



PONTIFICIA **UNIVERSIDAD CATÓLICA** DEL PERÚ

Esta obra ha sido publicada bajo la licencia Creative Commons
Reconocimiento-No comercial-Compartir bajo la misma licencia 2.5 Perú.

Para ver una copia de dicha licencia, visite
<http://creativecommons.org/licenses/by-nc-sa/2.5/pe/>



PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA



**DISEÑO DE UN SISTEMA DE CONTROL DE ACCESOS ORIENTADO A UN
EDIFICIO DE OFICINAS EN PROCESO DE AUTOMATIZACIÓN**

Tesis para optar el Título de Ingeniero Electrónico

Presentado por:

LUIS ARIEL NORIEGA CHÁVEZ

Lima - Perú

2007

Resumen

La presente tesis se desarrolla en una empresa estatal del rubro petrolero que tiene como objetivo automatizar su Edificio de Oficinas principal. Se aborda desde la perspectiva del área de proyectos de La Empresa en donde el autor se encuentra laborando durante el desarrollo del presente trabajo.

La problemática se basa en la necesidad que tiene La Empresa de automatizar su Edificio de Oficinas Principal debido a la inversión que trae la Ley de Modernización de dicha empresa. En particular, en la presente tesis se aborda El Sistema del Control de Accesos como problemática a resolver siendo parte de la problemática global de la automatización del edificio.

El objetivo de la tesis es realizar el diseño del Sistema de Control de Accesos en el edificio de La Empresa que se encuentra en proceso de automatización. Se tiene siempre en cuenta la necesidad de que el Sistema debe estar preparado para integrarse con los demás sistemas del edificio que se instalarán en un futuro.

Para cumplir con el objetivo se llevan a cabo reuniones con los Departamentos de La Empresa que presentan requerimientos en el Sistema, tales como Recursos Humanos y Seguridad Integral, así como con las empresas especializadas en el rubro de Automatización de Edificios que en este caso desempeñan la función de expertos en el tema y actúan como consultores.

Finalmente, se realiza la selección del Sistema que mejor responde a las necesidades de La Empresa y se hace un análisis de los costos de estos equipos.

FACULTAD
DE CIENCIAS
E INGENIERÍA

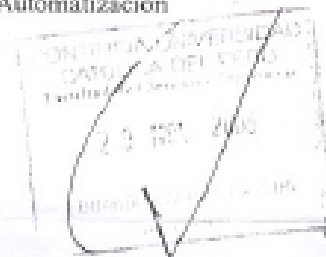


90
AÑOS

PONTIFICIA
UNIVERSIDAD
CATÓLICA
DEL PERÚ

TEMA DE TESIS PARA OPTAR EL TÍTULO DE INGENIERO ELECTRÓNICO

Título : Diseño de un Sistema de Control de Accesos Orientado a un Edificio de Oficinas en Proceso de Automatización
 Área : Comunicaciones * 4 0 0
 Asesor : Angelo Velarde
 Alumno : Luis Ariel Noriega Chávez
 Código : 20022127
 Fecha : 27 de noviembre de 2006



Descripción y Objetivos

La presente tesis tiene como objetivo realizar el diseño de un Sistema de Control de Accesos en un edificio de oficinas en proceso de automatización. El diseño debe contemplar los requerimientos de la empresa y además el hecho de que el proceso de automatización implica que el sistema ha diseñarse debe integrarse con los demás sistemas electrónicos del edificio, tales como Sistema de Control de Incendios, de Circuito Cerrado de Televisión, entre otros.

Para cumplir con este objetivo se ha llevado a cabo un proceso de investigación sobre el tema de edificios automatizados para poder tener una visión clara en donde será instalado el sistema que se diseñará.

Luego, se han llevado a cabo reuniones periódicas con los Departamentos de la Empresa que opera en el edificio. Como resultado de estas reuniones, y en concordancia con lo que ofrece el mercado en este rubro, se elaboró el documento de requerimientos de la Empresa, que ha servido como base en el diseño del sistema.

Luego de realizar el diseño, se presenta un presupuesto detallado de los componentes que están involucrados.

Finalmente, se presentan las recomendaciones para la instalación y recomendaciones para futuras mejoras del sistema.

MAXIMO: 100 PÁGINAS

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
FACULTAD DE CIENCIAS Y DE INGENIERÍA

ING. ANDRÉS FLORES ESPINOZA
Decano Incauto de la Especialidad de Ingeniería Electrónica

FACULTAD
DE CIENCIAS
E INGENIERÍA



90
AÑOS

PONTIFICIA
UNIVERSIDAD
CATÓLICA
DEL PERÚ

TEMA DE TESIS PARA OPTAR EL TÍTULO DE INGENIERO ELECTRÓNICO

Título : Diseño de un Sistema de Control de Accesos Orientado a un Edificio de Oficinas en Proceso de Automatización

Índice

Introducción

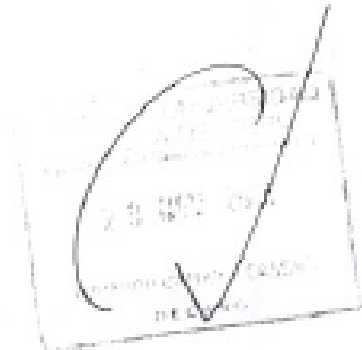
1. Análisis de la situación actual de Empresa.
2. Análisis del Sistema de Control de Accesos.
3. Determinación de los requerimientos de la Empresa.
4. Diseño del Sistema de Control de Accesos.

Conclusiones

Recomendaciones

Bibliografía

Anexos



PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
SECCIÓN DE ELECTRICIDAD Y ELECTRÓNICA

Ing. ANDRÉS FLORES ESPINOSA
Coordinador de la Especialidad de Ingeniería Electrónica

Índice

Capítulo 1

Análisis de la situación actual de Empresa.

1.1. Presentación.	1
1.2. Edificios inteligentes en el mundo.	1
1.3. Edificios inteligentes en el Perú.	2
1.4. El Edificio de Oficina Principal de La Empresa en la Actualidad.	3
1.4.1. Infraestructura	3
1.4.2. Sistemas electrónicos con los que cuenta el edificio en la actualidad	4
1.4.3. Manejo actual de la seguridad en La Empresa	5
1.4.4. Personal de La Empresa	6
1.5. Situación actual de La Empresa.	6
1.5.1. Ley de Modernización y fortalecimiento de La Empresa.	7

Capítulo 2

Análisis del Sistema de Control de Accesos.

2.1. Automatización de Edificios: Edificio Inteligente.	13
2.2. Sistemas usados en el diseño de Edificios Inteligentes en la actualidad.	13
2.2.1. Sistemas de Evacuación y Perifoneo.	14
2.2.2. Circuito Cerrado de Televisión CCTV.	15
2.2.3. Sistema de detección y alarma de incendio.	16
2.2.4. Cableado estructurado.	17
2.2.4.1. Fibra Óptica.	17
2.2.4.2. Cable Coaxial.	17
2.2.4.3. Cable UTP .	18
2.2.5. Control de Accesos.	18
2.2.6. Integración.	20
2.3. Situación actual del Sistema de Control de Accesos en La Empresa.	20
2.4. Deficiencias en el actual Sistema de Control de Accesos.	21
2.5. Sistema de Control de Accesos en Edificio de Oficinas en la actualidad.	22
2.5.1. Servidor de Control de Accesos.	23

2.5.2. Controlador Central del Sistema de Control de Accesos.	23
2.5.3. Interfaz de lectoras.	24
2.5.4. Lectoras.	24
2.5.4.1. Lectora de teclado.	24
2.5.4.2. Lectora de proximidad.	25
2.5.4.3. Lectoras biométricas.	25
2.6. Indicadores que permiten conocer la calidad, los grados de mejora que ofrece la instalación de un Sistema de Control de Accesos en un edificio de oficinas.	25

Capítulo 3

Determinación de los requerimientos de La Empresa.

3.1. Objetivo de la tesis.	27
3.1.1. Uso de tecnología moderna.	27
3.1.2. Diseño de sistema distribuido.	27
3.1.3. Diseño de sistema integrable.	28
3.1.4. Cumplimiento de los Requerimientos de La Empresa.	28
3.2. Características deseables del Sistema.	28
3.2.1. Características deseables del Software del Sistema.	29
3.2.1.1. Características basadas en la integrabilidad.	29
3.2.1.2. Características basadas en requerimientos de seguridad.	29
3.2.2. Características deseables del Servidor del Sistema.	30
3.2.2.1. Características basadas en la integrabilidad.	30
3.2.2.2. Características basadas en requerimientos de seguridad.	31
3.2.3. Características de los Paneles Controladores de Lectoras.	31
3.2.3.1. Características basadas en la integrabilidad.	31
3.2.3.3. Características basadas en requerimientos de seguridad.	32
3.2.4. Características de las Lectoras de Proximidad Peatonales.	32
3.2.4.1. Características basadas en la integrabilidad.	32
3.2.4.2. Características basadas en requerimientos de seguridad.	33
3.2.5. Características de las lectoras de proximidad de largo alcance.	33
3.2.5.1. Características basadas en la integrabilidad.	33

3.2.5.2. Características basadas en requerimientos de seguridad.	33
3.2.6. Interfaz Wiegand.	34
3.2.6.1. Características basadas en la integrabilidad.	34
3.2.6.2. Características basadas en requerimientos de seguridad.	34
3.2.7. Barreras vehiculares.	34
3.2.8. Tarjetas de proximidad.	35
3.2.8.1. Características basadas en la integrabilidad.	35
3.2.8.2. Características basadas en requerimientos de seguridad.	35
3.2.9. Integración con el Sistema de Control de Incendios.	35
3.2.10. Baterías para voltaje auxiliar.	36
3.2.11. Accesorios para las puertas.	36

Capítulo 4

Diseño del Sistema de Control de Accesos.

4.1. Introducción.	37
4.2. Selección del Sistema.	37
4.3. Sistema de Control de Accesos seleccionado.	38
4.3.1. El Software del Sistema	38
4.3.1.1. Integración	39
4.3.1.2. Seguridad ideal para empresas del gobierno	39
4.3.1.3. Niveles de alarmas	39
4.3.1.4. Control de los niveles de ocupación de las áreas	40
4.3.1.5. Capacidad de cambiar el comportamiento del sistema en casos de emergencia.	40
4.3.1.6. Interfaz gráfica para manejo de Control de Accesos	40
4.3.2. Selección del servidor del sistema	40
4.3.3. Panel Controlador de Lectoras	42
4.3.3.1. Fácil de configurar con DHCP	42
4.3.3.2. Ofrece una comunicación efectiva cuando trabaja en grupo	42
4.3.3.3. Capacidad para actuar con programación 'Anti-passback'.	43

4.3.3.4. Seguridad en los datos.	43
4.3.4. Lectoras	44
4.3.4.1. Las lectoras peatonales: HID Indala Standard Card Readers	44
4.3.4.2. Las lectoras de largo alcance: HID Indala Long Range Card Readers	44
4.3.5. Interfaz Wiegand: Software House RM-4	45
4.3.6. Software de integración con el CCTV, Software House C CURE NetVue	46
4.3.7. Barreras Vehiculares	47
4.3.7.1. Barrera vehicular de 3 metros: BA 1200 Alta Velocidad.	47
4.3.7.2. Barrera vehicular de 6 metros: BA 7000	48
4.3.8. Tarjetas de Proximidad: HID Indala Flex Card	48
4.3.9. Interfaz de integración con el Sistema Contra Incendios: Software House ACM-8.	49
4.4. Esquema final del sistema.	49
4.5. Ubicación de los equipos	52
4.6. Cableado.	55

Introducción

La automatización edificios consiste en proveer a la construcción de herramientas tecnológicas que faciliten las labores de las personas que trabajan en el lugar, que permitan hacer un mejor uso de los recursos de energía y que proporcionen herramientas que faciliten el control de la seguridad. Este concepto propone la integración de todos los sistemas existentes en el edificio tales como Control de Accesos y Circuito Cerrado de Televisión.

El objetivo de la tesis presentada es realizar el diseño del Sistema de Control de Accesos en un edificio de oficinas en proceso de automatización, teniendo en cuenta los requerimientos de la empresa que labora en el edificio y lo que el mercado ofrece en este tipo de tecnología.

Para cumplir con el objetivo se debe tener en cuenta que el proyecto global es automatizar todo el edificio y que esta automatización se realizará de forma discreta, se diseñarán e instalarán los sistemas uno a uno siempre teniendo en cuenta la necesidad de que al final estos sistemas puedan establecer comunicación entre sí.

El presente diseño busca cubrir las expectativas que presenta La Empresa teniendo en cuenta lo que el mercado ofrece en este tipo de tecnologías.

Debido al carácter confidencial de parte de la información que se declara en este documento se ha considerado conveniente nombrar a la empresa en cuestión como 'La Empresa'.

El documento final se ha dividido en 4 capítulos. A continuación un breve resumen de cada uno:

En el Capítulo 1 se aborda el tema de la automatización de edificios, partiendo desde el punto de vista mundial hasta llegar al peruano. Luego se analiza la situación por la que esta atravesando La Empresa. Al ser una empresa estatal ha sido necesario mencionar y describir normas legales que son necesarias para situar la problemática en su contexto real.

En el Capítulo 2 se aborda el tema del Control de Accesos, se analizan las tecnologías existentes en la actualidad en este tema, aplicados a edificios de oficinas en proceso de automatización. Además se hace un análisis del Sistema con el que La Empresa actualmente cuenta, poniendo énfasis en las deficiencias que muestra. Finalmente se presentan las partes de los Sistemas de Control de Accesos modernos, que será la base para el diseño final.

Luego se aborda el Capítulo 3, en donde se determinan los requerimientos de La Empresa, para el desarrollo de este capítulo se llevaron a cabo reuniones con los Departamentos de La Empresa y con las empresas especializadas en este tipo de sistemas.

Finalmente se presenta el Capítulo 4, en donde se hace la selección del sistema que mejor responde a las necesidades de La Empresa. Se hace un análisis de los costos de los equipos del Sistema y se muestra el metrado del cableado necesario para interconectar todos los equipos.

En las conclusiones se hace un análisis de los principales factores que intervinieron en el desarrollo de la Tesis desde diferentes perspectivas.

CAPÍTULO 1

Análisis de la situación actual de Empresa.

1.1. Presentación.

El desarrollo de la presente tesis se llevó a cabo en una empresa del rubro petrolero del Estado peruano. Muchos de los datos utilizados han sido obtenidos a través de entrevistas con los Departamentos de La Empresa que presentaban requerimientos sobre el Sistema que se diseña en este trabajo.

Antes de entrar al análisis de la situación actual de La Empresa se mostrará cómo se ha venido desarrollando el tema de la automatización de edificios para poder tener una idea clara de lo que La Empresa desea lograr con el suyo.

1.2. Edificios inteligentes en el mundo.

En la actualidad el tema del ahorro de energía se ha vuelto muy importante para todos. La escasez de los recursos no renovables de fuentes de energía, origina que cada vez se busque con mayor vehemencia nuevas formas de ahorro.

Asimismo, a raíz del atentado del 11 de septiembre, nació en el mundo una disposición más marcada a buscar tener la mayor seguridad posible, para poder así minimizar la posibilidad de que vuelvan a ocurrir catástrofes de tal índole.

El tema de Edificio Inteligente adopta las dos premisas anteriores y las integra con otras características más, tales como comodidad y desempeño laboral, para lograr una construcción que pueda cumplir con las expectativas actuales tanto de seguridad, como de buen manejo de la energía.

Las edificaciones de este tipo en el mundo son planeadas desde el momento de su concepción como idea. Teniendo en cuenta factores tales como la posición de las ventanas para maximizar el uso de la luz solar, la construcción de tragaluces tal que puedan dirigir la luz natural a través de toda la construcción, entre otros.

Para ilustrar la idea tomaremos como ejemplo la construcción “El Edificio”, ubicado en España.

Según Rafael Barzanallana, docente de la Universidad de Murcia, “este es el primer Edificio de Oficinas de España totalmente ecológico, electrónico y reciclable, con una estructura abierta al exterior que se beneficia con los elementos ambientales que lo rodean (lluvia, calor, frío, energía solar, etc.) y se cierra a ellos cuando son adversos”.

En este edificio el agua de lluvia se recoge del tejado y se recicla para uso propio, además la energía solar es almacenada a través de paneles para usos diversos. La climatización del edificio se realiza con la ayuda de paneles fríos ubicados en el techo del edificio, que actúan como refrigerantes. Con respecto a la iluminación, esta se activa solo cuando se detecta escasez de luminosidad y hay alguien presente en la habitación. En la Figura 1.1. se aprecia una imagen de El Edificio.

Como se puede apreciar, los Edificios Inteligentes en la actualidad buscan aprovechar al máximo los recursos tecnológicos para poder conseguir ahorrar energía y brindar seguridad y comodidad a las personas que se encuentren en el interior.

1.3. Edificios inteligentes en el Perú.

En el Perú el tema es relativamente nuevo, las construcciones que cuentan con esta tecnología en su mayoría pertenecen a empresas de capitales extranjeros.

El ejemplo más resaltante en Lima posiblemente sea el edificio del Banco Interbank, ubicado en el cruce de la Av. Javier Prado y la Vía Expresa. Este edificio, construido en el 2001, tiene una posición tal que permite a los usuarios utilizar en gran medida la luz solar para desarrollar sus actividades. Cuenta con sistemas electrónicos, tales como Control de Accesos y Circuito Cerrado de Televisión, que son operados a través del centro de control de una manera centralizada. En la Figura 1.2. se muestra una fotografía del edificio.

Figura 1.1. Edificio Inteligente: “El Edificio”



Cortesía de Rafael Barzanallana

La tecnología de Edificios Inteligentes ya está presente en el país. Poco a poco las empresas se están dando cuenta que a largo plazo, la inversión inicial que implica el uso de esta tecnología, se verá reflejada en el ahorro de energía posterior y en una mayor comodidad y seguridad de los empleados, lo que repercutirá en su productividad.

1.4. El Edificio de Oficina Principal de La Empresa en la Actualidad.

1.4.1. Infraestructura

El Edificio de Oficina Principal (OFP) tiene cerca de 30 años de antigüedad, fue construido a raíz de que el edificio donde operaba La Empresa quedó pequeño ante el crecimiento de ésta.

Con sus 23 pisos, es uno de los edificios más altos de la zona empresarial de Lima y pese a su antigüedad, su arquitectura le permite tener un aspecto que no se ve opacado por los edificios modernos construidos recientemente en el lugar.

Sin embargo, a diferencia de estos edificios modernos, cuando OFP fue construido, la tecnología estaba mucho de la actual y no daba indicios de lo que se avecinaba en el tema de automatización de edificios. Por lo tanto, su arquitectura no fue diseñada para alojar sistemas electrónicos ni mucho menos automatizados.

Figura 1.2. Edificio del Banco Interbank.



Cortesía de Skyscrapercity.com

Pese a esto, con el paso del tiempo, al darse toda la revolución tecnológica que hemos y aún seguimos viviendo, el edificio fue dotándose paulatinamente de la tecnología vigente, acoplando los sistemas a la arquitectura de la construcción.

Asimismo, el edificio cuenta con una montante que lo atraviesa desde el Sótano 2 hasta el Piso 22. A través de esta montante se trasladan los cables de telefonía y el cableado estructurado vertical. En cada uno de los pisos se tiene accesos a esta montante para realizar actualizaciones en el cableado telefónico.

1.4.2. Sistemas electrónicos con los que cuenta el edificio en la actualidad

- Red LAN con cableado estructurado de Categoría 5E, cuenta con Switches de última generación con capacidad de manejar VLANS y enrutamiento (capa 3). El cableado vertical se realiza a través de la montante y el horizontal a través de entubados dispuestos en el falso techo.

- Central Telefónica con troncales analógicas y digitales, y con capacidad para manejar telefonía IP. Esta Central se encuentra ubicada en el Sótano 1, en una oficina a cargo del Departamento de Telecomunicaciones. Cuenta con una Estructura de Distribución Principal; MDF, entre la Central Telefónica y la montante.

- Circuito Cerrado de Televisión (CCTV), en los lugares de mayor seguridad como Gerencia General y Presidencia. Las cámaras son manejadas actualmente desde un Centro de Control acondicionado temporalmente en un ambiente del Área de Telecomunicaciones.

- Equipos de Video Conferencia con los cuales La Empresa se mantiene comunicada en todas las Operaciones del Perú. La conexión se realiza en parte por Ethernet y en parte por la red RDSI, contratada para este propósito.

- Tres líneas dedicadas RDSI para ser usadas por los equipos de Video Conferencia. Estas líneas son utilizadas como respaldo de la conexión Ethernet.

- Sistema de Control de Accesos en la entrada principal y los ascensores ejecutivos. Este sistema tiene la opción de emitir reportes de asistencia al Departamento de Recursos Humano, pero al no estar distribuido en todo el edificio uniformemente, no cumple con las expectativas actuales de La Empresa.

- Tercerización del área de Sistemas a cargo de IBM, que se encarga de realizar labores de seguridad, administración y mantenimiento sobre la red LAN. Esta tercerización este supervisada por el Departamento de Telecomunicaciones.

El funcionamiento de todos estos sistemas electrónicos permite a las personas que trabajan en el edificio contar con herramientas suficientes para desempeñar sus labores. Suficientes, pero no óptimas.

1.4.3. Manejo actual de la seguridad en La Empresa

La Empresa cuenta con el Departamento de Seguridad Integral para salvaguardar la seguridad de los ocupantes del edificio. Asimismo, cuenta con personal del Cuerpo de Bomberos de Lima que están siempre pendientes de cualquier emergencia.

Es perceptible que el Departamento de Seguridad Integral no cuenta con las herramientas suficientes para realizar eficientemente sus funciones. La carencia de un

Sistema de Control de Accesos distribuido y moderno y la escasez de Cámaras de Seguridad en el edificio impiden que se pueda tener un control completo del edificio.

Parte del objetivo de la automatización del edificio es brindar a este Departamento las herramientas para que puedan llevar un control óptimo de la seguridad en el edificio.

1.4.4. Personal de La Empresa

En La Empresa actualmente laboran alrededor de 1200 personas en los 23 pisos.

Las personas que laboran en el edificio tienen en su mayoría edades que pasan los 40 años. Es importante tener en cuenta que a esta edad el aprender a manejar herramientas tecnológicas se hace más difícil y esto es un factor que se debe tener en cuenta al momento de seleccionar la tecnología que va a ser instalada en el edificio.

Con respecto al tema de seguridad, el personal del Departamento de Seguridad Integral con ayuda del Cuerpo de Bomberos organiza periódicamente charlas al personal para orientarlos en lo que se debe hacer en caso de emergencia.

1.5. Situación actual de La Empresa.

La Empresa presenta una situación muy particular que merece ser analizada para situar el contexto.

Al ser una empresa estatal, está regida por normas dictadas por el Estado peruano y las decisiones tomadas por las personas encargadas de dirigir a la institución muchas veces se ven afectadas debido al tiempo que toma que se realicen los trámites burocráticos y las aprobaciones de los proyectos que, en muchos casos, son urgentes.

Además, La Empresa fue parcialmente privatizada años atrás debido a los problemas financieros que tenía el gobierno de turno, por lo que en la actualidad solo cuenta con una fracción de los recursos con los que contaba antes.

Esta situación actualmente está siendo modificada y La Empresa pasa por un período de transición debido a la aprobación de la ley que se expone a continuación.

1.5.1. Ley de Modernización y fortalecimiento de La Empresa.

Artículo 1°.- Objeto de la Ley

Declárese de interés nacional el fortalecimiento y modernización de La Empresa, debiendo desarrollar sus actividades regidas por la presente Ley, su Ley Orgánica, el Decreto Legislativo N° 43 y su modificatoria, la Ley N° 26224, su Estatuto Social, y supletoriamente por las disposiciones de la Ley General de Sociedades.

El resumen de lo acordado en esta ley se presenta en el siguiente extracto del artículo presentado por el diario La República del día 14 de Julio de 2006:

FORTALECIMIENTO - Con 63 votos, el Pleno del Congreso otorgó autonomía a petrolera estatal - Se convocará a concurso público internacional para iniciar obras de mejoramiento de La Empresa.

Con 63 votos a favor, nueve en contra y once abstenciones, el Pleno del Congreso de la República aprobó la autógrafa de Ley de Modernización de La Empresa, después de que el pedido de reconsideración hecho por el congresista José Carrasco Távara, fuese aprobado.

Con esta ley, La Empresa actuará con autonomía económica, financiera y administrativa y con arreglo a los objetivos anuales y quinquenales que apruebe el Ministerio de Energía y Minas (MEM).

El presidente del directorio de La Empresa, Róger Arévalo, calificó de "excelente" la aprobación de esta ley, porque finalmente le da la

autonomía que La Empresa necesita para su modernización y competir con las empresas privadas.

Además aclaró que esta ley ya no puede ser observada por el Ejecutivo, ya que se trata de una insistencia, la cual se ha votado dos veces. "En cuanto se promulgue la ley, se realizará la convocatoria a concurso público internacional, para elegir a la empresa encargada de la modernización de toda La Empresa. Algunos estudios de factibilidad indican que en este proceso se invertirá alrededor de US\$ 900 millones", precisó Arévalo a La República.

Juan Castillo, secretario del sindicato de trabajadores de La Empresa en Talara, manifestó que después de que la autógrafa fuese rechazada en el Pleno, emprendieron un diálogo con los congresistas que se abstuvieron, para explicarles los beneficios de esta ley. "De acuerdo al cronograma que manejamos, tenemos ocho meses de labor administrativa, y estamos en tratativas con empresas especializadas en modernización de refinerías, para iniciar lo más pronto posible las obras de la refinería de Talara", manifestó.

Róger Arévalo aclaró que el artículo que establecía la fusión, por absorción, de la empresa estatal de derecho privado Perupetro por parte de La Empresa, fue retirado de la Ley de Fortalecimiento aprobada.

No obstante, informó que en el Plan de Gobierno del Partido Aprista existe un plan para que esta fusión se concrete y "así tener una visión integrada del mercado de hidrocarburos nacional".

Con la aprobación de la ley de Fortalecimiento, La Empresa queda excluida del ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE) y además del reglamento del Sistema Nacional de Inversión Pública (SNIP).

Como se aprecia en el resumen presentado de la ley, La Empresa queda excluida del ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE). Con esto se consigue que La Empresa tenga un mejor manejo de sus recursos y pueda hacer inversiones con mayor libertad.

Con respecto a las empresas que forman parte de la competencia, es preciso señalar que existen alianzas estratégicas que buscan sacar a La Empresa de su liderazgo, como se aprecia en el siguiente artículo, escrito por Humberto Campodónico - Diario La República.

La siguiente cita refleja, de manera exacta, el comportamiento de este gobierno ante La Empresa: "La funcionaria indicó que, tras la pérdida del mejor cliente de La Empresa, se podría incluso reevaluar el proyecto de modernización y ampliación de la capacidad que se esperaba realizar en las refinerías de dicha empresa estatal, y acondicionarla a las nuevas circunstancias del mercado" (El Comercio, 3 de junio 2006).

Lo que la funcionaria está diciendo es que, ahora que La Empresa ha perdido a su mejor cliente –Mobil, cuyos grifos acaban de ser comprados por Repsol/YPF en US\$ 37,6 millones-, se puede reducir el monto de la inversión en la mejora y ampliación de la Refinería de Talara. En otras palabras, se avala que La Empresa pierda buena parte de su participación en el mercado de venta de combustibles.

La mencionada funcionaria es Hilda Sandoval, directora ejecutiva del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE), entidad del MEF propietaria del 100% de las acciones de La Empresa y las demás empresas estatales. Como se aprecia, Sandoval no está preocupada –como debiera- por la amenaza de una seria reducción de los ingresos de "su" empresa.

Y no lo está porque lo que en verdad se quiere, desde el gobierno, es que La Empresa se privatice. Como no lo pudieron hacer debido a la oposición mayoritaria de la población, su debilitamiento es una excelente

oportunidad "de mercado" para realizar sus deseos. Seguramente por eso, el ministro de Economía, Fernando Zavala, dijo el miércoles pasado (antes de que se concrete la venta de los grifos de Mobil), que La Empresa no tenía el dinero suficiente para comprar los grifos, "olvidándose" de que la estatal tiene utilidades: solo en el 2005 su utilidad neta fue de S/. 245 millones (US\$ 75 millones).

Mientras tanto, la estatal petrolera de Chile ENAP, en alianza con el Grupo Romero, a través de Primax, se hace fuerte aquí: "La participación de mercado de Primax ha aumentado, llegando a 27%, siendo la empresa líder en Perú y una excelente fuente para las exportaciones de combustibles que realiza ENAP" (El Mercurio, 22/12/2005). Como se aprecia, en Chile no quieren vender su empresa estatal. Por el contrario, la autorizan a invertir aquí para que coloque sus excedentes de gasolinas.

De su lado, Repsol, con su mercado ampliado por la compra de los grifos de Mobil y el traspaso de sus importantes clientes (Antamina, Yanacocha, Southern y Enersur), ahora podrá vender 16,000 barriles diarios (bd) adicionales por US\$ 600 millones anuales (lo que La Empresa le vendía a Mobil). Para atender estos nuevos clientes, seguramente Repsol-La Pampilla importará más petróleo del Ecuador, donde opera el Bloque 16 que produce 53,000 bd. En el 2004, Repsol importó 25,000 bd del Ecuador (Dirección General de Hidrocarburos).

Repsol está integrada verticalmente a nivel internacional, lo que le permite obtener una amplia renta petrolera: en Ecuador el costo de producción es de US\$ 6/barril pero Repsol/La Pampilla lo compra a US\$ 60/barril. También Repsol tiene integración vertical en Perú pues opera en el mercado de GLP, grifos, refinación y exploración.

Aquí es donde se cierra el círculo al que hacía mención Hilda Sandoval: como La Pampilla va a refinar más petróleo proveniente del Ecuador para atender a los clientes de Mobil, entonces la Refinería Talara de La Empresa (que ahora ve amenazadas sus ventas) va a refinar

menos petróleo. Por tanto, ¿para qué ampliarla? Está clarísimo: la compra de los grifos de Mobil es una estocada proprivatización de La Empresa.

Todo se ha hecho de manera sincronizada, aprovechando los últimos días de este gobierno complaciente con el capital extranjero, enemigo de las empresas públicas, y continuador de las políticas neoliberales de Fujimori. Esta venta de los grifos de Móbil tiene que ser revertida porque lesiona gravemente, y de manera artera, los intereses del Perú.

El hecho de que se haya aprobado la Ley de Modernización trajo varias consecuencias inmediatas, una de ellas fue la agilización en el desarrollo de proyectos como el que se diseña en la presente tesis. Antes de esta Ley, la dificultad para realizar estos trabajos era mayor ya que los trámites burocráticos dificultan mucho el manejo de proyectos. Por ejemplo, en una empresa privada, los proyectos más grandes deben alcanzar la aprobación de la Directiva para poder realizarse, en el caso de La Empresa, una empresa del Estado peruano, estas decisiones deben salir fuera de la misma y ser evaluadas por entidades externas, que en este caso hacen la función de Directiva, como el FONAFE.

Muchas veces las políticas que tiene el FONAFE no concuerdan con las políticas que tiene La Empresa y el resultado es que ésta se estanca y pierde competitividad ante sus homólogos privados.

La aprobación de la Ley le da una mayor autonomía a La Empresa para tomar sus decisiones y poder hacer un uso más independiente de sus recursos. Esta situación trajo a los trabajadores de La Empresa nuevas fuerzas para seguir trabajando, sabiendo que ahora sus esfuerzos estaban mejor encaminados.

En este contexto, la modernización tecnológica toma un papel muy importante. Todas las operaciones que forman parte de La Empresa han entrado en proceso de modernización y el Edificio de Oficinas Principal (OFP), lugar donde se toman las decisiones más importantes, no podía dejar de unirse a este proceso.

CAPÍTULO 2

Análisis del Sistema de Control de Accesos.

2.1. Automatización de Edificios: Edificio Inteligente.

En la actualidad el avance de la tecnología proporciona herramientas que permiten resolver problemas que en el pasado hubieran sido imposibles de resolver. Este avance da a las empresas mayores competencias para desarrollarse en sus respectivos medios.

El Edificio Inteligente se define, según la Dra. Ofelia Cervantes Villagómez [31], como una estructura que facilita a usuarios y administradores, usando herramientas y servicios integrados a la administración y comunicación. El concepto de Edificio Inteligente propuso por primera vez la integración de todos los sistemas existentes dentro del edificio, tales como telefonía, comunicaciones por computadora, seguridad, control de todos los subsistemas de edificio tales como, calefacción, ventilación y aire acondicionado, y todas las formas de administración de energía.

El asunto de estudio que se presenta en la presente tesis consiste en el diseño de un Sistema de Control de Accesos para el edificio que cumpla con los requerimientos de La Empresa y que pueda ser integrado con los demás sistemas del edificio para poder llegar a una optimización del sistema global.

En éste contexto, se realizará un estudio de los sistemas involucrados en la automatización de edificios para poder tener una visión clara del medio en donde se instalará el sistema.

2.2. Sistemas usados en el diseño de Edificios Inteligentes en la actualidad.

En este nivel de la investigación se presentarán las tecnologías con las que el Edificio de Oficina principal cuenta o esta proyectando instalar en este proceso de

modernización, como son: Sistemas de Evacuación y Perifoneo, Circuito Cerrado de Televisión CCTV, Sistema de detección y Alarma de Incendios y Control de Accesos.

El concepto de Edificio Inteligente agrupa todas estas tecnologías y las hace trabajar en una forma integrada para poder aprovechar al máximo las funciones que brindan.

2.2.1. Sistemas de Evacuación y Perifoneo.

Este sistema tiene como misión principal la de salvaguardar la integridad de las personas ocupantes del edificio. Consiste en una serie de parlantes especiales ubicados en lugares estratégicos que sirven para informar a las personas si hay alguna anomalía en el edificio (emergencias). Sin embargo, también puede ser utilizado para hacer anuncios públicos o difusión musical (megafonía).

La empresa internacional BOSCH [23] nos habla de los alcances de estos sistemas: 'La gama del sistema de sonido para megafonía y emergencias incluirá controladores de red, amplificadores de potencia, estaciones de llamada, expansores de audio e interfaces de alto y bajo nivel para la conexión de sistemas externos. El sistema es capaz de monitorear todos sus equipos y de notificar al controlador de la red cualquier fallo que pueda producirse. Cada uno de los equipos provistos de entradas o salidas de audio contará con un conector de auriculares para controlar el sonido.

El sistema de megafonía incorpora numerosas funciones, las más importantes se enumeran a continuación:

- Difundir emisiones públicas de avisos rutinarios, de situaciones importantes y de emergencia.
- Emitir difusiones simultáneas de diferentes llamadas a distintas ubicaciones.
- Difundir música ambiental a todas las ubicaciones o a ubicaciones seleccionadas

- Proporcionar una función automática de anuncio para emitir avisos rutinarios, de situación y de emergencia.

La compañía Bosch emplea fibra óptica para intercomunicar estos componentes, para los enlaces menores a 50 metros usa Fibra de plástico y para distancias más largas usa Fibra de vidrio debido a su mejor desempeño en estas distancias.

La intercomunicación entre los componentes del sistema se hace en Topología Anillo, lo que permite que el sistema soporte la ruptura en un punto de la red sin tener problemas en su operación. Además estos tipos de sistemas están equipados para poder trabajar en red con otros sistemas lo que permite una rápida integración entre ellos. Esta última característica es muy importante ya que asegura que el sistema trabaje en conjunto con los demás sistemas del Edificio Inteligente.

2.2.2. Circuito Cerrado de Televisión; CCTV.

Este sistema consiste en un conjunto de cámaras interconectadas directamente con el propósito de brindar seguridad a determinadas áreas en las esto es un factor crítico [36]

El CCTV permite acceder visualmente a los distintos ambientes del edificio desde el centro de control, cuando este sistema está integrado con los demás sistemas del edificio puede ser programado para reaccionar de acuerdo a la alarmas que generan los demás sistemas y enviar imágenes del lugar en donde se ha generado la alarma inmediatamente.

La tecnología usada en la actualidad en este tipo de sistemas es la del DVR (Digital Video Recorder) [12], esta tecnología permite almacenar las grabaciones en forma digital, lo que permite usar las computadoras para manejar las cámaras y almacenar los archivos que éstas generan.

Actualmente el protocolo TCP/IP [11] es también usado para transmitir los datos que generan las cámaras, con esto se logra poder aprovechar el cableado estructurado existente y se evita el tener que instalar una red independiente.

2.2.3. Sistema de detección y alarma de incendio.

El sistema de detección y alarma contra incendios tiene como finalidad la de salvaguardar la vida de las personas que se encuentran dentro del edificio, facilitando de manera rápida y eficiente la detección de fuegos primarios indicando el lugar donde éstos se están produciendo [26].

Este sistema consta de una serie de sensores y dispositivos que al actuar en conjunto permiten ubicar inicios de posibles incendios para poder tomar las medidas correspondientes en el momento adecuado.

Debido al grado de confiabilidad que debe tener un sistema encargado de salvaguardar las vidas de las personas, se han encargado estándares que ayudan a que los diseños sean eficientes y puedan cumplir su función.

La NFPA (Asociación Nacional de Protección de Fuego) es la asociación que se encarga de normar las instalaciones de sistemas de detección y alarmas contra incendios. Esta organización busca constantemente mejorar la calidad de estos sistemas para brindar una mayor seguridad al usuario. Los sistemas que se instalan en la actualidad deben, por seguridad estar sujetos a estas normas para asegurar el buen funcionamiento de la red en caso de ocurrir una emergencia.

Asimismo, el sistema instalado deberá tener una simbología adecuada que permita a las personas saber como actuar en un momento de riesgo. Para este fin se ha buscado estandarizar también los símbolos que se usan para señalar las acciones a seguir en caso de una emergencia. Con esto se logra que las personas se familiaricen con la simbología en cualquier sitio en el que estén y puedan actuar rápido en cualquier circunstancia de riesgo.

El EN54 es el documento actualizado en donde se establecen cuales son los símbolos estandarizados y su respectivo significado.

Es deseable además que los sistemas de detección y alarma contra incendio actúen en conjunto con el sistema de CCTV, así se podrá tener, a parte de la ubicación del siniestro, una figura clara de lo que está pasando, para poder tomar las medidas que requiera la emergencia en el menor tiempo posible.

2.2.4. Cableado estructurado.

A continuación se presentan los medios por los cuales se transmiten los datos a través del edificio.

2.2.4.1. Fibra Óptica.

Según la enciclopedia Encarta [28]. Los circuitos de fibra óptica son filamentos de vidrio (compuestos de cristales naturales) o plástico (cristales artificiales), del espesor de un pelo (entre 10 y 300 micrones). Llevan mensajes en forma de haces de luz que pasan a través de ellos de un extremo a otro, donde quiera que el filamento vaya (incluyendo curvas y esquinas) sin interrupción.

Las fibras ópticas pueden ahora usarse como los alambres de cobre convencionales, tanto en pequeños ambientes autónomos (tales como sistemas de procesamiento de datos de aviones), como en grandes redes geográficas (como los sistemas de largas líneas urbanas mantenidos por compañías telefónicas).

2.2.4.2. Cable Coaxial.

Este cable está formado por dos conductores concéntricos. El conductor central o núcleo está formado por un hilo sólido de cobre (llamado positivo o vivo), rodeado por una capa aislante (llamado dieléctrico) que lo separa de exterior, formado por una malla trenzada de cobre o aluminio, este conductor produce un efecto de apuntalamiento y además sirve como retorno de las corrientes. Todo el conjunto está protegido por una cubierta aislante. Existen múltiples tipos de cable coaxial, cada uno

con un diámetro e impedancia diferentes. El cable coaxial se utiliza en redes de comunicación de banda ancha y cables de banda base. El cable coaxial no es habitualmente afectado por interferencias externas, y es capaz de lograr altas velocidades de transmisión en largas distancias [29].

2.2.4.3. Cable UTP.

Según la enciclopedia Encarta [28]. El cable UTP es el tipo de cable más usado en las redes de computadoras. Es una variante del cable de par trenzado. Los cables UTP usualmente también son llamados 'Cables Ethernet', ya que es el estándar de redes más usado que utiliza cables UTP. En contraste con los cables FTP y STP, los cables UTP no tienen una cubierta conductora, por lo que no están protegidos contra el ruido externo, sin embargo, es el más usado debido a su flexibilidad y fácil manejo.

Este tipo de cableado cuenta con el efecto de cancelación que producen los pares trenzados de hilos para limitar la degradación de la señal.

En el caso de la Red LAN del edificio en el que se desarrolla la problemática, se usa el cableado UTP de Categoría 5e. Esta categoría está definida en la TIA/EIA - 568-B y provee un desempeño de hasta 125MHz. Es usada para redes 100Mbps/s y hasta Gigabit Ethernet en algunos casos, pero no es recomendable.

2.2.5. Control de Accesos.

Los Sistemas de Control de Accesos son usados por muchas organizaciones privadas y del Estado, grandes negocios y plantas industriales para identificar y dar acceso a cualquiera que pertenezca a un área a la que se desee acceder.

Estos sistemas no son usados únicamente para bloquear o desbloquear accesos, también puede ser usado para almacenar información del personal, cargar cuentas del personal para compras dentro del lugar, como en la cafetería, o para acceder a determinados equipos tales como computadoras personales o impresoras.

Las lectoras del sistema generalmente cuentan con mecanismos de seguridad tales que envíen señales en caso de que algún extraño quiera manipularlas o forzarlas.

Entre los dispositivos empleados para el control de accesos se encuentran las lectoras de tarjetas, las tarjetas de acceso de los usuarios y los contactos magnéticos que manejarán la apertura y cierre de las puertas de forma automática.

Estos elementos terminales se comunican con un controlador principal a través de un protocolo de comunicación predeterminado. En los últimos años la necesidad de uso de diferentes fabricantes un mismo sistema ha dado origen a la creación de estándares comunes a todos los fabricantes y cada vez más usuarios prefieren el uso de estos protocolos. Para el caso de la comunicación entre los terminales y el controlador principal se maneja el protocolo de comunicación Wiegand.

El protocolo Wiegand es abierto, maneja niveles de voltaje TTL a velocidades bajas (500 baudios). La tarjetas de acceso tienen en su interior un cable ferromagnético que al ser excitado por la lectora genera un voltaje que es sentido y reconocido como un código por la lectora. Estos niveles de voltaje actúan como una codificación binaria, la mayor capacidad que pueden alcanzar es la de 84 bits, es decir, puede llegar a almacenar información de hasta 137 billones de usuarios.

La comunicación entre el controlador principal y el servidor de Control de Accesos se realiza a través de la Red LAN, teniendo opción a conectarse mediante cableado redundante directamente al servidor, mediante protocolo RS-485. El uso de este protocolo asegura que la información viaje sin problemas a través de distancias largas, de hasta 1,2 km. El cableado para este propósito debe ser apantallado y la pantalla debe estar aterrada.

Es preciso mencionar que el ancho de banda que consume el sistema es despreciable en comparación con las capacidades de transmisión que tienen actualmente el cableado estructurado de los edificios de oficinas.

Según la Asociación BICSI, es muy importante que el Sistema de Control de Accesos tenga comunicación con otros sistemas del Edificio Inteligente, tales como el CCTV o el Sistema de Alarma Contra Incendio, para poder alcanzar un uso óptimo de los recursos.

2.2.6. Integración.

El objetivo del Edificio Inteligente es integrar todas las herramientas mencionadas para que puedan cumplir en conjunto con su fin fundamental, asegurar el bienestar de los ocupantes del edificio.

El concepto de integración involucra que todas las tecnologías trabajen de forma que puedan compartir información cuando sea necesario.

2.3 Situación actual del Sistema de Control de Accesos en La Empresa.

El sistema actual cuenta con lectoras de proximidad marca Indala, con un alcance de 30 cm. Las lectoras encargadas de llevar el registro de ingresos del personal se encuentran en el piso 1 y en el sótano 1 del edificio, que son los lugares por donde el personal ingresa. Además, existe una lectora en cada piso, a la salida de los ascensores ejecutivos, usados por las personas de mayor rango en La Empresa.

Las tarjetas utilizadas son del tipo pasivas, es decir, no consumen energía. Lo bueno de esta característica es que no es necesario el uso de baterías en las tarjetas y además, el costo es la quinta parte del costo de las tarjetas activas, lo malo es que el rango de alcance es más limitado.

Las lectoras son manejadas en conjuntos de hasta tres por interfaz Wiegand. Ésta pequeña red, formada por las lectoras y la interfaz, es de Topología Bus y usan la norma RS-485 para transferir información.

El protocolo utilizado en esta comunicación es el RS-485, el cual permite conectar hasta 32 dispositivos en topología bus, para la transmisión de información

usa voltaje diferencial de -7 y +12. Puede alcanzar distancia de hasta 1.2 Km. usando cable trenzado y apantallado.

La comunicación entre la interfaz Wiegand y el servidor principal se hace mediante cableado estructurado dedicado para éste propósito. Este cableado estructurado se desplaza a través de las tuberías del cableado estructurado de la Red de Área Local (LAN).

El servidor del Sistema de Control de Accesos emite reportes diarios que pueden ser impresos y enviados a Recursos Humanos para el control de personal y al Departamento de Seguridad cuando es necesario.

2.4. Deficiencias en el actual Sistema de Control de Accesos.

Actualmente el Edificio de Oficinas de La Empresa se cuenta con un Sistema de Control de Accesos ineficiente. El sistema en su instalación inicial fue diseñado para llevar un control de accesos trabajando de manera independiente de los demás sistemas, en la actualidad se busca integrar todos los sistemas electrónicos del edificio, por lo que el sistema actual no cumple con los niveles tecnológicos que se requieren para este proceso.

Por otro lado, la seguridad de un Edificio de Oficinas como el de La Empresa representa un tema álgido ya que la información que se maneja es muchas veces de carácter confidencial y sería muy peligroso que terceros tengan acceso a esta. El Sistema de Control de Accesos que se encuentra instalado en la actualidad al no estar distribuido en todos los pisos ocasiona que se requiera de mucho personal de seguridad contratado para que cumpla con estas funciones.

El sistema en mención permite llevar un control de las horas de llegada y salida de los empleados, esto le permite al Departamento de Recursos Humanos emitir informes de asistencia y puntualidad. Sin embargo, este Departamento no puede obtener otro tipo de información valiosa como por ejemplo, cuanto tiempo las personas permanecen en lugares que no son sus oficinas.

El Departamento de Seguridad también utiliza la información tomada por el Sistema de Control de Accesos. Esto sucede cuando se necesita conocer que personas se encontraron presentes en un determinado lugar en un momento determinado. Sin embargo, no se puede obtener información acerca de un lugar específico ya que las lectoras destinadas a los empleados comunes solo se encuentran en el Piso 1 y en el Sótano 1, lo que dificulta el trabajo del Departamento de Seguridad.

En cuanto al punto de vista tecnológico, el sistema actual cuenta con equipos obsoletos. Esto afecta el trabajo de mantenimiento ya que se hace más difícil encontrar repuestos para los equipos que presentan alguna falla, lo que muchas veces ocasiona que se tengan que comprar nuevos equipos y esto, a su vez, ocasiona que se tenga un sistema híbrido, con equipos de diferentes marcas, lo que disminuye el desempeño del sistema total.

Además, la obsolescencia del sistema restringe la posibilidad de acoplarlo al sistema global del Edificio Inteligente ya que, al ser obsoleto, se hace incompatible con las nuevas tecnologías.

2.5. Sistema de Control de Accesos en edificios de oficinas en la actualidad.

La siguiente información ha sido obtenida de reuniones periódicas con empresas dedicadas a brindar seguridad electrónica en edificios de oficinas.

Los Sistemas de Control de Accesos constituyen una herramienta muy útil en el área de seguridad de las empresas. Entre sus principales funciones se encuentran:

- Establece niveles de seguridad en el acceso a las instalaciones de La Empresa. Por ejemplo, en la puerta principal todos los empleados deben contar con suficientes privilegios para acceder, por el contrario, en el ingreso a presidencia solo se debe dejar acceder a personas que desempeñen funciones en ese lugar.
- Establecer un control de acceso a los visitantes del edificio. Según lo conversado con las empresas proveedora de estos sistemas, éstos están preparados

para programar tarjetas de acceso en la recepción del edificio para los visitantes. Estas tarjetas le dan al visitante acceso solo a las áreas en donde se requiere su presencia.

- Da a conocer en tiempo real la posición de las personas en el edificio. Esto se logra gracias a que el sistema guarda en memoria los accesos y salidas de las personas en todos los controles del edificio. Esta herramienta permite elaborar informes a seguridad en caso de ser requeridos.

- Emite reportes al Departamento de Recursos Humanos para poder tener un control de asistencias y horas extra del personal.

Los sistemas de control de accesos están compuestos de 4 elementos fundamentales:

2.5.1. Servidor de Control de Accesos.

Es una computadora dedicada al manejo del Sistema de Control de Accesos. Cuenta con un software que permite a la persona encargada de supervisar la seguridad obtener la información que necesite en forma rápida y segura. Las diferentes tareas que puede desarrollar un servidor se dan de acuerdo al software que este maneja, y este software, a su vez, depende del fabricante.

Los software de las empresas consultadas permiten el uso de los planos del edificio para poder visualizar en todo momento la ubicación de las lectoras y, en caso de producirse una alarma, encontrar el lugar donde se produjo en tiempo real.

2.5.2. Controlador Central del Sistema de Control de Accesos.

Es el equipo encargado de mantener la integración en los sistemas del edificio. Se encarga de tomar las decisiones en los intentos de acceso en tiempo real.

El Controlador Central se encarga del procesamiento de todos los eventos. Esto asegura la integridad del sistema incluso si el servidor no funcionase. El controlador recibe la información del portador de la tarjeta a través de la interfaz de lectora cada vez

que se realiza un intento de ingreso. Luego, verifica la información y si el portador de la tarjeta tiene suficientes privilegios, la puerta se abrirá.

2.5.3. Interfaz de lectoras.

Cumple la función de interfaz entre el controlador y hasta 2 lectoras. Esto permite a la interfaz, en el mejor de los casos, recibir información de un portador de tarjeta a la entrada y salida de una misma puerta (una lectora a la entrada y otra a la salida). Luego envía esta información al controlador principal para su procesamiento. Además, la interfaz puede emitir información de cerrado o abierto de la puerta al controlador principal.

Asimismo cuenta con entradas supervisadas de relé para recibir eventos tales como alarma del sistema contra incendios o forzado de puertas.

Cuando un portador de tarjeta presenta su tarjeta de acceso a una lectora de entrada o salida, la información va a la interfaz, esta la codifica y la envía al controlador principal, donde es procesada y se decide si la puerta será abierta o no de acuerdo a los privilegios asignados al portador de la tarjeta.

2.5.4. Lectoras.

Son los terminales del sistema, encargados de recibir los datos de las personas que solicitan acceso.

Los principales tipos de lectoras son los siguientes:

2.5.4.1. Lectora de teclado.

Esta lectora recibe la información del usuario a través de un teclado matricial.

2.5.4.2. Lectora de proximidad.

Recibe la información del usuario mediante tarjetas de control de accesos. Éstas tarjetas pueden ser del tipo pasivas (sin energía propia) o activas (con fuente de energía propia). Las tarjetas activas tienen la ventaja de permitir una mayor distancia entre lectora y tarjeta, sin embargo, tienen el defecto de que la fuente de la tarjeta debe ser reemplazada cada cierto tiempo.

2.5.4.3. Lectoras biométricas.

Recibe la información del usuario mediante el escaneo de alguna parte de su cuerpo, por ejemplo, huella dactilar, iris, entre otros.

Existen otros tipos de lectoras que ofrecen más seguridad combinando las características de las lectoras mencionadas, por ejemplo, lectora biométrica con teclado.

2.6. Indicadores que permiten conocer los grados de mejora que ofrece la instalación de un Sistema de Control de Accesos en un Edificio de Oficinas.

- Satisfacción del Cliente. Este indicador puede ser medido mediante la evaluación de las quejas y/o sugerencias que tengan los usuarios luego de la instalación. Depende de la calidad del servicio brindado y de la capacidad de los operarios para manejar el sistema

- Calidad del Servicio de Acceso a la red. Medido en función a la velocidad promedio de conexión, y el tiempo de disponibilidad de la red. Estos factores influirán en gran manera a la percepción que los usuarios tengan del servicio que se les ofrece. Éste indicador se debe tener en cuenta ya que la información del Sistema viajará por la red LAN del edificio.

- Mejora en el desempeño de los usuarios: Las mejoras del sistema también podrán ser percibidas en un aumento del rendimiento de los usuarios, ya que al

mejorar la seguridad en el ambiente en el que se trabaja, se aumenta la capacidad de los empleados en realizar un buen trabajo.

- Seguridad en el edificio. El aumento de la seguridad en el edificio debe cuantificarse a través de una reducción de situaciones no deseadas, como pérdidas de objetos personales o documentos.



CAPÍTULO 3

Determinación de los requerimientos de La Empresa.**3.1. Objetivo de la tesis.**

La presente tesis tiene como objetivo diseñar un Sistema de Control de Accesos tal que cumpla con las expectativas de seguridad de La Empresa y, además, que utilice equipos de última generación que permitan al sistema poder integrarse a los demás sistemas del edificio en una solución del tipo Edificio Inteligente.

El diseño incluirá tanto la selección como las ubicaciones de los componentes del sistema y el cableado del mismo, así como una cotización detallada de los equipos involucrados en el sistema.

Luego de analizar el estado actual de la problemática se han tomado las siguientes condiciones iniciales para el diseño:

3.1.1. Uso de tecnología moderna.

Los estándares y las normas usadas en la actualidad en los sistemas de seguridad permiten que la información fluya a través del medio físico sin problemas, por lo tanto, la utilización de los mismos es fundamental en todo diseño. Asimismo, se debe garantizar que el sistema maneje protocolos que permitan su integración con otros sistemas del edificio.

3.1.2. Diseño de sistema distribuido.

El Sistema de Control de Accesos actual del edificio no se encuentra distribuido uniformemente. Esta circunstancia genera que no sea una herramienta muy útil para el Departamento de Seguridad. Por lo tanto, el nuevo diseño debe tener una distribución adecuada de las lectoras en todo el edificio.

3.1.3. Diseño de sistema integrable.

La solución integradora que se implementará en el edificio exige que los sistemas estén diseñados teniendo en cuenta esta integración, para luego no tener problemas en las comunicaciones entre los distintos sistemas. Por lo tanto, se debe garantizar el diseño de un sistema que cumpla con los estándares y normas de telecomunicaciones y seguridad que se requieren en un Sistema de Control de Accesos, teniendo principal consideración en usar protocolos de comunicación abiertos.

3.1.4. Cumplimiento de los Requerimientos de La Empresa.

El sistema debe estar orientado a satisfacer los requerimientos que han sido recogidos de los Departamentos involucrados del edificio.

3.2. Características deseables del Sistema.

Para la recopilación de los requerimientos de La Empresa se han llevado a cabo reuniones con los Departamentos de Seguridad y Telecomunicaciones. Relacionando estos requerimientos con los sistemas que ofrecen las empresas proveedoras de Sistemas de Control de Accesos, se han obtenido las características deseables del sistema.

Además, se han tenido en cuenta los sistemas que ya están instalados en el edificio y los que serán instalados en el futuro, para garantizar que se pueda integrar.

A continuación se procederá a mostrar los requerimientos recogidos de La Empresa en las reuniones que se realizaron con los Departamentos involucrados. Se ha considerado conveniente mostrar las necesidades recogidas para cada parte del sistema. Por cuestión de orden se mostrará en cada uno de los puntos las características deseables basadas en la seguridad, separadas de las características deseables debido a la integrabilidad que se exige. En los puntos más simples se han colocado las características deseables sin hacer esta separación.

Para la selección del sistema se han tenido en cuenta los siguientes puntos:

- Software del sistema
- Servidor del sistema
- Panel controlador de lectoras
- Lectoras de proximidad peatonales
- Lectoras de proximidad de largo alcance
- Interfaz Wiegand
- Barreras vehiculares
- Tarjetas de proximidad
- Integración con el Sistema de Control de Incendios

3.2.1. Características deseables del Software del Sistema.

3.2.1.1. Características basadas en la integrabilidad.

- El software deberá estar preparado para ejecutarse sobre el sistema operativo Windows XP, que es el más usado en La Empresa.
- El software que maneja el sistema deberá interactuar con las demás plataformas de seguridad que se encuentran o que se vayan a instalar en el edificio, como el CCTV. Éste último maneja protocolo de compresión ACC, que se detalla en los anexos, por lo que el sistema deberá estar preparado para interactuar con este formato propietario.
- El software deberá tener capacidad para emitir reportes personalizados de los eventos que ocurren en el sistema. Deberá contar con una interfaz gráfica intuitiva que permita generar estos reportes fácilmente.

3.2.1.2. Características basadas en requerimientos de seguridad.

- Se necesita un mínimo de 4 licencias para que el sistema pueda ser manejado desde 4 estaciones en simultáneo, con lo cual se asegura que en caso de emergencia, el sistema pueda ser manejado de lugares que no sean el Centro de Control. Esta

cantidad se debe a que el sistema deberá poder ser usado desde Telecomunicaciones, Presidencia y Gerencia General y, a parte, se tendrá una licencia más como respaldo.

- El software del sistema debe poder ser programado para que los usuarios tengan diferentes privilegios de acuerdo a la configuración en el nivel de accesos. Esta característica ayudará a los agentes de seguridad a brindar un servicio más seguro.

- Debe contar con un mecanismo de encriptación tal que garantice que los datos no puedan ser manipulados ni plagiados del sistema.

- Debe tener capacidad de enviar alarmas vía correo electrónico a las personas que se indique, con esto se podrá generar alarmas a los distintos Departamentos Involucrados en el Sistema de Control de Accesos, como lo son Telecomunicaciones y Seguridad.

- El software del sistema deberá contar con programación de 'N personas máximas' en un área, con lo que se asegura que no se exceda el número de personas máximo que se puede evacuar de un lugar en caso de emergencia.

- Debe contar con un sistema de monitoreo de alarmas y eventos y mostrar el estado del monitoreo en imágenes y planos. Con esto La Empresa garantiza que se le instale un software gráfico con el que se pueda interactuar amigablemente.

- Debe poder realizar la importación de mapas y planos de archivos, para disponer de una referencia visual dinámica cuando se produzca alguna incidencia en el sistema.

3.2.2. Características deseables del Servidor del Sistema.

3.2.2.1. Características basadas en la integrabilidad.

De acuerdo a la experiencia que tiene La Empresa en el uso de servidores, se ha buscado que el servidor que maneje el Sistema de Control de Accesos sea semejante a los que La Empresa está acostumbrada a manejar.

Procesador Intel® Xeon o equivalente	Mínimo 3,00 GHz
Bus del Sistema	Mínimo 800MHz
Memoria Cache	Mínimo 2MB
Disco Duro	Mínimo 80 GB
DVD/DVDRAM Grabador integrado	Si
Puertos E/S externos	Paralelo, Serial, PS2, USB; RJ-45
Memoria estándar (RAM)	Mínimo 1GB
Monitor, teclado, Mouse	Si
Sistema Operativo con licencia a nombre de La Empresa	Si

Tabla 3.1. Características deseables del Servidor de Control de Accesos.

3.2.2.2. Características basadas en requerimientos de seguridad.

El sistema debe poder ser manejado a través de las redes LAN y WAN, por usuarios con suficientes privilegios. La Empresa exige esta característica debido a que es necesario que el personal de seguridad tenga acceso al sistema desde lugares diferentes al centro de control.

3.2.3. Características de los Paneles Controladores de Lectoras.

3.2.3.1. Características basadas en la integrabilidad.

- Debe manejar el protocolo DHCP. Con esta característica se podrá usar el dispositivo con dirección IP tanto fija como variable
- Debe poder conectarse a la red LAN. Con esto se garantiza que el sistema sea administrable, si se tienen los privilegios de seguridad, desde otros puntos de la red.
- Los paneles deben estar ubicados en gabinetes para evitar que los factores externos disminuyan la vida útil del equipo.

3.2.3.3. Características basadas en requerimientos de seguridad.

- Se debe contar con una conexión redundante al servidor del sistema. Con esto el Departamento de Seguridad garantiza que en caso de que haya problemas con la red, el sistema no pierda conectividad con el servidor.
- El sistema debe contar con programación 'Anti-passback', que asegura que una misma tarjeta no pueda acceder a la misma puerta si es que no ha pasado por la lectora de salida. De ésta manera, una misma tarjeta no podrá ser usada para abrir la misma puerta si es que el usuario no ha abandonado el ambiente.
- La comunicación debe estar cifrada debido a que la información que se desplaza a través del medio es confidencial para La Empresa.
- Los controladores debe formar una red entre sí para poder operar sin necesidad de intervención del servidor. Esta característica permite al sistema seguir operando sin necesidad del servidor.
- El panel controlador debe cumplir con las normas UL y FCC. Estas normas garantizan la calidad de los equipos.

3.2.4. Características de las Lectoras de Proximidad Peatonales.

3.2.4.1. Características basadas en la integrabilidad.

- Las lectoras deben ser compatibles con las lectoras y tarjetas existentes en La Empresa: Indala Flex Pass Motorola. Con esta característica La Empresa busca disminuir sus gastos reutilizando lo que aún sirve.
- Deben soportar comunicación mediante el Protocolo Wiegand, según documento "SIA AC-01-1996.10" de los Estándares SIA, acreditados por la ANSI. Este protocolo es un estándar de comunicación en este tipo de sistemas.

3.2.4.2. Características basadas en requerimientos de seguridad.

- Según el estudio realizado en La Empresa, se requiere un mínimo de 62 lectoras nuevas (ver Tabla 4.4. del Capítulo 4).
- Las lectoras deben tener un alcance mínimo de 10 cm. para permitir un avance rápido en las zonas de mayor tránsito.
- Las lectoras de proximidad deben cumplir con las normas UL y FCC. Estas normas garantizan la calidad de los equipos.

3.2.5. Características de las lectoras de proximidad de largo alcance.

3.2.5.1. Características basadas en la integrabilidad.

- Las lectoras a instalar deben ser compatibles con las lectoras existentes en La Empresa: Indala Flex Pass Motorola. Con esta característica La Empresa busca disminuir sus gastos reutilizando lo que aún sirve.
- Las lectoras deben soportar el Protocolo Wiegand, según documento “SIA AC-01-1996.10” de los Estándares SIA, acreditados por la ANSI.

3.2.5.2. Características basadas en requerimientos de seguridad.

- Para asegurar la comodidad del usuario, las lectoras deberán tener un alcance mínimo de 50 cm.
- Se requieren como mínimo 6 lectoras para la zona de ingreso vehicular (Ver Tabla 4.4).
- Las lectoras deben estar diseñadas para actuar en exteriores, teniendo en cuenta el clima húmedo de la ciudad y las lluvias.

3.2.6. Interfaz Wiegand.

3.2.6.1. Características basadas en la integrabilidad.

La interfaz debe soportar el Protocolo Wiegand, según documento “SIA AC-01-1996.10” de los Estándares SIA, acreditados por la ANSI.

3.2.6.2. Características basadas en requerimientos de seguridad.

- Debe contar con mínimo 2 entradas de relés supervisadas para recibir alarmas de eventos de alta prioridad, como cuando se fuerza una puerta o se intenta alterar el funcionamiento de la lectora.
- Debe contar con mínimo 2 salidas de relés supervisadas para generar alarmas de eventos de alta prioridad, para avisar inmediatamente al sistema si algún evento ha sucedido, como cuando se fuerza una puerta o se intenta alterar el funcionamiento de la lectora.

3.2.7. Barreras vehiculares.

La Empresa cuenta con tres puertas vehiculares, en la puerta de mayor tamaño se requiere un solo brazo para entrada y salida, en las otras 2 se requieren 2 brazos por cada puerta, por lo tanto se requiere:

- Cuatro barreras vehiculares para brazo de tres metros.
- Cuatro brazos de tres metros de aluminio con protector de caucho cada uno.
- Una barrera vehicular para brazo de seis metros.
- Un brazo de seis metros de aluminio con protector de caucho.
- Lazo de sensado de autos en las puertas, dos por puerta, entrada y salida, en total seis.

3.2.8. Tarjetas de proximidad.

3.2.8.1. Características basadas en la integrabilidad.

Compatibilidad con lectoras existentes en La Empresa: Indala Flex Pass Motorola para que se puedan reutilizar las lectoras instaladas en el edificio.

3.2.8.2. Características basadas en requerimientos de seguridad.

- Deberá soportar como mínimo el uso de 3000 tarjetas de proximidad. En el edificio laboran cerca de 1200 personas, pero según el Departamento de Seguridad, en momentos donde hay un mayor tráfico de visitantes, la cantidad ha llegado a rebasar las 2000 personas, por lo que el número requerido cubre el peor de los casos.
- Las tarjetas deberán ser del tipo pasivas para evitar el problema del cambio de batería en las tarjetas activas.
- No deben existir duplicados de tarjetas, lo cual debe estar garantizado por escrito por el fabricante.
- El material de la tarjeta debe ser rígido y debe permitir la impresión de textos y fotografías. El material debe garantizar una durabilidad mínima de 3 años en condiciones de uso normales.
- El diseño de la tarjeta debe contener la foto del usuario y el logotipo de La Empresa para que pueda ser identificada en forma visual.

3.2.9. Integración con el Sistema de Control de Incendios.

El sistema deberá estar preparado para recibir señales del Sistema de Control de Incendios, en caso de emergencia, el Sistema de Control de Accesos debe liberar todas las puertas como primera prioridad, es decir, la liberación de las puertas se realizará inmediatamente después de generada la alarma de incendios sin importar otros eventos.

3.2.10. Baterías para voltaje auxiliar.

El sistema deberá contar con un sistema de baterías que permita la autonomía del sistema en caso de corte de energía por lo menos 2 horas. En este tiempo La Empresa podrá activar su sistema de energía alterno.

3.2.11. Accesorios para las puertas.

En el diseño se debe tener en cuenta que en las puertas que serán controladas por las lectoras se deberá instalar Seguros Electromagnéticos (SEM) y brazos hidráulicos que aseguren que las puertas permanezcan cerradas.



CAPÍTULO 4

Diseño del Sistema de Control de Accesos.

4.1. Introducción.

El presente capítulo tiene como objetivo elegir el sistema que satisfaga de la mejor manera las necesidades de La Empresa, teniendo en cuenta los requerimientos tecnológicos y lo que el mercado ofrece.

4.2. Selección del Sistema.

Para la selección del sistema a utilizar se han tenido en cuenta tres factores: Los requerimientos obtenidos de La Empresa, los sistemas que ofrecen la empresas en el rubro de seguridad electrónica y el hecho de que el proceso de automatización involucra una solución global centralizada que integre a todos los sistemas electrónicos del edificio.

El proceso de obtención de requerimientos de La Empresa fue realizado en continua comunicación con las empresas especializadas ya que el objetivo era que los requerimientos estén acordes a lo que el mercado ofrece. Gracias a esto, todas las empresas consultadas finalmente contaban con sistemas que podían satisfacer estos requerimientos, con excepción del tema del Protocolo de Compresión ACC.

El formato ACC es de características propietarias, es decir, sus códigos no pueden ser leídos ni manipulados por equipos que no sean del mismo fabricante, en este caso, de la empresa American Dynamics. Si bien éste formato presenta un gran desempeño en el tema del CCTV, por sus característica de compresión y por la seguridad que ofrece, perjudica en el sentido de que no puede establecer comunicación con equipos de diferentes fabricantes.

Para que el Sistema de Control de Accesos opere con el desempeño deseado debe poder comunicarse con el CCTV, ya que ambos son sistemas de seguridad y en

caso de producirse alguna alarma en los controles de accesos, estos sistemas deben actuar en conjunto para ofrecer la mejor herramienta.

Por lo tanto, para el diseño del Sistema de Control de Accesos se decidió utilizar el sistema ofrecido por la empresa American Dynamics, que cumple con los requerimientos recogidos de La Empresa, puede comunicarse con el CCTV sin ningún problema y además permite el uso de hardware de otras marcas gracias a que utiliza el protocolo Wiegand, estándar en sistemas de control de accesos.

4.3. Sistema de Control de Accesos seleccionado.

En el capítulo 2 se presentó la estructura de los Sistemas de Control de Accesos que ofrecen las empresas que fueron consultadas para el desarrollo de la presente tesis, a continuación se procederá a indicar los modelos de los equipos que forman parte del sistema seleccionado.

Descripción	Modelo seleccionado
Software del Sistema	Software House C CURE 800/8000
Servidor del sistema	Servidor Dell Power Edge 840
Panel Controlador de Lectoras	iSTAR Pro
Lectora de proximidad peatonales	HID Indala Standard Card Readers
Lectora de proximidad de largo alcance	HID Indala Long Range Card Readers
Interfaz Wiegand	Software House RM-4
Barreras Vehiculares	BA 1200 de alta velocidad y BA 7000
Tarjetas de proximidad	HID Indala Flex Card
Interfaz de integración con el Sistema Contra Incendios	Software House ACM-8
Software de Integración con CCTV	Software House Net Vue

Tabla 4.1. Sistema de Control de Accesos seleccionado

4.3.1. El Software del Sistema

El sistema Software House C CURE 800/8000 (Figura 4.1.) presenta las siguientes características principales:

4.3.1.1. Integración

Se integra con las aplicaciones más importantes del edificio, tales como CCTV, los ERP, alarma de incendios y otros tipos de alarmas. Es capaz de ejecutarse sobre Sistema Operativo Windows XP.

4.3.1.2. Seguridad ideal para empresas del gobierno

Gracias a su mecanismo de compresión, es ideal para el uso en entidades gubernamentales en donde la seguridad de la información es una gran prioridad.

Cumple con los estándares FIPS, que han sido desarrollados en los Estados Unidos para el uso en entidades de gobierno no militares. Esto garantiza el nivel de seguridad que La Empresa exige en sus requerimientos

4.3.1.3. Niveles de alarmas

El software permite definir prioridades a los eventos que generen señales de alarma. Asimismo permite asignarle color a los diferentes niveles de alarma para facilitar la labor de los operarios que se encuentren monitoreando el sistema.

Figura 4.1. Software House C CURE 800/8000



Imagen tomada de Software House Datasheet

4.3.1.4. Control de los niveles de ocupación de las áreas

El sistema permite configurar un nivel máximo de personas que pueden estar en una determinada área al mismo tiempo. En caso se exceda el número, se activará una alarma automáticamente.

4.3.1.5. Capacidad de cambiar el comportamiento del sistema en casos de emergencia.

El sistema puede ser configurado para actuar de diferente forma en situaciones de emergencia, por ejemplo, en casos de que se sospeche de algún intruso en el edificio se puede llevar el sistema a un estado tal que los accesos de mayor prioridad, como Presidencia o Gerencia General, solo puedan ser activados por personal de Seguridad.

4.3.1.6. Interfaz gráfica para manejo de Control de Accesos

Es posible importar archivos del tipo .bmp, de esta manera se puede tener el control de accesos situado en los planos reales del edificio y poder saber exactamente el lugar donde se están produciendo los eventos. Además, es posible generar reportes personalizados de los eventos.

4.3.2. Selección del servidor del sistema

Los requisitos mínimos recomendados del software de Control de Accesos se muestran en la tabla 4.2.

Procesador	2.4 GHz Intel Pentium IV o superior
Disco Duro	10 GB de espacio libre
Sistema Operativo	Windows Server 2003
Memoria RAM	Memoria RAM de 2GB
Puertos	2 puertos Seriales, 1 Paralelo y USB
Tarjeta de red	Tarjeta de Red 10/100 Base-T

Tabla 4.2. Requisitos mínimos del Software del Sistema

En vista de que es necesario cumplir con estos requerimientos además de los requerimientos de La Empresa, se ha optado por seleccionar un servidor con características específicas indicadas en el pedido, las características seleccionadas, teniendo en cuenta todos los requerimientos, se muestran en la tabla 4.3.

Procesado	Dual Core Intel® Xeon® 3050, 2MB Cache, 2.13GHz
Bus del sistema	1066 MHz
Sistema Operativo	Windows Server® 2003 R2, Standard x64 Edition
Memoria RAM	2GB DDR2, 667MHz, 4x512MB "Single Ranked" DIMMs
Disco Duro	80GB, SATA, 3.5-inch, 7.2K RPM Hard Drive
Dispositivo Óptico	Combo 24X CDRW/DVD (CDRWDVD)
Tarjeta de Red	Tarjeta de Red Integrada 10/100/1000
Monitor	Dell 17 Inch Analog FP LCD
Teclado	Teclado Silencioso Dell USB, Inglés (USBK4)
Mouse	Optical Two-Button Mouse, USB
Módem	56K Internal Modem (INMODM)
Garantía	3 años de garantía en partes y mano de obra con servicio en sitio

Tabla 4.3. Servidor Dell Power Edge 840

El procesador de doble núcleo seleccionado ofrece mejores prestaciones que el del Procesador Intel® Xeon de 3Ghz de un solo núcleo que se usa en La Empresa.

La memoria de 2GB fue seleccionada debido a las características del Software del Sistema. Asimismo, el servidor cuenta con un grabador de Cd's para poder extraer información del sistema.

Figura 4.2. Servidor Dell Power Edge 840



Imagen tomada de Dell.com

4.3.3. Panel Controlador de Lectoras

El iSTAR Pro es el equipo seleccionado. Se encarga de tomar las decisiones en los intentos de acceso en tiempo real. Asimismo cuenta con aprobación de las normas UL Y FCC.

Entre sus características principales se contemplan:

4.3.3.1. Fácil de configurar con DHCP

El controlador soporta el protocolo DHCP, lo que le permite al administrador de red asignarle una dirección IP al equipo cuando se conecta a la red.

4.3.3.2. Ofrece una comunicación efectiva cuando trabaja en grupo

El iSTAR Pro soporta comunicación Ethernet, RS-232 y además cuenta con una ranura PCMCIA para comunicaciones de otro tipo.

Los grupos de trabajo son formados por hasta 16 controladores, en una configuración del tipo Maestro-Esclavo. El Maestro es el encargado de regir la comunicación entre el Servidor y los demás controladores del grupo, es decir, al producirse algún evento, este es comunicado primero al controlador maestro y luego este le envía la información al Servidor. El sistema está preparado para operar aún sin presencia del servidor.

4.3.3.3. Capacidad para actuar con programación 'Anti-passback'.

La programación 'Anti-passback' asegura que una misma tarjeta no pueda abrir una puerta dos veces si antes esa tarjeta no ha pasado por la lectora de salida de la puerta.

Gracias a que los controladores trabajan en grupos de trabajo, todos los controladores pueden manejar una misma base de datos de entradas y salidas, esta única base de datos permite la programación 'Anti-passback'.

4.3.3.4. Seguridad en los datos.

El controlador iStar Pro cuenta con un mecanismo de encriptación de 256 bits denominado ciphertext. Este mecanismo asegura que la información que se transfiera a través de los medios de comunicación no pueda ser alterada y plagiada por agentes externos al sistema.

4.3.4. Lectoras

Las lectoras a instalar: Peatonales, HID Indala Standard Card Readers y de largo alcance, HID Indala Long Range Card Readers son de la misma familia que las lectoras existentes en el edificio, por lo que estas se reutilizaran en su totalidad, generando así un ahorro a La Empresa. Ambos modelos son compatibles con el protocolo de comunicación Wiegand.

Figura 4.3. Panel Controlador iSTAR Pro

Imagen tomada de Software House Datasheet

4.3.4. Lectoras

Las lectoras a instalar: Peatonales, HID Indala Standard Card Readers y de largo alcance, HID Indala Long Range Card Readers son de la misma familia que las lectoras existentes en el edificio, por lo que estas se reutilizarán en su totalidad, generando así un ahorro a La Empresa. Ambos modelos son compatibles con el protocolo de comunicación Wiegand.

4.3.4.1. Las lectoras peatonales: HID Indala Standard Card Readers

Estas son lectoras de proximidad, cuentan con un rango de sensibilidad de hasta 12cm, lo que da al usuario cierta comodidad al momento de registrar su ingreso. Este rango cubre con el requerimiento de La Empresa de mínimo 10 cm. De rango.

Tienen un consumo de corriente de 65mA y se alimenta con auto voltaje en un rango de 4 a 16 v. La alimentación de energía viene directamente del controlador principal a través de la línea de datos. Al ser voltaje continuo no genera interferencia a la señal de datos.

Figura 4.4. Lectora de proximidad: HID Indala Standard Card Readers



Imagen tomada de Indala Flex Secure Datasheet

4.3.4.2. Las lectoras de largo alcance: HID Indala Long Range Card Readers

Estas son lectoras de proximidad, cuentan con un rango de sensibilidad de hasta 66 cm., lo que evita que el usuario tenga que bajar del auto cuando tenga que acceder al edificio. Este rango cubre el requerimiento de La Empresa de mínimo 50 cm. de rango.

Las lectoras de largo alcance tienen un consumo de corriente de 750mA y se alimenta con auto voltaje en un rango de 12 a 24 v. La alimentación de energía viene directamente del controlador principal a través de la línea de datos. Al ser voltaje continuo no genera interferencia a la señal de datos.

4.3.5. Interfaz Wiegand: Software House RM-4

El Software House RM-4 crea la conectividad entre el Controlador y las lectoras. Cuenta con dos entradas supervisadas de relé, que en este caso son usadas para sensar los seguros electromagnéticos y el estado de las puertas, y dos salidas de relé para activar alarmas, como sirenas o luces.

Cada una de estas interfaces está preparada para comunicar una lectora con el Panel controlador, por lo tanto se tendrá la misma cantidad de lectoras que Interfaces Wiegand.

Esta interfaz es fundamental en el desempeño del sistema ya que permite que se puedan agregar lectoras de tarjetas sin que haya la necesidad de que estas lectoras sean de la misma marca del sistema. Esta característica permite al usuario aumentar los terminales sin tener que estar supeditado a los precios de un solo fabricante.

4.3.6. Software de integración con el CCTV, Software House C CURE NetVue

Este software actúa como una interfaz entre el software del CCTV y el Sistema de Control de Accesos, entre sus principales funcionalidades se tiene:

- Permite al Software de Control de Accesos recibir imágenes del CCTV de American Dynamics.
- Permite ver eventos del CCTV, en vivo o grabados, desde el software de Control de Accesos.
- Permite manejar el zoom de las cámaras desde el software de Control de Accesos.

Figura 4.5. Lectora de proximidad: HID Indala Long Range Card Readers



(Imagen tomada de Indala Flex Secure Datasheet)

Figura 4.6. Interfaz Wiegand: Software House RM-4



Imagen tomada de Software House Datasheet

- Ver hasta 4 imágenes de video del CCTV en simultáneo.
- La activación automática de ventanas de video en el software de Control de Accesos cada vez que se produce una alarma en el sistema.
- Las características de seguridad de este software que la grabación original de video no pueda ser alterada en ningún sentido.
- Permite manipular las ventanas de video, moverlas y cambiar sus dimensiones.

4.3.7. Barreras Vehiculares

4.3.7.1. Barrera vehicular de 3 metros: BA 1200 Alta Velocidad.

- Según el catálogo: Modelo de alta velocidad y uso intensivo Tiempo de apertura y cierre: 1,2 segundos. El mecanismo posee una transmisión de engranajes que optimiza el funcionamiento del motor logrando una mayor velocidad en el ciclo de maniobra. Este tipo de transmisión simple asegura una vida útil muy prolongada del equipo. Esta diseñada para soportar lanzas de hasta 3 metros, de sección redonda o rectangular. El motor que acciona la barrera tiene una potencia de 1/5 de HP

Figura 4.7. Software House C CURE NetVue



Imagen tomada de Software House Datasheet

4.3.7.2. Barrera vehicular de 6 metros: BA 7000

Según el catálogo: Modelo caracterizado por poseer doble lanza de hasta 7 metros. Se accionan con un motor de 1/3 de HP. Realiza la apertura y el cierre en 8 segundos. La transmisión se realiza directamente desde el motor al eje que soporta la lanza.

4.3.8. Tarjetas de Proximidad: HID Indala Flex Card

Estas tarjetas son fabricadas con un material de larga duración, sus dimensiones son similares a las de una tarjeta de crédito, por lo que puede ser guardado en cualquier billetera o tarjetero. El modelo se aprecia en la Figura 4.8.

Figura 4.8. Tarjetas de proximidad



Imagen tomada de Indala Flex Secure Datasheet

Figura 4.7. Barrera Vehicular

Imagen tomada de <http://www.tecron.com.ar>

4.3.9. Interfaz de integración con el Sistema Contra Incendios: Software House ACM-8.

Esta interfaz permite la comunicación entre el Sistema de Control de Incendios y el Sistema de Control de Accesos en caso de alguna emergencia. En caso ocurra este suceso, el ACM-8 inmediatamente enviará una señal directa a los seguros electromagnéticos de las puertas y los abrirá sin importar lo que el Sistema de Control de Accesos disponga.

4.4. Esquema final del sistema.

En la figura4.9. se muestra el esquema del sistema seleccionado.

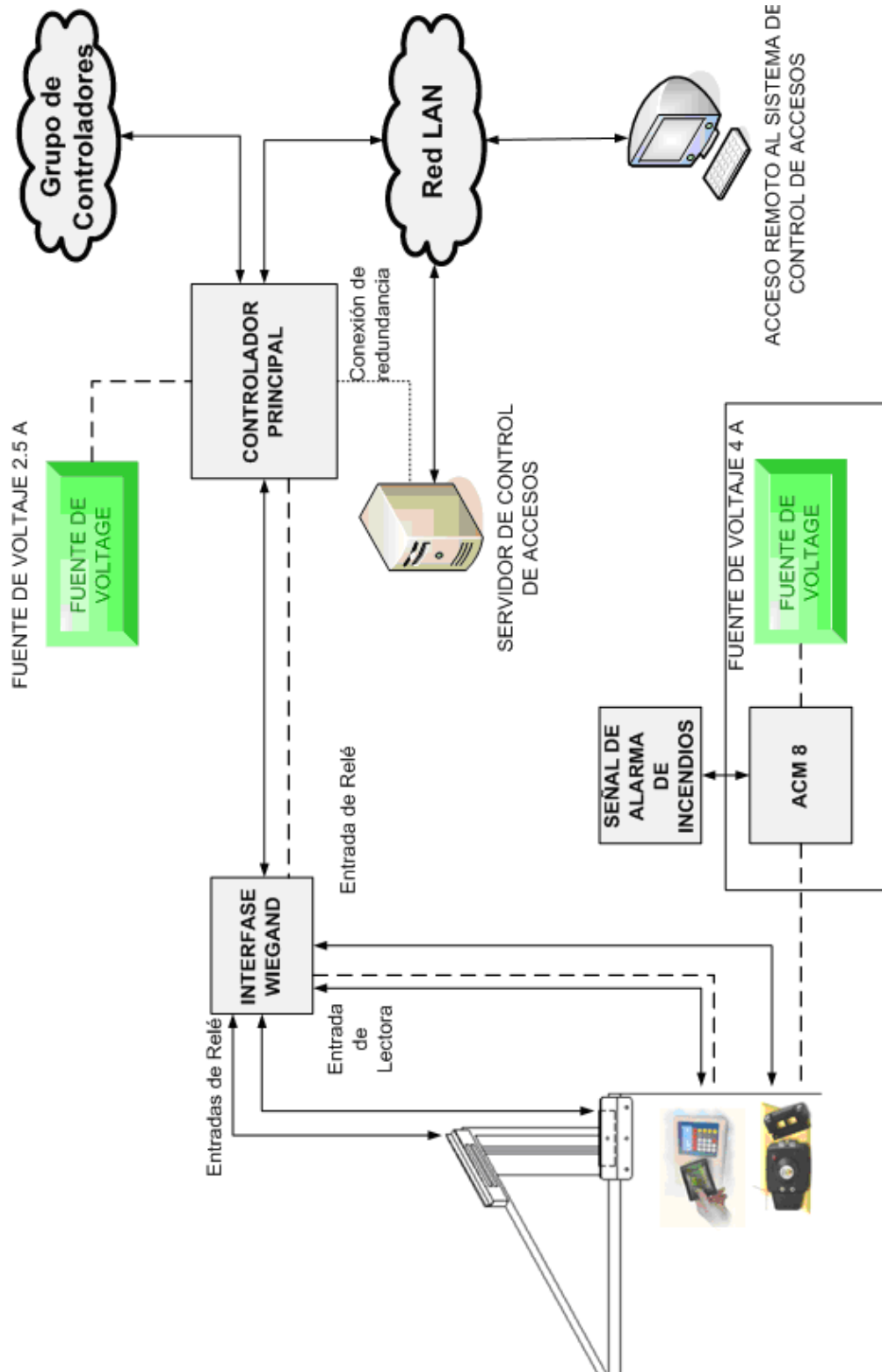


Figura 4.9. Esquema Final del Sistema

Las líneas continuas representan transmisión de datos, las discontinuas son de alimentación y la punteada representa la conexión redundante.

La lectora que se aprecia en el esquema está conectada a la Interfaz Wiegand, de tal manera que cuando recibe información la envía al controlador a través de la interfaz.

El seguro electromagnético está siendo alimentado por una fuente a través del ACM-8. La función de este equipo es sensar si el Sistema de Control de Incendios envía alguna señal de alarma, en caso de que esto ocurra, le enviará una señal al seguro para que libere la puerta sin importar ninguna otra condición.

Además la interfaz Wiegand está sensando constantemente el estado del seguro y de los sensores magnéticos que indican si la puerta está abierta o cerrada. En caso de que detecte anomalías en éstos dispositivos emitirá una alarma al sistema.

El controlador principal está conectado a la Red LAN de La Empresa para poder tener conectividad con el Servidor del Sistema y las estaciones remotas. Además se ha dispuesto una conexión redundante con el Servidor del Sistema mediante protocolo RS-485 para evitar la interferencia por largas distancias.

Asimismo, todos los controladores estarán conectados entre sí mediante cable trenzado, apantallado y usando protocolo RS-485 para no tener problemas con las largas distancias.

Se ha seleccionado la fuente de 2.5 A para el Controlador Principal debido a que la alimentación de la interfaz y de las lectoras será mediante esta fuente. En el peor de los casos, con 16 lectoras, 16 Interfaces Wiegand y 1 Controlador Principal se tendrá un consumo total de:

16Lectoras	x	0.05 Amperios/lectora	=	0.96	Amperios
16 Interfaces	x	0.05 Amperios/Interfaz	=	0.96	Amperios
1 Controlador	x	0.5Amperios/Controlador	=	0.5	Amperios

Se aprecia que en el peor de los casos esta fuente proporcionará 2.1 Amperios, se elige 2.5 amperios que cubre el caso en el que todos los dispositivos consuman el máximo de energía.

Se elige la fuente de 4 Amperios debido a que cada una manejará 5 seguros electromagnéticos de 600 libras, donde cada uno consume 0.5 Amperios. Por lo tanto, la máxima cantidad de corriente que proporcionará la fuente es de 2.5 Amperios, conservando un factor de reserva de 1.5 Amperios.

Con respecto a las lectoras de largo alcance, se decidió darles alimentación independiente ya que las largas distancias podían ocasionar caídas de potencial que repercutirían en el desempeño del sistema. Se decidió instalar lazos por debajo de las pista ubicadas en las tres entradas vehiculares del edificio para evitar que el brazo metálico baje cuando un auto se encuentre debajo de él. Además se adicionarán protectores de caucho para que los brazos no dañen los autos en caso de que los brazos cuando no deben.

Para la alimentación del sistema, en el presupuesto se ha contemplado la adquisición de una batería por cada fuente, con esto se asegura la total autonomía del sistema cuando haya falta de energía por un período de tiempo.

El servidor del Sistema será instalado en primera instancia en la sala de computadoras del edificio debido a que aún no se cuenta con el centro de control acondicionado. Se ha preferido actuar de esta manera para que el Departamento de Telecomunicaciones pueda supervisar el funcionamiento del sistema durante los primeros meses de funcionamiento antes de ser llevado a seguridad.

4.5. Ubicación de los equipos

En la tabla 4.4. se muestran las ubicaciones de los elementos que componen el Sistema de Control de Accesos. En el presente diseño se reutilizan las lectoras que ya están instaladas en el edificio, para bajar el costo.

Asimismo se mencionan las ubicaciones de Seguros Electromagnéticos (SEM), los sensores de las puertas y de los brazos hidráulicos que aseguran que las puertas se mantengan cerradas.

Las lectoras de largo alcance serán usadas para el estacionamiento, para que los usuarios que entren en sus vehículos no tengan que bajar de los mismos para poder registra su ingreso.

También se puede apreciar que en este sistema la Interfaz Wiegand soporta una lectora cada una, por lo que el número de Interfaces Wiegand es igual a la cantidad total de lectoras usadas, incluyendo las antiguas.



Piso	Lectoras peatonales existentes	Lectoras peatonales requeridas	Lectoras vehiculares requeridas	Interfazs Wiegand	Paneles Controladores	Sensor Magnético de puerta	SEM de 600LBS	Brazo hidráulico
Sot 2	0	2	0	2	Panel #1. Sot 1	2	1	1
Sot 1	3	3	6	12		6	3	3
1	1	4	0	5	Panel #2. Piso 2	4	2	2
2	0	6	0	6		6	3	3
4	0	2	0	2	Panel #3. Piso 5	2	1	1
5	3	7	0	10		10	1	1
11	1	3	0	4	Panel #4. Piso 11	4	2	1
12	1	5	0	6		6	3	2
14	0	2	0	2	Panel #5. Piso 15	2	0	0
15	1	5	0	6		6	3	2
16	1	3	0	4		4	2	1
17	1	3	0	4	Panel #6. Piso 18	4	2	1
18	1	3	0	4		4	2	1
19	1	3	0	4		4	2	1
20	2	4	0	6	Panel #7. Piso 21	6	3	1
21	2	4	0	6		6	3	1
22	1	3	0	4		4	3	1
Totales	19	62	6	87	7 Paneles Controladores	80	36	23

Tabla 4.4. Ubicaciones de los componentes del Sistema

4.6. Cableado.

Para la solución del cableado se usará el entubado existente en el edificio ya que el cableado de datos es apantallado y no inducirá ruido a los demás pares del tubo. Para el sistema se usaran tres tipos de cables:

a) Belden 8741: (AWG22) este cable es usado generalmente para telefonía o comunicaciones en el área de control para los sensores. Cada cable cuenta con dos pares de conductores y será usado para la comunicación entre las entradas de relé de las Interfaces Wiegand y los sensores de las puertas. Sus características eléctricas más importantes son las siguientes:

Capacitancia Nominal a 1KHz	30 pF/ft
Resistencia DC @ 20°C	16.5 Ohms/1000 ft
Voltaje máximo @ 20°C	300 V RMS
Corriente máxima recomendada @ 20°C por conductor	2.8 Amps

Tabla 4.5. Características eléctricas del cable Belden 8741

Los sensores magnéticos de las puertas actúan en el orden de 0 y 12 v, y manejan corrientes del orden de los mA por lo que el cable manejará la comunicación sin ningún problema.

Cabe mencionar que el cable fue recomendado por el fabricante del sistema, ya que lo usa constantemente en las instalaciones de éstos.

b) Belden 9842: (AWG24) cable trenzado y apantallado, será utilizado para la comunicación mediante protocolo RS-485 y la comunicación mediante protocolo Wiegand. Cuando se aterra su pantalla presenta un buen desempeño frente al ruido exterior, y permite transmitir señal a lo largo de distancias de hasta 1000 metros.

Entre sus principales características eléctricas se encuentran:

Capacitancia Nominal@ 1 KHz	12.8 pF/ft
Velocidad de propagación nominal	66%
Retardo Nominal	1.6 ns/ft
Resistencia DC nominal @ 20°C del conductor	24 Ohms/1000 ft
Resistencia DC nominal @ 20°C de la pantalla	3.4 Ohms/1000 ft
Voltaje máximo	300 V
Corriente máxima recomendada	2.1 A

Tabla 4.6. Características eléctricas del cable Belden 9842

c) Cables de poder: La alimentación de las lectoras, el Controlador y las interfaces Wiegand se realiza desde la fuente conectada al Controlador, como se muestra en el esquema del sistema. Para la selección de este cable se tomo la máxima corriente que puede dar la fuente, 2.5 amperios y una temperatura máxima de operación de 75 °C.

Los Seguros Electromagnéticos tienen alimentación independiente, para este caso se toma también una temperatura máxima de operación de 75 °C, pero con una corriente nominal de 4 amperios.

Para el caso de las lectoras de largo alcance, que manejan corrientes de 750mA se utilizarán fuentes independientes debido a su ubicación y consumo. La temperatura máxima de operación para este tramo se considerará de 75°C al igual que en los casos anteriores.

Para los casos mencionados se utilizará el cable THW de 1.5 mm, que trabaja con una corriente máxima de 12 amperios y tiene una temperatura máxima de operación de 75°C.

El metrado del cableado se realizó en los planos teniendo en cuenta el hecho de que éste irá por el falso techo y bajará por la pared verticalmente hacia la lectora, el

entubado existente en el edificio será reutilizado para este sistema, se ha verificado que estos tubos tienen capacidad para alojar los cables del Sistema de Control de Accesos. El hecho de que el cableado de datos sea apantallado proporciona la ventaja de que no induce ruido a los demás cables existentes, ni estos le inducen ruido a él, por lo que no existe problema en que viajen los cables juntos.

En la página siguiente se muestra la longitud de los cables en los pisos del edificio, esta longitud se halló utilizando los planos del edificio. En esta parte es necesario mencionar que debido a la seguridad que La Empresa desea mantener en sus instalaciones se ha considerado necesario no mostrar los planos en la presente tesis.



Piso	Cableado de datos por techo (m)	Distancia Techo-Lectora (m)	Cableado total de datos(m)	Factor de reserva	Cableado total de datos con reserva (m)	Cableado total de poder con reserva (m)	Cableado total de sensores con reserva (m)
Sot 2	21.36	1.2	23.76	1.2	28.512	28.512	1.44
Sot 1	284.93	1.2	299.33	1.2	359.196	164.036	4.32
1	129.98	1.2	135.98	1.2	163.176	163.176	2.88
2	69.41	1.2	76.61	1.2	91.932	91.932	4.32
4	27.06	1.2	29.46	1.2	35.352	35.352	1.44
5	90.68	1.2	102.68	1.2	123.216	123.216	1.44
11	44.26	1.2	49.06	1.2	58.872	58.872	2.88
12	44.58	1.2	51.78	1.2	62.136	62.136	4.32
14	31.22	1.2	33.62	1.2	40.344	40.344	0
15	45.1	1.2	52.3	1.2	62.76	62.76	4.32
16	36.03	1.2	40.83	1.2	48.996	48.996	2.88
17	36.03	1.2	40.83	1.2	48.996	48.996	2.88
18	34.79	1.2	39.59	1.2	47.508	47.508	2.88
19	36.03	1.2	40.83	1.2	48.996	48.996	2.88
20	37.75	1.2	44.95	1.2	53.94	53.94	4.32
21	38.61	1.2	45.81	1.2	54.972	54.972	4.32
22	35.95	1.2	40.75	1.2	48.9	48.9	4.32
Totales	1043.77	1.2	1148.17	1.2	1377.804	1182.644	51.84

Tabla 4.7 Longitud de cables del Sistema de Control de Accesos

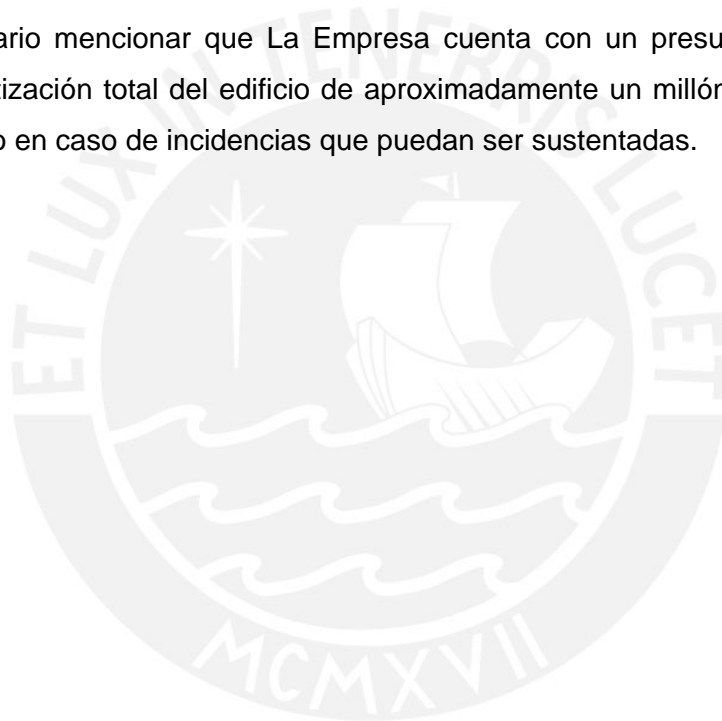
Nótese que la longitud de los cables de poder es igual a la longitud de los cables de datos en casi todos los pisos, excepto en el Sótano 1, ya que las lectoras de largo alcance tienen alimentación independiente.

4.7. Costo de los equipos y accesorios

A continuación se muestra la tabla 4.8. con los costos de los equipos necesarios para la implementación del sistema. La justificación de cada uno de los equipos mostrados se ha realizado en el capítulo 3 y el capítulo 4 de la presente tesis.

Los precios indicados fueron en su mayoría proporcionados por las empresas especialistas en estos sistemas. Para el costo del cableado se utilizó la longitud de los cables mostrada en los planos que se adjuntan y se muestran en la tabla anterior.

Es necesario mencionar que La Empresa cuenta con un presupuesto estimado para la automatización total del edificio de aproximadamente un millón de dólares, con opción a cambio en caso de incidencias que puedan ser sustentadas.



ITEM	DESCRIPCIÓN	CTD	P. UNIT.	TOTAL
1	Software de control de accesos	1	9,375.00	9,375.00
2	Software de integración con grabador de video digital	1	3,500.00	3,500.00
3	Servidor de control de accesos	1	9,791.00	9,791.00
4	Panel controlador inteligente para 16 lectoras, memoria de 50MB. Conexión IP hasta el servidor.	7	9,750.00	68,250.00
5	Gabinete para Panel controlador. Incluye display LCD 16 caracteres	7	500.00	3,500.00
6	Lectora de proximidad peatonal Indala 10-12cm	62	270.00	16,740.00
7	Lectora de proximidad de largo alcance: 71cm. Marca Indala	18	1,030.00	18,540.00
8	Interfaz wiegand para lectoras de proximidad y control de dispositivos de puerta	99	330.00	32,670.00
9	Tarjetas de Proximidad Indala	3000	6.00	18,000.00
10	Interfaz de integración con Panel de alarma de incendio (ACM8).	36	250.00	9,000.00
11	Servicio de impresión de tarjetas	3000	2.60	7,800.00
12	Seguro Electromagnético de 600lb	36	170.00	6,120.00
13	Cierra puerta hidráulico	23	180.00	4,140.00
14	Sensores Magnéticos	80	12.00	960.00
15	Barrera vehicular para brazo de 3m	4	2,800.00	11,200.00

16	Barrera vehicular para brazo de 6m	1	3,500.00	3,500.00
17	Brazo de aluminio de 3m	4	256.00	1,024.00
18	Brazo de aluminio de 6m	1	321.00	321.00
19	Protector de caucho para brazos de aluminio	5	88.00	440.00
20	Sensor de detección de vehículo	6	120.00	720.00
21	Fuente de poder 2.5A centralizada protegido por fusibles para lectoras de largo alcance	6	275.00	1,650.00
22	Fuente de poder 2.5A centralizada protegido por fusibles para lectoras y panel controlador	7	275.00	1,925.00
23	Fuente de poder 4A centralizada protegida por fusibles para seguros electromagnéticos	36	315.00	11,340.00
24	Baterías 12v 12amp/h	43	88.00	3,784.00
25	Gabinetes para baterías y fuentes	43	60.00	2,580.00
26	Cables de data y voltaje	1	4,200.00	4,200.00
27	Instalación del Sistema y Capacitación	1	10,000.00	10,000.00

Total (\$)	251,080.00
I.G.V. (\$)	47,705.20
Total con I.G.V. (\$)	298,785.20

Tabla 4.8. Costos de los Equipos y Accesorios

Conclusiones

El diseño del Sistema de Control de Accesos se desarrolló teniendo en cuenta la tecnología con la que dispone el Edificio de Oficinas. Asimismo, se llevaron a cabo reuniones con los Departamentos involucrados para obtener un producto final de acuerdo a los requerimientos de La Empresa. Durante todo el desarrollo de la tesis se contó con asesoramiento de empresas técnicas especializadas que ayudaron tener una mejor visión de lo que ofrece el mercado.

Se logró llevar una comunicación clara con los interesados en el proyecto, tanto con los proveedores como con La Empresa. Gracias a esto se realizó una retroalimentación constante a lo largo del desarrollo de la tesis, lo que repercutió en un producto final de mejor calidad.

Con respecto a la parte técnica, en el diseño de este tipo de sistemas es necesario siempre tener en cuenta la capacidad que tengan estos equipos para interactuar con otros equipos electrónicos de diferente fabricante. En la actualidad se busca que los sistemas puedan comunicarse entre sí para poder obtener el máximo de beneficios de los mismos. Los equipos de características propietarias, es decir, que solo pueden comunicarse con equipos de la misma marca, son cada vez menos usados en los diseños de sistemas ya que limitan la expansión del mismo.

Un punto muy importante para la selección del sistema fue el hecho de que el Circuito Cerrado de Televisión de La Empresa maneja un formato de compresión de características propietarias. El Sistema de Control de Accesos es el sistema que debe interactuar más con el CCTV y por lo tanto es necesario que maneje el mismo formato para que la comunicación entre los dos sistemas se pueda dar de manera fluida. Sin embargo, este punto debe ser considerado como una desventaja que ahora tiene La Empresa, ya que siempre que se requiera instalar un sistema nuevo, las empresas que deseen proveer este sistema deberán tener en cuenta el formato propietario que se maneja, reduciendo cantidad de proveedores interesados en darle este servicio a La Empresa.

A propósito de la labor de ingeniería, es preciso mencionar en esta parte del análisis la continua labor administrativa a la que están expuestos los ingenieros en las empresas, si bien el conocimiento técnico es importante, también lo son las estrategias de gestión que se van adquiriendo. La comunicación con las personas es un tema elemental en los proyectos, una de las partes más importantes de esta tesis ha sido el conjunto de reuniones que se tuvieron con los departamentos interesados de La Empresa y con las empresas técnicas especializadas. En este nivel uno tiene que actuar como un traductor entre lo que La Empresa necesita y lo que el mercado puede proporcionar. Fue necesario interactuar mucho con las personas involucradas, teniendo en cuenta que no se puede hablar de la misma manera con una persona especializada en seguridad electrónica que con otra especializada en el tema de seguridad empresarial.

Con respecto al costo total del sistema, según consultas hechas a diferentes proveedores, el monto es similar al que presentan otros fabricantes. El monto representa aproximadamente la cuarta parte de lo que La Empresa tiene planeado invertir en la automatización del edificio por lo que se encuentra dentro del rango de lo que se espera gastar.

Recomendaciones

Con respecto a la parte técnica, La Empresa debe esforzarse por evitar adquirir sistemas del tipo propietario ya que éstos solo pueden actuar con total eficiencia con los sistemas de su misma marca. Con respecto al problema que existe actualmente con el protocolo de compresión ACC, es necesario hacer un estudio de las posibilidades que hay de utilizar otro formato, o bien encargar a alguna entidad el diseño de un software que actúe como conversor de este formato a uno abierto, o en su defecto, que al menos permita visualizar las imágenes desde dispositivos de otras marcas.

La instalación del sistema debe realizarse durante días en los que no haya gente laborando, para no interferir con sus funciones. Se considera, según expertos consultados, que trabajando un fin de semana en turnos de día y noche el sistema puede ser implementado. Se recomienda que se realicen pruebas en cada una de las lectoras cuando el sistema termine de instalarse, además, parte del personal encargado de la instalación deberá asistir a La Empresa durante toda la primera semana de funcionamiento del sistema para que pueda solucionar cualquier problema que se presente.

Es preciso instalar lo antes posible el Sistema de CCTV a lo largo de todo el edificio, sobre todo en los lugares en donde hay lectoras, ya que esto permitirá identificar de manera más rápida cualquier eventualidad que ocurra.

Es necesario implementar el centro de control para poder instalar definitivamente los sistemas de seguridad, el mejor desempeño se conseguirá teniendo todos los sistemas trabajando en forma centralizada, ya que los operarios podrán tener un control de la seguridad del edificio desde un solo lugar.

Es necesario que las empresas estatales agilicen el tema burocrático para que puedan obtener resultados más rápidos. Si bien es necesario llevar un orden en las acciones que se realizan, es posible valerse de herramientas informáticas para tener un mejor manejo de esta situación.

Se recomienda que las puertas vehiculares estén ubicadas dentro de las rejas del edificio o, en caso contrario, que cuenten con algún tipo de protección adicional. Esto debido a que en el edificio laboran otras entidades estatales que muchas veces provocan marchas frente al edificio que pueden dañar el sistema.

Con respecto al punto de vista tecnológico, es recomendable que se trabaje el tema de los protocolos de comunicación propietarios. Si se cuenta con las herramientas necesarias es posible desarrollar conversores de protocolos que permitan a las empresas dejar de estar ligadas a sistemas que las obliguen a usar equipos de un solo fabricante.

Durante el transcurso de las reuniones que se llevaron a cabo con las empresas especializadas en sistemas de seguridad electrónicos se pudo observar que cada una de estas orientaba sus consejos a la selección de equipos de su marca. Esto constituye un problema para La Empresa en la medida de que es óptimo que en el concurso público puedan participar la mayor cantidad de empresa. Por lo tanto, se recomienda la creación de grupos de interés en el área de Domótica y que participen activamente en este tipo de procesos brindando asesoría técnica a las empresas que lo requieran.

Fuentes

- [1] Anónimo
2006 Building Integration through oBIX.. Buildings Cedar Rapids
Volumen 100, página 24.
- [2] Arlene Franchini
2005 Cabling Installation and Maintenance Tulsa.
Volumen 13, páginas 20, 22, 24.
- [3] Michel Marriott Lights.
2006 Mood. Video. All at the Touch of a Screen. New York Times .Página 11
- [4] Terry McIver
2005 Building Automation: A Real Turn-On. Contracting Business Cleveland.
Volumen 62, Página 24, 26, 28, 30.
- [5] Matt Chamberlain.
2005 Building Automation Systems Benefit from Resettable Circuit Protection
Volumen 49, Páginas 35-36.
- [6] Carlos Petty
2005 Integration Opportunities. Building Operating Management Milwaukee
Volumen 52, Páginas 69-70, 72, 74.
- [7] John Weaver
2006 Voice Evacuation Becoming Big Priority for Small Installations.
Volumen 100, Página 28.
- [8] Scott Jordan
2003 Spreads the reach of lighting controls.
Volumen 28, Página 16

- [9] Robert Moore
2006 Resetable Over Current Protection for ADSL Equipment: Transmission measurement conducted at the University of New Hampshire ADSL Interoperability Laboratory demonstrate the performance of PPTC circuit protection.
- [10] Milestone
2006 XProtect™ Enterprise version 6.0 is the most comprehensive packaging of IP video surveillance management tools to date.
www.milestonesys.com
- [11] Automated Buildings
2003 Year of the Smart Building.
<http://www.automatedbuildings.com/news/mar05/articles/mcgnw/mcgnw.htm>
- [12] Azsecurity
2006 Cámaras de CCTV
<http://www.azsecurity.net/camaras.htm>
- [13] Nacional FIRE Protection Asociation
2006 NFPA supports Paulison for FEMA Director
<http://www.nfpa.org/newsReleaseDetails.asp?categoryid=488&itemId=28044>
- [14] Amtel Security
2006 Sistema de Control de Accesos
<http://www.amtel-security.com/products/ACS.html>
- [15] Emeral Insight
2006 Emeral Engeneering
<http://www.emeraldinsight.com/Insight/>

- [16] Honeywell
2006 Honeywell Building Solutions
<https://buildingsolutions.honeywell.com/Cultures/en-US/>
- [17] Asicontrols
2006 ASI Controls HVAC and lighting control systems
www.asicontrols.com
- [18] NFPA
2006 Capacitación NPFA
www.capacitacionnfpa.com
- [19] EN54-11 Guidance Notes
2006 www.kac.co.uk/final/PDF/2006/Mark_Guide/EN54-guide.pdf
- [20] Greg Zimmerman
2006 De Facto Standards. Building Operating Management
Career and Technical Education, pg. 30
- [21] Valdis Krebs y June Holley
2006 Building Smart Communities through Network Weaving
- [22] Beau Wardsworth
2006 Smart Building Control applications
- [23] Bosch Praesideo Enterprise
2006 Digital Public Address and Emergency Sound System
- [24] Gill, K. E., and C. W. Hyman,
1995 “Environmental Control of Courthouses—The Next Generation,”
Heating/Piping/Air Conditioning

- [25] Mike Soper
2006 An investment in automation can power major savings
Nation's Restaurant News
- [26] Tecrom
2006 Información de barreras vehiculares
http://www.tecron.com.ar/web%20general/control/compartido/barreras_molinetes/barreras_molinetes.html#barre
- [27] Sensormatic
2006 Recomendaciones al proyecto integral de seguridad electrónica
Sensormatic del Perú S.A
- [28] Eveliux
2006 Estándares de Telecomunicaciones
www.eveliux.com/fundatel
- [29] Enciclopedia Encarta
2006 <http://www.encarta.msn.es>
- [30] Edificios Inteligentes y Cableado Estructurado
2006 Luis Angelo Velarde Criado
- [31] Dra. Ofelia Cervantes Villagómez
2006 Edificios Inteligentes.
pantera.itch.edu.mx:8080/apacheco/expo/view.jsp?file=ai15 - 85k -
- [32] Learn Ethernet
2006 Ancho de Banda
<http://www.learnthenet.com/SPANISH/glossary/bandwth.htm>

- [33] Dell
2006 Selección de servidor
www.lastore.dell.com
- [34] Economía
2006 Diario La República, 14 de Julio de 2006
- [35] Siemens del Perú S.A
2006 Recomendaciones al proyecto integral de seguridad electrónica
- [36] Belden
2006 Catálogo de conductores
www.belden.com
- [37] Software House
2006 Equipo iSTAR
www.swhouse.com/products/hardware_iSTAR.aspx
- [38] Software House
2006 Equipo RM4
www.swhouse.com/products/accessories_RM-4.aspx
- [39] Indala
2006 Tarjetas de acceso
www.indala.com/mediacenter.php?subpage_id=5#flexproducts
- [39] Software House
2006 Software CCURE8000
www.swhouse.com/products/software_CCURE800.aspx