nuestro rango de capacidad, hay que tomar en cuenta que las cámaras de nuestro proyecto tienen programación de grabación por movimiento lo cual reducíria esta cifra considerablemente en un 40%.

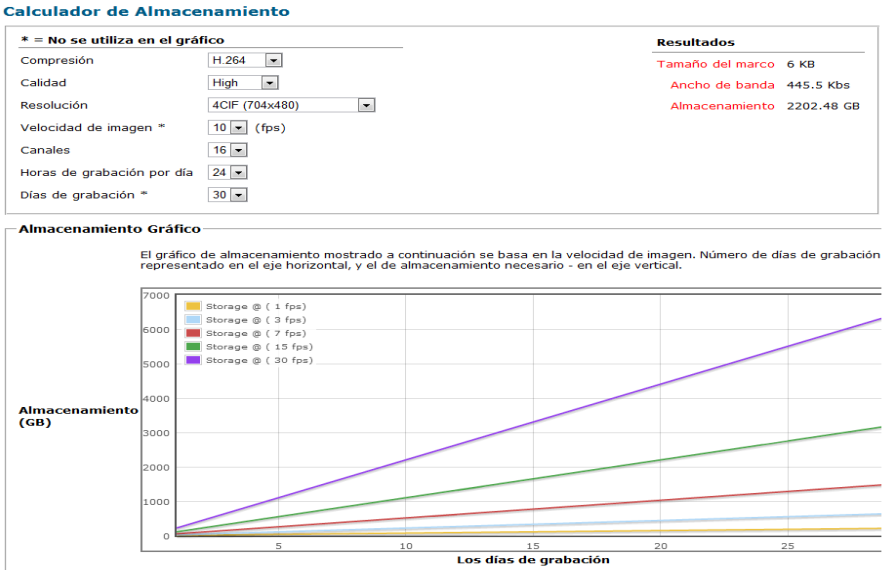


Fig. 6.59 Cálculo de almacenamiento

Elaborado por el investigador

Como otro ejemplo reduciremos la calidad de grabación.

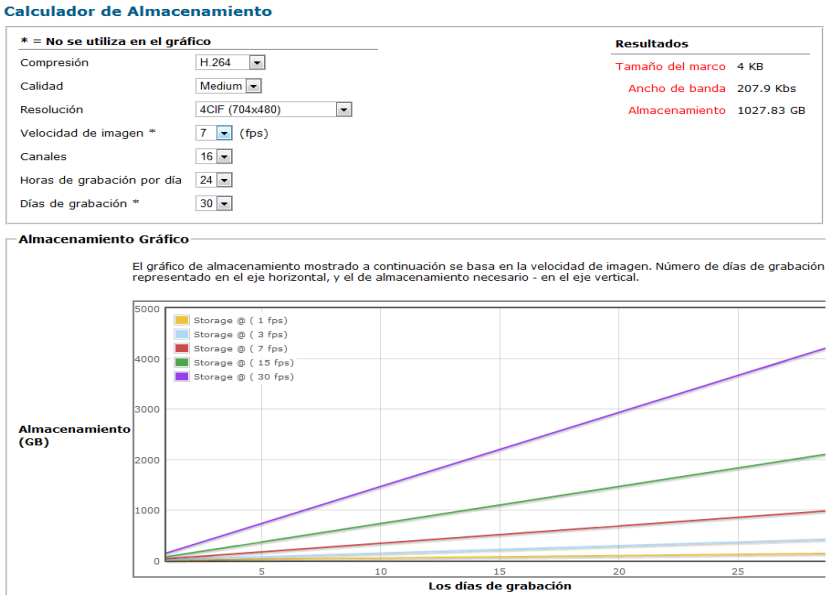


Fig. 6.60 Cálculo de almacenamiento 2

Elaborado por el investigador

Como podemos observar el espacio en disco disminuye considerablemente aumentando la capacidad a 2 meses continuas de grabación aproximadamente, por lo cual se escoge este formato para las cámaras que no representen mayor índice de uso durante los periodos de grabación.

- **Configuración de grabación**

Se detallan los paso para la configuración avanzada de grabación la cual será la usada en el hotel Destiny.

- Haga clic con el botón derecho para visualizar el menú principal y seleccione “CONFIGURACIÓN AVANZADA” > “GRABACIÓN”.
- No modifique la fecha o la hora de su DVR después de que haya activado la función de grabación. De lo contrario, los datos grabados estarán desordenados y no podrá encontrar dichos archivos a través de la búsqueda por tiempo.

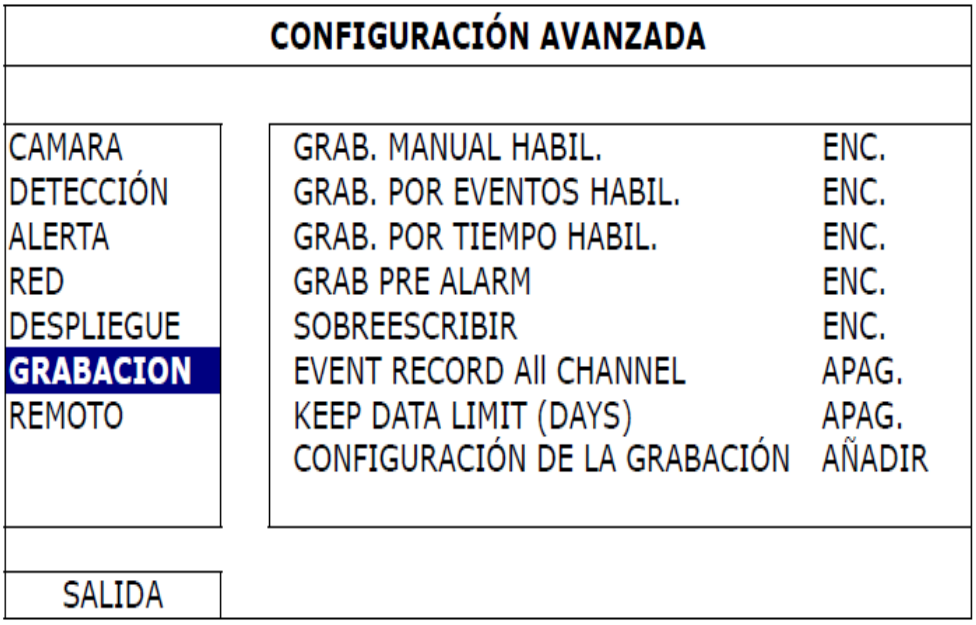


Fig. 6.61 Configuración de grabación

Fuente: Manual DVR AVTECH

- Cuando las funciones de pre-alarma y de grabación por eventos estén activadas, el DVR grabará un archivo de 8 MB antes de que un evento de disparo por alarma por movimiento sea activado.
- Configuramos el tamaño de imagen y los demás parámetros

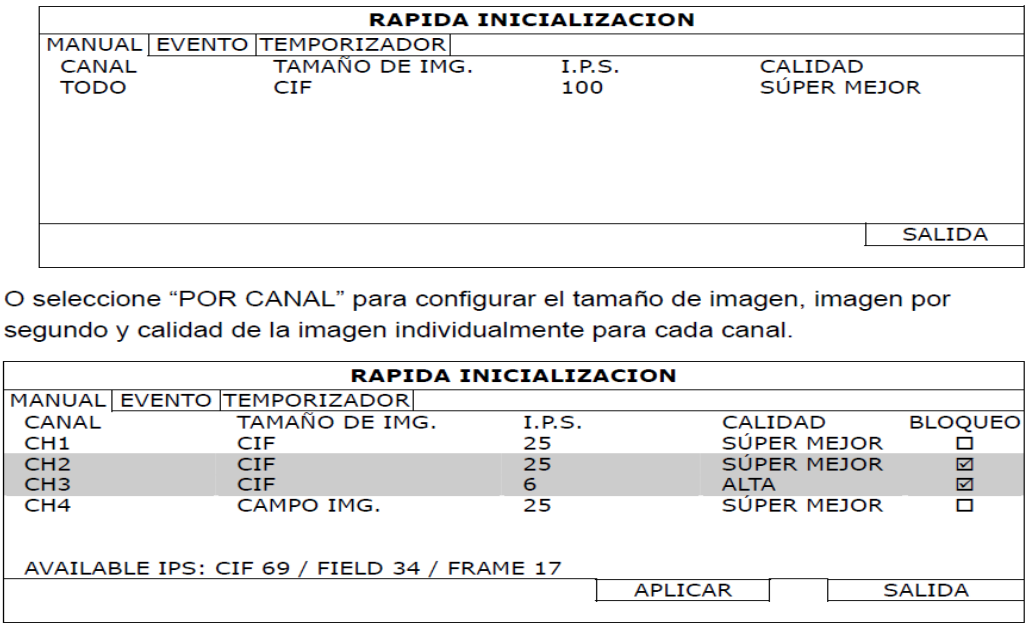


Fig. 6.62 Configuración de requerimientos CCTV

Fuente: Manual DVR AVTECH

La IPS (imagen por segundo) asignada en cada tamaño de imagen para el DVR está fijada. Cuando se esté asignando la IPS para cada canal, seleccione "BLOQUEO" para recordar los IPS restantes de los tamaños de cada imagen disponibles para el resto de los canales.

- **Configuración de detección de movimiento**

  Esta configuración se aplica para las cámaras que se indicó con anterioridad detalladamente según su zona.

  - Haga clic con el botón derecho para visualizar el menú principal y seleccione "CONFIGURACIÓN AVANZADA" > "DETECCIÓN".

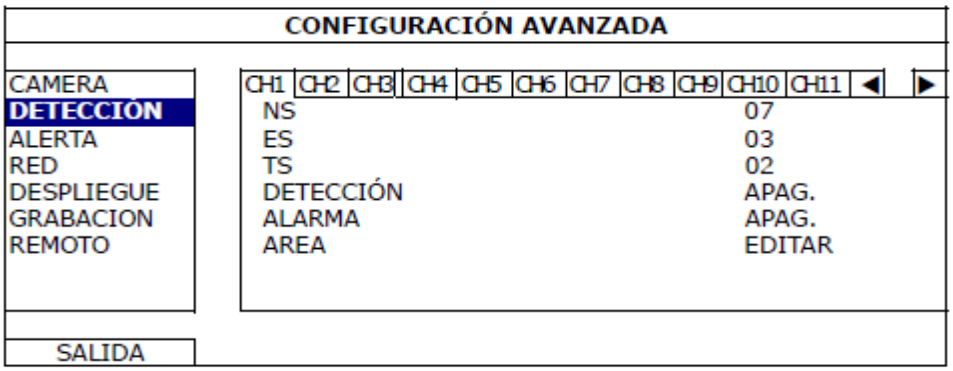


Fig. 6.63 Configuración de detección de movimiento

Fuente: Manual DVR AVTECH

- **NS (Nivel de sensibilidad):** "NS" sirve para configurar la sensibilidad al comparar dos imágenes diferentes. Cuanto menor es el valor, mayor será la sensibilidad de la detección de movimiento. El valor de mayor sensibilidad corresponde al 00 y el de menor al 15. El valor por defecto es el 07.
- **ES (Sensibilidad Espacial):** "ES" sirve para configurar la sensibilidad al detectar el tamaño de un objeto (el número de electrodos) en la pantalla. Cuanto menor es el valor, mayor será la sensibilidad de la detección de movimiento. El valor de mayor sensibilidad corresponde al 00 y el de menor al 15. El valor por defecto es el 03
- **TS (Tiempo de sensibilidad):** "TS" sirve para configurar la sensibilidad sobre el tiempo que permanece un objeto en el área de detección hasta activar la grabación. Cuanto menor es el valor, mayor será la sensibilidad de la detección de movimiento. El valor de mayor sensibilidad corresponde al 00 y el de menor al 15. El valor por defecto es el 02.
- **DETECCIÓN:** Seleccione esta opción si desea activar la función de detección de movimiento en el canal seleccionado (ENC. / APAG.).
- **ALARMA:** Seleccione N.C. / N.O dependiendo de sus necesidades de instalación. El valor por defecto para la alarma es APAG.
- **ÁREA:** Haga clic en "EDITAR" para programar el área de detección de movimiento. Existen rejillas de 16 x 12 por cámara en todos los canales. Los bloques rosados representan un área que no está siendo detectada, mientras que los bloques transparentes son áreas detectadas.

- **Ajustes de red y acceso remoto**

El acceso remoto se lo puede hacer desde diferentes dispositivos como celulares, tabletas, palms, etc. El software de acceso tiene un costo para estos dispositivos una vez hecha la descarga se realizan los pasos que indiquen cada una de las aplicaciones, para acceder mediante computador se debe realizar los siguientes pasos que indica el manual para manera más detallada consultar el mismo.

La siguiente descripción solo es para el tipo de red Estática:

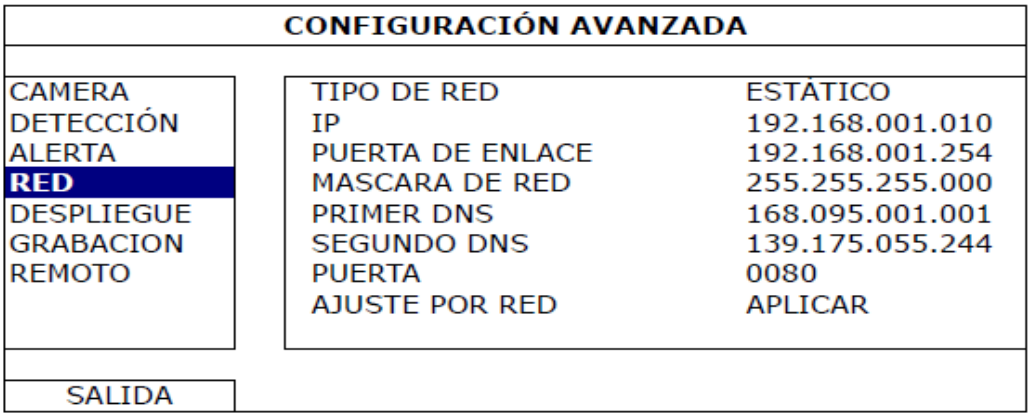


Fig. 6.64 Programación de DVR para visualización en red

Fuente: Manual DVR AVTECH

- **TIPO DE RED:** Seleccione el tipo de red ESTÁTICO y configure toda la información necesaria en el DVR.
- **INFORMACIÓN DE RED (IP / PUERTA DE ENLACE / MASCARA DE RED):** Introduzca toda la información de red que le suministre su proveedor de servicios de Internet.
- **DNS (PRIMER DNS / SEGUNDO DNS)** Introduzca la dirección IP del servidor de nombres de dominio que le ha entregado su proveedor de servicios de Internet).
- **PUERTA:** El número válido está comprendido entre el 1 y el 9999. El valor predeterminado es 80. Generalmente, el puerto TCP utilizado por HTTP es el 80. Sin embargo, en algunos casos es mejor modificar el número de puerto para mejorar la flexibilidad o la seguridad.
- **AJUSTE POR RED** Pulse "APLICAR" para confirmar la configuración

- **Visualización remota**
  - Introduzca la dirección IP que utilice su DVR en el cuadro de dirección URL, por ejemplo 60.121.46.236, y pulse ENTRAR. El sistema le pedirá que introduzca su nombre de usuario y su contraseña para acceder al DVR.
  - Si el número de puerto de su DVR no es 80, necesitará introducir además el número de puerto. El formato es dirección ip: num puerto. Por ejemplo, si la dirección IP es 60.121.46.236 y el puerto es el 888, introduzca en "http://60.121.46.236:888" la barra de dirección URL y pulse "Enter"

- Paso 2: Introduzca el nombre de usuario y la contraseña similares a las utilizadas en el inicio de sesión de Video Viewer y haga clic en “OK” Podrá ver una pantalla similar a la siguiente

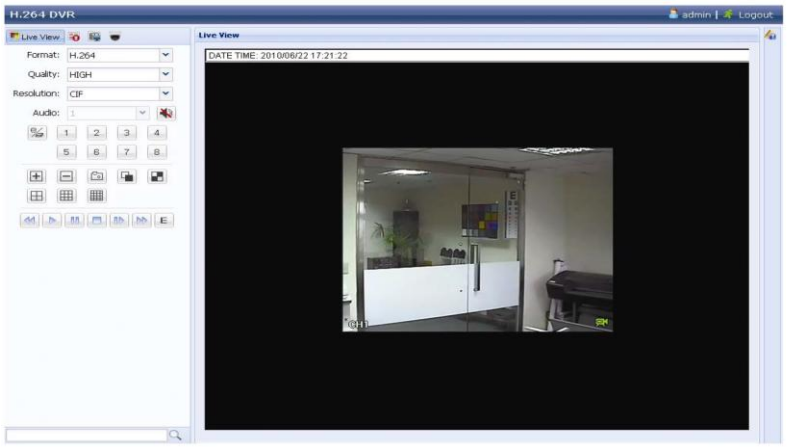


Fig. 6.65 Visualización remota DVR

Elaborado por el investigador

Con esto se da por concluido la configuración de equipos de equipos de control de acceso y video vigilancia, todos los equipos de video vigilancia están en espera de la terminación de la obre interna para su instalación y funcionamiento.

Cualquier duda en cuanto al funcionamiento y configuración faltante de equipos en la bibliografía se encuentran los enlaces directos a las configuraciones.

6.8.4 Propuesta económica

La propuesta económica se realiza en base a los datos reales, de la compra de equipos y puesta en funcionamiento los cuales se detallan a continuación.

- Asignación de presupuesto

El presupuesto asignado por parte de los propietarios para proyecto: **CONTROL DE ACCESO PARA LA DOTACIÓN DE SEGURIDAD EN DORMITORIOS Y ÁREAS RESTRINGIDAS EN EL HOTEL** DESTINY se presenta en la siguiente tabla con una variante de un 10% de imprevistos.

	Control de accesos	Video vigilancia
Presupuesto	$ 18.000,00 + 10%	$ 6.000,00 + 10%
Total	$ 26.400,00	

Tabla 6.32 Presupuesto asignado para el proyecto

Elaborado por el investigador

A continuación se detallan los costos que fueron cubiertos en cada una de las partes de la propuesta.

- **Control de acceso**

La empresa encargada de la distribución de los equipos del sistema de control de acceso fue CETA los cuales contemplan los siguientes puntos.

  - Importación y venta de equipos de control de acceso
  - Instalación física de equipos de control
  - Capacitación sobre uso y funcionamiento de equipos de control

Una vez asignado el presupuesto se realizó la compra de los siguientes equipos.

COSTO EQUIPOS				
Ítem#	Cant.	Descripción	Precio u.	Precio total
01	38	Cerraduras Kaba E 790-K Acabado: Satín Cromo	$295,00	$11.210,00
02	06	Lectores Kaba exos para ascensor	$100,00	$600,00
03	01	FDU (Computadora compacta)	$1.750,00	$1.750,00
04	01	Cable de programación	$130,00	$130,00
Subtotal				$13.690,00
(+)12% I.V.A.				$1.642,80
TOTAL				$15.332,80

Tabla 6.33 Costo equipos control de accesos

Elaborado por el investigador

COSTO MATERIALES PARA EL FUNCIONAMIENTO				
Ítem#	Cant.	Descripción	Precio u.	Precio total
01	250	Tarjetas huésped (Logo Ilco)	$0,95	$237,50
02	25	Tarjetas Personal (logo Ilco)	$1,40	$35,00
03	05	Tarjetas auditor (Logo Ilco)	$2,30	$11,50
04	01	Kit de herramientas Kaba	$150,00	$150,00
Subtotal				$434,00
(+)12% IVA				$52,08
TOTAL				$486,08

Tabla 6.34 Costo materiales control de accesos

Elaborado por el investigador

INSTALACIÓN Y CONFIGURACIÓN				
Ítem#	Cant.	Descripción	Precio u.	Precio total
01	38	Instalación cerradura y corrección de fallas de puertas	$25,00	$950,00
02	06	Instalación lectora ascensor	$15,00	$90,00
03	44	Configuración de cerraduras y lectoras ascensor	$2,00	$88,50
04	01	Configuración FDU y puesta en marcha del sistema	$150,00	$150,00
Subtotal				$1278,50
(+)12% IVA				$153,42
TOTAL				$1.431,92

Tabla 6.35 Costo instalación sistema de control de accesos

Elaborado por el investigador

INVERSIÓN TOTAL	
COSTO DE EQUIPOS	$13.690,00
COSTO DE MATERIALES	$434,00
INSTALACIÓN Y CONFIGURACIÓN	$1278,50
Subtotal	**$15.402,50**
(+)12% IVA	**$1.848,30**
TOTAL	**$17.250,00**

Tabla 6.36 Inversión total control de accesos

Elaborado por el investigador

- **Video vigilancia CCTV**

La empresa encargada de la distribución de los equipos del sistema de control de acceso fue IMPOMAX los cuales contemplan los siguientes puntos.

  - Venta de equipos de video vigilancia
  - Instalación física de equipos de video vigilancia
  - Capacitación sobre uso y funcionamiento

Los demás ítems de instalación de cableado son realizados por el encargado del cableado eléctrico del hotel.

Una vez asignado el presupuesto se realizó la compra de los siguientes equipos.

COSTO EQUIPOS				
Ítem#	Cant.	Descripción	Precio u.	Precio total
01	02	DVR 16 CH AVTECH AVC798PV	$750,00	$1.500,00
02	03	Cámara HAWELL tipo tubo HD 520 TVL	$75,00	$225,00
03	26	Cámara HAWELL tipo domo SD 420 TVL	$50,00	$1.300,00
04	04	Disco duro Samsung 1 Tb 5400 RPM	$130,00	$520,00
05	02	Monitor led AOC 23 pulgadas Slim	$180,00	$360,00
Subtotal				$3.905,00
(+)12% IVA				$468,60
TOTAL				$4373,60

Tabla 6.37 Costo equipos sistema de video vigilancia

Elaborado por el investigador

COSTO MATERIALES				
Ítem#	Cant.	Descripción	Precio u.	Precio total
01	01	Rollo de 305 metros cable nexxt UTP cat6	$175,00	$175,00
02	30	Video Balun Pasivo, Un Par BNC UTP Cat6 400 Mt	$8,00	$240,00
03	30	Adaptadores de Voltaje HAWELL 12 Vcd 2 Amp	$8,00	$240,00
04	01	Kit de herramientas	$50,00	$50,00
05	30	Cajas de pared para voltaje	$3,00	$90,00
Subtotal				$795,00
(+)12% IVA				$95,40
TOTAL				$890,40

Tabla 6.38 Costo materiales video vigilancia

Elaborado por el investigador

INSTALACIÓN Y CONFIGURACIÓN				
Ítem#	**Cant.**	**Descripción**	**Precio u.**	**Precio total**
01	30	Puntos de instalación de cable UTP y voltaje	$10,00	$300,00
02	7	Instalación de puntos control cada piso hacia el cuarto de equipos	$20,00	$140,00
03	30	Instalación física de cámaras y calibración.	$15,00	$450,00
04	01	Configuración DVR y puesta en marcha del sistema de video vigilancia	$100,00	$100,00
Subtotal				$990,00
(+)12% IVA				$118,80
TOTAL				$1.108,8

Tabla 6.39 Costo instalación de video vigilancia

Elaborado por el investigador

INVERSIÓN TOTAL	
COSTO DE EQUIPOS	$3.905,00
COSTO DE MATERIALES	$795,00
INSTALACIÓN Y CONFIGURACIÓN	$990,00
Subtotal	**$5.690,00**
(+)12% IVA	**$682,80**
TOTAL	**$6372,80**

Tabla 6.40 Inversión total sistema de video vigilancia

Elaborado por el investigador

- **INVERSIÓN TOTAL EN EL PROYECTO**

INVERSIÓN TOTAL	
REQUERIMIENTO	**Costo**
CONTROL DE ACCESOS	**$17.250,00**
SISTEMA DE VIDEO VIGILANCIA	**$6.372,80**
TOTAL	**$23.622,80**
PRESUPUESTO	**$26.400,00**

Tabla 6.41 Inversión total en el proyecto

Elaborado por el investigador

Como podemos ver la inversión del proyecto está dentro del presupuesto establecido por los propietarios, la correcta elección de empresas distribuidoras y equipos, hace que la inversión cumpla los requerimientos establecidos, incluso existe un ahorro de $2.777,20, lo cual indica que el proyecto es todo un éxito.

6.9 Conclusiones y recomendaciones

6.9.1 Conclusiones

- La tecnología de control de accesos autónoma brinda todas las características necesarias que se establecen en los parámetros de funcionamiento del hotel y su puesta en funcionamiento.
- El sistema de control de accesos y su correcta distribución crea un ambiente seguro tanto para trabajadores como huéspedes.
- El fácil uso de los dispositivos de control de acceso permite que los empleados realicen sus actividades en un menor tiempo y los huéspedes sientan la confianza necesaria para su estadía
- La correcta elección de equipos de control de acceso Kaba permitieron conocer el producto, que mantiene un alto prestigio a nivel nacional e internacional con soporte y servicio técnico
- Una sola tarjeta de personal puede dar acceso a más de 30 habitaciones, bodegas y otros, evitando el uso innecesario de llaves y ahorrando el costo que representa el cambio de cerradura en caso de pérdida.
- El sistema cuenta con un proceso de verificación de ingreso de personal, en caso exista perdida de pertenecías u objetos se realiza una auditoria de ingreso que se respalda con el sistema de video vigilancia.
- El sistema de video vigilancia respalda el control de acceso en todo sentido, gracias a su configuración y distribución se puede acceder al momento preciso si se rompe las reglas de seguridad
- Gracias al potente almacenamiento de los dispositivos de video vigilancia se puede almacenar 2 meses continuos de grabación que permitirá la revisión permanente en caso se susciten actos delictivos.
- La inversión del proyecto está dentro del presupuesto establecido lo cual es satisfactorio para los propietarios, que vieron con buenos ojos los beneficios y características a corto y largo plazo que presenta el proyecto

6.9.2 Recomendaciones

- Antes de realizar cualquier tipo de inversión en equipos de control de acceso o seguridad, es necesaria la visita a lugares que tengan implementados dichos sistemas para su conocimiento
- Buscar empresas que realicen distribución directa de equipos y dispositivos antes de la compra, ya que estas representan un gran ahorro
- Para la implementación de un proyecto de gran magnitud, reunir a los encargados de construcción, cableado y otros para que no exista desacuerdos al momento de realizar cualquier modificación a la infraestructura física
- En los hoteles es necesario contar con sistemas electrónicos de uso agradable que permitan la fácil interacción entre el equipo y el operador
- Es necesario preservar la vida útil de los equipos con mantenimientos periódicos y capacitación de uso en caso de emergencias
- Contar con un respaldo eléctrico en caso de corte, esto ayudara a que el sistema no sufra desperfectos
- Realizar revisión de pilas semanalmente en las cerraduras para que no exista perdida de información
- Capacitar al administrador para el uso básico de todos los sistemas electrónicos en caso de des configuración llamar al soporte técnico
- Realizar respaldos permanentes de la información que se catalogue como importante para el hotel
- En caso de violación de seguridad ponerse en contacto con el guardia o encargado de la seguridad del hotel

6.10 Bibliografía

6.10.1 Libros, manuales, folletos

- OLIVA, N. CASTRO MA. (2006). Sistema de cableado estructurado, Primera edición
- TESIS DE ELECTRÓNICA; tema: Sistema de video vigilancia mediante cámaras IP, autor: Walter Urrutia, año 2011
- TESIS DE ELECTRÓNICA; tema: Red de video vigilancia mediante cámaras Ip, autor: Eugenia Laura, año 2011
- **MARTORELL MANUEL, Control de Accesos**
- MCGRAW-HILL, -Media Osborne, Redes de computadoras
- Manual de Referencia FDU Kaba Nueva Generación
- Control de accesos – todo sobre control de accesos, 2011, Ing. Luis Cosentino consultor independiente RNDS
- Técnica de vídeo IP. - Axis Communications - 2006-2009
- Ilco Solutions Access control for the hotels 2011
- Central Management System (CMS) USER MANUAL DVR
- H.264 Network DVR
- EagleEyes For Mobile surveillance

6.10.2 Fuentes de internet

Control de accesos

- https://www.provisualusa.com/es/productos/access-control/8
- http://www.scssa.com.ar/control-de-acceso.htm
- http://www.tecnycomp.com.ec/index.php?option=com_content&view=article&id=255&Itemid=90
- http://www.directindustry.es/prod/came-cancelli-automatici/sistemas-de-control-de-acceso-centralizados-18723-411035.html
- http://www.kaba.es/
- http://www.kaba-ilco.com/lodging-systems
- http://rnds.com.ar/
- http://ceta.com.ec/serraduras.html

- http://www.kaba.es/Productos-y-soluciones/22612/cerraduras-de-hotel.html
- http://www.kaba.es/Aplicaciones/Hoteles/22648/kaba-messenger.html
- http://www.articulosinformativos.com.mx/Sistemas_de_Control_de_Acceso-a854249.html#8063374
- http://repo.uta.edu.ec/handle/123456789/16
- http://tecnoseguridad.netii.net/introduccion/81/
- http://www.paph-oea.com/seguridad/marco_concephotel.htm
- http://www.softwareseguridad.com/
- http://www.consultoresml.com/
- http://www.atiempo.com.ec/
- http://www.kaba-ilco.com/lodging-systems/en/Products-Solutions/Access-Control-Systems/294430/frontsk-unit.html

Video vigilancia

- http://blogdeseguridad.com/?p=135
- http://netpointdeargentina.blogspot.com/2010/04/cctv-ip-o-analogico.html
- http://www.sistemasdeseguridad.com.ec/?tabid=6
- http://www.cctvhw.com/english/index.php
- http://www.accesor.com/esp/art2_query.php?fam=5
- http://www.avtech.com.tw/
- http://es.scribd.com/doc/51863053/29/MEDIOS-DE-TRANSMISION-NO-GUIADOS
- http://probo69.blogspot.com/2010/02/cctv-analogo-vs-ip.html
- http://www.2mcctv.com/blog/2011_05_13-hd-cctv-vs-megapixel-ip/
- http://rowantechnologies.com.mx/blog/?p=37
- http://www.sistemasdeseguridad.com.ec/
- http://www.axis.com/es/products/video/about_networkvideo/bandwidth.htm
- http://www.i3international.com/es/storagecalculator.html

ANEXOS

Anexo 1 Características DVR

AVTECH

EagleEyes for Mobile Surveillance
Official Website : www.eagleeyescctv.com
Video Demo : www.eagleeyescctv.com/video
Facebook : www.eagleeyescctv.com/facebook

AVC798PV

16CH H.264 DVR

USB Mouse Control with GUI Display

PUSH VIDEO

FEATURES

Push Video - Active Event Notification with EagleEyes App

- Supports sending Push Video to your iPad, iPhone and Android mobile device for instant event notification for an alarm event when an alarm sensor is connected to the DVR.

Mobile Surveillance with EagleEyes App

- Compatible with many popular mobile devices, such as iPhone, iPad, BlackBerry, Windows Mobile, Symbian & Android mobile devices.

Remote Surveillance with Browsers and CMS

- For web browsers, compatible with Internet Explorer, Mozilla Firefox, Google Chrome, Safari & Opera.
- For CMS software, available with our self-developed and free software, "Video Viewer.
- Applicable also to Apple's media player, QuickTime.

High Performance Design

- Definable "Resolution" / "Quality" / "IPS" by channels at your preferences to increase the recording efficiency, and avoid any important scenes to be missed.

Video Output

- Supports video output for both composite & VGA simultaneously.
- Support VGA resolution output up to 1600 x 1200.

Intelligent Motion Recording

- Only the channel with an event will be recorded to effectively save a significant amount of hard disk space and have the maximized recording time.
- Supports pre-alarm recording.

Remote Independent Operation

- Channel switching is independent from the local site, allowing users to have private image monitoring remotely.

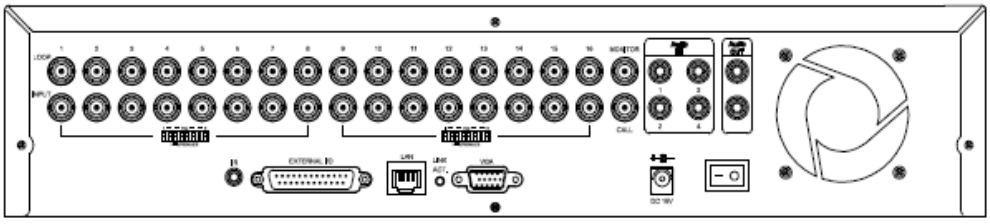
Multiplex

- Allows live display, record, playback, backup and network operation at the same time.

Backup Function

- Supports DVD writer (optional), USB flash drive and network backup.

REAR PANEL



AVTECH

EagleEyes for Mobile Surveillance
Official Website : www.eagleeyescctv.com
Video Demo : www.eagleeyescctv.com/video
Facebook : www.eagleeyescctv.com/facebook

SPECIFICATIONS

Video System		NTSC / PAL (auto detection)
Video Compression Format		H.264
Video Input		16 channels (Composite video signal 1 Vp-p 75Ω BNC)
Video Loop Output		16 channels (Composite video signal 1 Vp-p 75Ω BNC)
Video Output (BNC)	Main Monitor	For stable display
	Call Monitor	For sequence display
Video Output (VGA)		Built-in (Output resolution up to 1600 x 1200)
Audio Input / Output		4 audio inputs, 2 audio output (Mono)
Maximum Recording Rate	Frame	704×480 pixels with 120 IPS <NTSC> / 704×576 pixels with 100 IPS <PAL>
	Field	704x240 pixels with 240 IPS <NTSC> / 704×288 pixels with 200 IPS <PAL>
	CIF	352×240 pixels with 480 IPS <NTSC> / 352×288 pixels with 400 IPS <PAL>
Image Quality Setting		SUPER BEST / BEST / HIGH / NORMAL
Hard Disk Storage		Accommodates 2 SATA HDDs (1 HDD capacity up to 2TB)
Quick Search		Time / Motion / Alarm search mode
SATA Interface		Built-in
Recording Mode		Manual / Timer / Motion / Alarm / Remote
Multiplex Operation		Live display / record / playback / backup / network operations
USB Mouse Control		YES
Motion Detection Area		16 × 12 grids per channel
Motion Detection Sensitivity		3 adjustable parameters for accurate detection
Pre-alarm Recording		YES
Backup Device		DVD Writer (optional) / USB 2.0 flash drive / Network
Web Transmitting Compression Format		H.264
Ethernet		10/100 Base-T. Supports remote control and live view via Ethernet
Mobile Surveillance		YES (Including iPad, iPhone, BlackBerry, Windows Mobile, Symbian & Android)
Remote Surveillance (Operating System: Windows 7 / Vista / XP)	CMS:	Our self-developed and free software, "Video Viewer"
	Web Browser:	Internet Explorer, Mozilla Firefox, Google Chrome, Safari & Opera
	Media Player:	QuickTime
	Max. on-line user:	10
Network Protocol		TCP/IP, PPPOE, DHCP and DDNS
Remote Independent Operation		YES
Remote Event Download & Playback		YES
Event Notification		Push Video / FTP / E-Mail
R.E.T.R. (Remote Event Trigger Recording)		YES
IR Remote Control		YES (IR receiver built-in)
Picture Zoom		2X digital zoom
PTZ Control		YES
Alarm I/O		16 inputs, 1 output
Key Lock (Password Protection)		YES
User Level		Administrator & Operator
Video Loss Detection		YES
Camera Title		Supports up to 12 letters
Video Adjustable		Hue / Saturation / Contrast / Brightness
Date Display Format		YY/MM/DD, DD/MM/YY & MM/DD/YY
Daylight Saving		YES
Power Source (±10%)		DC 19V
Power Consumption (±10%)		< 64 W
Operating Temperature		10℃ ~ 40℃ (50℉~104℉)
Dimensions (mm)**		432(W) × 90(H) × 326(D)
System Recovery		System auto recovery after power failure
Optional Peripherals		Keyboard Controller

*The specifications are subject to change without notice.
** Dimensional tolerance: ±5mm

Anexo 2 Características adicionales manual de referencia FDU

Tarjetas

El FDU puede codificar dos tipos de tarjetas: de banda magnética o Mifare (ISO 14443), y tarjetas para la cerradura de proximidad 790.

Tarjetas de banda magnética

Disponibles en Alta y Baja Coercitividad. Las tarjetas de Alta Coercitividad son ligeramente más caras pero son menos propensas a desmagnetizarse. La auditoría no se almacena. Los Hoteles pueden tener ya sea codificación de Alta coercitividad o de Baja coercitividad pero no ambos.

Tarjetas de proximidad Mifare

Disponibles en versiones Mini, de1K o de 4K. Las Mini son las de mayor costo-beneficio por su precio pero no tienen memoria para grabar las auditorías (ideales para los huéspedes). Las tarjetas de 1K tienen la capacidad de almacenar 80 eventos (ideales para las tarjetas del personal). Las tarjetas de 4K tiene la capacidad de almacenar 300 eventos (ideal para realizar auditorías).

La siguiente tabla describe los diferentes tipos de tarjeta que están disponibles y son compatibles con cada cerradura, además de sus usos.

	Capacidad de la cerradura				Uso de la cerradura			
Tipo de Tarjeta	Solitaire 710-II	Generación E-760 Electrónica 770	Proximidad 790	Autorización FDU	Huésped	Acción de la cerradura o Reinicio	Personal	Auditar Cerradura
Tarjeta de banda magnética de Baja Coercitividad	☑	☑		☑	☑	☑	☑	
Tarjeta de banda magnética de Alta Coercitividad	☑	☑		☑	☑	☑	☑	
MIFARE Mini (Huésped)		☑		☑	☑			
MIFARE 1k (Personal)		☑	☑		☑	☑		
MIFARE 4k (auditoría)		☑					☑	☑

7.5 NIP de Administrador

El NIP puede ser utilizado por empleados nuevos o ya existentes si así lo decide el administrador, como una alternativa al uso de tarjeta autorizada.

El NIP es de 4 a 8 dígitos seleccionados por el administrador o el empleado, o puede ser sugerido por el FDU.

Para facilitar el acceso al FDU, un empleado con un NIP podrá acceder al FDU sin su tarjeta autorizada. En lugar del deslizamiento de la tarjeta en la cerradura, el NIP es el acceso utilizando el teclado del FDU.

Tipo de creador	Tipo de usuarios con NIP del FDU permitido
Administrador general	Programador, botones, mostrador, POS
Propietario	Mostrador, POS

1. Deslice una tarjeta autorizada GMA o MA.

   Para la cerradura de proximidad 790, presente una tarjeta de Autorización válida para el FDU sobre el codificador de proximidad externo.

2. Presione 7 para seleccionar la opción "configuración FDU".

3. Presione 2 para seleccionar la opción "características FDU".

4. Presione 5 para seleccionar la opción "NIP de Administrador".

5. Deslice o presente una tarjeta al autorizador de escritorio.

6. El FDU mostrará la Autorización número 55 (ejemplo) y mostrará el número de 1234 (ejemplo) (Nota: Si la tarjeta FDA no tiene un NIP puede asignarlo por una opción de agregar NIP? Opción Sí).

7. Presione la flecha abajo <▼> para modificar NIP? (Nota: usted no necesita modificar el número actual de NIP utilizado. Esta es una característica adicional para cambiar o cancelar el número de NIP si es necesario.

8. Presione la flecha derecha <▶> para cambiar la opción Si/No.

9. Presione la flecha abajo <▼> para Operación.
   Opción 1. Presione 0 para cambiar el número de NIP
   a. Presione la flecha abajo <▼> para cambiar el número de NIP.
   b. Nota: el FDU genera un número de NIP al azar que usted puede utilizar, o incorpora manualmente el nuevo número de NIP. Mínimo de 4 dígitos, máximo de 8 dígitos. Presiona <↵>.

   c. Usted no puede utilizar el número de NIP que recién utilizó, también el FDU le indicará reasignar un nuevo número de NIP. Presione <↵> para confirmar el cambio de NIP.
   d. FDU mostrará: nuevo NIP con éxito. Re-deslice la tarjeta para confirmar los cambios.

   Opción 2. Presione 1 para modificar el número de NIP
   a. Presione <↵>.
   b. Esta característica negará el acceso de FDU usando el número de a la tarjeta autorizada #55 (ejemplo) del mostrador. Sin embargo la tarjeta FDA #55 todavía trabajará en FDU.
   c. Presione <↵> para confirmar el cambio de NIP.
   d. FDU mostrará: NIP modificado con éxito. Re-deslice la tarjeta para confirmar los cambios.

10. Su configuración ha sido registrada.

Capítulo 11 – Mantenimiento Preventivo

11.1 Acciones Semanales

Deslice una tarjeta limpiadora en la unidad de escritorio de 10 a 15 veces una vez por semana.

11.2 Acciones Mensuales

La cubierta de la cerradura se debe limpiar y pulir cada mes con un paño seco y limpio.

No utilice limpiadores químicos ó abrasivos, dañaran el acabado.

La cabeza del lector magnético se debe limpiar cada mes. Simplemente inserte y retire varias veces la tarjeta limpiadora varias veces en cada cerradura. Si sus cerraduras están expuestas a niveles de polvo o sal, o se encuentran en los exteriores su limpieza debe ser mas a menudo (una vez al mes).

11.3 Acciones Semestrales

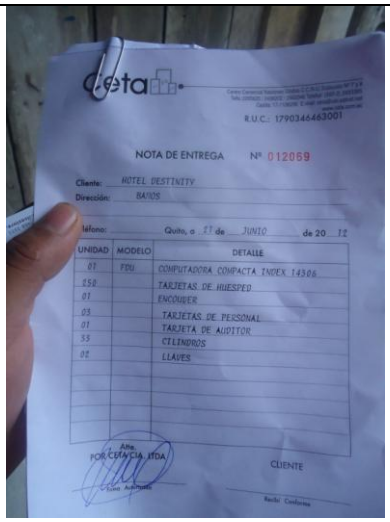
11.3.1 Sincronización de FDUs

Esto es realizar la transferencia de datos de un verificador FDU principal a otro FDU en el hotel. Esto es con la facilidad de que todos los FDUs se establezcan al mismo tiempo, que reconozcan las mismas tarjetas autorizadas y que tengan las mismas características de los ajustes.

1. Nombre las dos unidades de mostrador para distinguir quien recibe los datos (nuevos) y quien envía los datos (FDU viejo o principal).

2. Las características del FDU kaba pueden tener versiones distintas así como el modelo de la nueva generación que puede requerir diversos tipos de cables para la transferencia de FDU a FDU. Si la versión del FDU es desconocida favor de ponerse en contacto con el soporte técnico Kaba.

Anexo 3 Fotos de cerraduras en funcionamiento



NOTA DE ENTREGA Nº 012059

R.U.C.: 1790346463001

Cliente: HOTEL DESTINITY

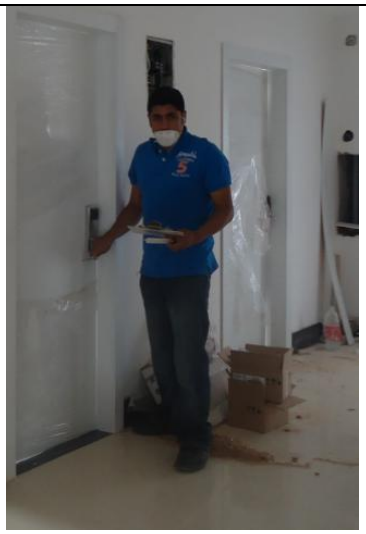
Dirección: BAÑOS

Teléfono: Quito, a 11 de JUNIO de 20 12

UNIDAD	MODELO	DETALLE
01	FDU	COMPUTADORA COMPACTA INDEX 14306
150		TARJETAS DE HUESPED
01		ENCODUER
03		TARJETAS DE PERSONAL
01		TARJETA DE AUDITOR
55		CILINDROS
01		LLAVES

Atte. POR LA COMPAÑIA ITDA

CLIENTE



Anexo 4 Encuesta realizada en la ciudad de Baños

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y COMUNICACIONES
ENCUESTA DIRIGIDA A HOTELES DE LA CIUDAD DE "BAÑOS"

OBJETIVO: El objetivo de la presente encuesta es para recopilar información sobre el deficiente control de acceso en dormitorios y áreas restringidas que presentan los distintos establecimientos dentro del perímetro central.

INSTRUCCIONES: Se solicita de la manera más comedida se sirva llenar la presente encuesta marcando una X en el lugar de la respuesta que a su criterio es la conveniente.

¿Cómo califica usted la seguridad en el interior de los dormitorios y áreas restringidas de su establecimiento?

- Excelente ☐ Buena ☐ Regular ☐

¿Conoce usted algún tipo equipo o software (programa) de seguridad para el control y supervisión de personas que se hospedan en su establecimiento?

- Si ☐
- No ☐

¿Al momento del ingreso de huéspedes usted solicita algún tipo de identificación para el registro del mismo?

- Si ☐
- No ☐

¿Estaría dispuesto a tomar medidas de seguridad implementando equipos de control de acceso en su establecimiento?

- Si ☐
- No ☐

¿Realiza usted una supervisión semanal o mensual de los objetos en cada habitación y área restringida después del ingreso del personal de aseo o de los huéspedes?

- Si ☐
- No ☐

¿Dentro de su establecimiento el personal dedicado al resguardo de la seguridad es?

- Suficiente ☐
- Poco ☐
- Insuficiente ☐

¿En el interior de su establecimiento y los alrededores se han suscitado actos delictivos?

- Sí ☐
- No ☐

¿Considera usted que la seguridad es importante para la reputación de su establecimiento?

- Si ☐
- No ☐

GRACIAS POR SU COLABORACIÓN

Anexo 5 Entrevista propietarios y encargados

PREGUNTA 1: ¿En el diseño de la edificación que criterios técnicos se consideraron para dotar de seguridad al edificio?

PREGUNTA 2: El hotel cuenta con la infraestructura para la instalación de equipos de seguridad.

PREGUNTA 3: En la planificación de la construcción se estableció un cuarto para el control de equipos de seguridad y otros.

PREGUNTA 4: ¿En el interior de áreas restringidas como bodegas y administración se planifico algún tipo de seguridad especial?

PREGUNTA 5: En la edificación se planifico zonas especiales en donde exista concentración de personas.

PREGUNTA 6: En la planificación de recursos tecnológicos se tomó en cuenta un control de acceso a las habitaciones

PREGUNTA 7: En la planificación administrativa el hotel contara o no con un plan de seguridad, para evitar perdida de objetos y robo

PREGUNTA 8: En la planificación del hotel se dispone la instalación de un software especializado en resguardo y seguridad