DISEÑO DE UN PROTOTIPO INMÓTICO PARA EL CONTROL DE ACCESO MEDIANTE TARJETAS CON CÓDIGO QR

GERALDINE BRICEÑO FURNIELES

TRABAJO DE GRADO PRESENTADO PARA OPTAR AL TITULO DE INGENIERA MECATRÓNICA

UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA

FACULTAD DE INGENIERÍA FISICOMECÁNICAS

INGENIERÍA MECATRÓNICA

BUCARAMANGA

FEBRERO, 2014

DISEÑO DE UN PROTOTIPO INMÓTICO PARA EL CONTROL DE ACCESO MEDIANTE TARJETAS CON CÓDIGO QR

GERALDINE BRICEÑO FURNIELES

TRABAJO DE GRADO PRESENTADO PARA OPTAR AL TITULO DE INGENIERA MECATRÓNICA

DIRECTOR

M.Sc. EDUARDO CALDERÓN PORRAS

EVALUADOR

PhD. OMAR LENGERKE

UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA

FACULTAD DE INGENIERÍA FISICOMECÁNICAS

INGENIERIA MECATRÓNICA

BUCARAMANGA

FEBRERO, 2014

Nota de Aceptación

M.Sc. Eduardo Calderón Porras
Director del Proyecto

PhD. Omar Lengerke
Jurado

Febrero de 2014

TABLA DE CONTENIDO

INDICE DE FIGURAS

AGRADECIMIENTOS

A mis padres por su apoyo incondicional en todas las metas que me he propuesto y por sus sabios consejos para superar cualquier adversidad que se me ha presentado en todo este trayecto.

A mi segunda familia; mis suegros y mi novio gracias por estar incondicionalmente para mí, ha sido más que un placer tenerlos en mi vida.

A la familia Zafra Rodríguez, gracias por la oportunidad tan grande que me brindaron, fue el gesto mas sincero y especial en mi vida. Mi Dianis eres mi ángel, a ti más que gracias.

A mis amigos y compañeros de aventuras, Rafael, Fredy, Laurenis, gracias por acompañarme y brindarme su valiosa amistad.

A todos mis compañeros de Mecatrónica y Energía que hicieron parte de este proceso, con los que compartí alegrías, tristezas, experiencias durante todo nuestro ciclo universitario.

A Nayibe Chio Cho por su paciencia, colaboración y experiencia durante toda la carrera.

A todos nuestros profesores que en el transcurso de nuestra carrera supieron brindarnos sus conocimientos para finalmente ponerlos en práctica en nuestra vida profesional.

DEDICATORIA

Dedico este trabajo a mis padres, son lo mejor que tengo. Su ejemplo de amor y constancia me han motivado a salir adelante.

INTRODUCCIÓN

En los últimos años, se han presentado numerosos avances en sistemas de control de acceso y seguridad en edificaciones, que brindan bienestar y confort a los usuarios que optan por estos beneficios.

Actualmente, algunas universidades manejan sistemas simples y antiguos, de control de acceso o seguridad, lo cual hace que deban ser sustituidos por mejor tecnología.

Las instalaciones de la facultad de Ingeniería Mecatrónica carecen de un sistema de control de acceso; con el diseño del prototipo inmótico y su futura implementación, se espera optimizar la entrada y los controles de seguridad en tres puntos específicos de la facultad.

1. PLANTEAMIENTO DEL PROBLEMA

En la Universidad Autónoma de Bucaramanga, específicamente el edificio de ingenierías no se tiene un control de acceso a personas en áreas específicas, lo cual hace que sea necesario el estudio e implementación de tecnologías que garanticen la seguridad del edificio, permitiendo la entrada y salida sólo a personal autorizado.

SOLUCIÓN DEL PROBLEMA

Diseñar un prototipo inmótico para el control de acceso en diferentes aulas de la Universidad Autónoma de Bucaramanga, lo cual resulta indispensable para la seguridad, protección ante un robo o usurpación tanto de bienes tangibles como intelectuales dentro del plantel educativo.

El prototipo obedece a un modelo concebido desde una metodología de diseño mecatrónico.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

- Diseñar un prototipo inmótico para el control de acceso mediante tarjetas con código QR.

2.2 OBJETIVOS ESPECÍFICOS

- Estudiar nuevas tecnologías para el control de acceso en áreas críticas de la Facultad de Ingeniería Mecatrónica.
- Conocer los estándares de una red inmótica que pueden ser utilizados para el control de acceso en un área específica.
- Evaluar diferentes alternativas que posibiliten la solución del problema.
- Seleccionar la mejor alternativa para dar solución al problema evaluado.
- Implementar una metodología de diseño mecatrónico que permita dar solución al problema.
- Identificar los diferentes accesos a instalaciones del edificio de ingenierías mediante un esquema.
- Definir la estructura del prototipo de control de accesos.
- Implementar la BeagleBoard XM como un servidor que permita el acceso desde diferentes locaciones.
- Generar códigos QR individuales para autorizar el ingreso a los laboratorios.
- Leer, identificar y procesar los códigos QR mediante la cámara web.
- Visualizar la autorización de ingreso a los respectivos laboratorios.
- Diseñar una interfaz de administrador para gestionar el control de acceso en los laboratorios.

3. ESTADO DEL ARTE

El concepto de edificio inteligente surge en Estados Unidos a finales de la década de los setenta y principio de los ochenta, cuando al desarrollo de las telecomunicaciones se le añade una época donde se produce una elevada actividad en la construcción de edificios de oficinas. A medida que transcurría el tiempo, la idea de edificio inteligente se iba diversificando con mayor intensidad, por lo que se inició una era donde la implementación de automatismos y equipamiento en edificios y grandes superficies marcaba la diferencia. A partir de este momento nace un fenómeno que más tarde fue denominado inmótica (MILLARES).

La inmótica es la incorporación de sistemas que proporcionan algún nivel de automatización dentro del equipamiento de las edificaciones del sector terciario, como son hospitales, edificios de oficinas, grandes superficies, parques tecnológicos, etc(MILLARES), (QUINTERO et Al, 2003).

De forma óptima e integrada proporciona a los distintos controles y automatismos que se incluyen en el edificio, comunicación, control, monitorización, gestión y mantenimiento de los mismos (MILLARES).

Algunos de los beneficios al aplicar inmótica están relacionados con el ahorro energético y mantenimiento, mejoramiento en la gestión de los parámetros del edificio, supervisión de eventos en tiempo real, gestión de históricos y tiempos de funcionamiento, notificación de averías, alarmas técnicas, telegestión remota, supervisión de consumo eléctrico, mayor confort, mejoramiento estético, etc.

Particularmente, en el ámbito de control de accesos, se han desarrollado innumerables proyectos que nos permiten tener una visión general de las tecnologías que se utilizan hoy en día, las diferentes topologías y/o estructuras de la red de control, sensórica, actuadores, procesamiento, interfaz, entre otros aspectos no menos importantes.

A continuación, se mencionan algunos proyectos realizados e implementados en el campo de la inmótica para el control de accesos a instalaciones, llevando un orden cronológico.

¨Diseño inmótico para ahorro energético, seguridad y control de instalaciones para el nuevo edificio de la FIEC¨, Tesis de grado, Ecuador, Escuela Superior Politécnica del Litoral; Este proyecto tiene como propósito asegurar a los usuarios de la edificación un aumento del confort, de la seguridad, del ahorro energético y de las facilidades de comunicación mediante la automatización de la gestión y la información de la misma.

Se explican los principios teóricos empleados en este proyecto. Se detallan conceptos básicos de Edificio Inteligente así como la definición y diferencias entre los conceptos que encierra la Domótica.

Además se realiza un estudio de la situación actual del edificio, tanto en su estructura de red como la tecnología con la que cuenta.

El diseño especifica el esquema de red LonWorks, que es la tecnología escogida para la red inmótica, esquema de red para cada tipo de gestión, descripción de equipos y configuraciones (COBOS et Al, 2005)

¨Aplicación Inmótica De Control De Aulas Docentes de la E.T.S.I.T.¨, Tesis de grado, Málaga, Universidad de Málaga; En este artículo se presenta la implementación de un sistema basado en dispositivos X10 y el protocolo TCP / IP para supervisar las aulas de la Escuela Superior Técnica de Ingeniería de Telecomunicación (E.T.S.I.T) de Málaga. La aplicación permite controlar y programar los dispositivos de las salas de lectura como la iluminación, el aire acondicionado o un proyector de vídeo de un mando a distancia. La aplicación también proporciona un complemento la seguridad de la comprobación del estado de los sensores de presencia una vez las puertas se han cerrado. Se define un modelo arquitectónico de tomar en cuenta los límites eléctricos y arquitectónicos del lugar, que se puede extrapolar fácilmente a cualquier otro edificio. El resultado es un sistema de bajo costo, fácil de usar y de instalar, que proporciona un control sencillo y preciso, además de un ahorro considerable de energía (RUBIO et Al, 2007)

¨Sistemas de control de accesos a edificios mediante tarjetas criptográficas y tarjetas RFID¨, Tesis de grado, Madrid, Universidad Pontificia Comillas; El proyecto Sistema de Control de Accesos a Edificios tiene como objetivo estudiar y desarrollar dos tecnologías de control de acceso, basadas en la utilización de tarjetas inteligentes y tarjetas de radiofrecuencia (RFID). Se ha desarrollado un sistema destinado al Instituto de Investigación Tecnológico (IIT) de la Universidad Pontificia Comillas, capaz de realizar dos tipos de controles de seguridad: por un lado, un control de acceso del personal de dicho departamento y por otro lado, un control de inventario(VELAYOS).

¨Plan piloto del diseño e implementación de un sistema de control de acceso de personal y seguridad para optimizar recursos de la facultad de arquitectura¨, Tesis de grado, Ecuador, Universidad Católica de Santiago de Guayaquil; Este proyecto utiliza las nuevas tecnologías para controlar el acceso y el seguimiento de las clases de la Escuela de Arquitectura, que está basado en microcontroladores y tecnología RFID (ALVARADO et Al, 2007).

¨Implementación del sistema inmótico para el control de accesos en el Aeropuerto de Latacunga basado en la tecnología Lonworks¨, Tesis de grado, Ecuador, Escuela Politécnica del ejército; Con el presente proyecto, se genera un grado de confort para

los operarios de los diferentes edificios del Aeropuerto de Latacunga al ya no tener que ellos poseer todo un juego de llaves para las puertas de las diferentes localidades, sino que ahora con una sola tarjeta de proximidad personal podrán tener el acceso a las oficinas que se les sea permitido(PONCE).

4. METODOLOGÍA

Para desarrollar un proyecto, es indispensable aplicar una metodología que nos permita establecer un orden en las actividades a realizar, reducir los tiempos de diseño e implantación y los costos asociados que estos representan.

En la ilustración 1, se muestra una metodología de diseño para productos mecatrónicos donde se establece una división en tres etapas: proceso de desarrollo, proceso de diseño y diseño conceptual.

Dentro del proceso de desarrollo, se encuentran el escalado de la producción y la optimización del ciclo de vida de gran utilidad para la puesta en marcha y ahorro de recursos del proyecto.

La etapa de diseño se ajusta a nivel de sistema y de forma detallada, ajuste del sistema de control, además tiene en cuenta la optimización y el prototipo final.

En la tercera etapa se identifica la necesidad, se da el establecimiento de las especificaciones, la generación, selección y prueba de conceptos y presentación de prototipos para validación de conceptos.

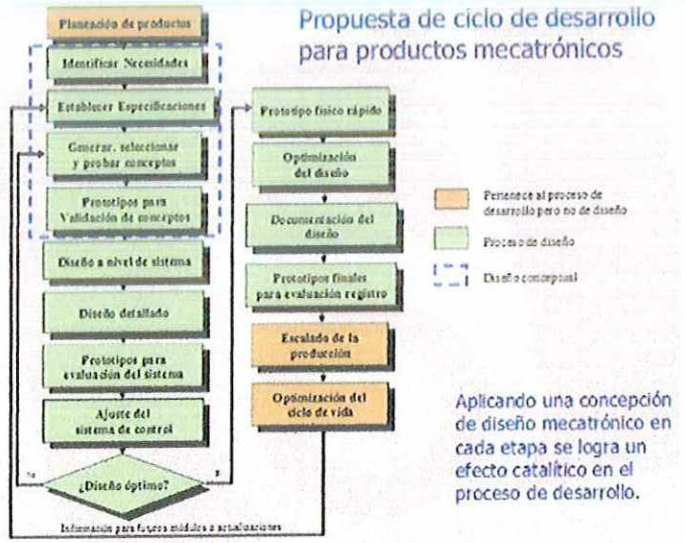


Ilustración 1. Metodología de diseño

Fuente: http://es.scribd.com/doc/3142632/Introduccion-al-Diseno-Mecatronico

Sin embargo, esta metodología de diseño necesita ser complementada para ser específica en los requerimientos de un proyecto de base mecatrónica. Para esto, se tiene en cuenta el esquema mostrado en la ilustración 2, que representa la relación de algunas actividades generales asociadas al desarrollo de una máquina de este tipo.

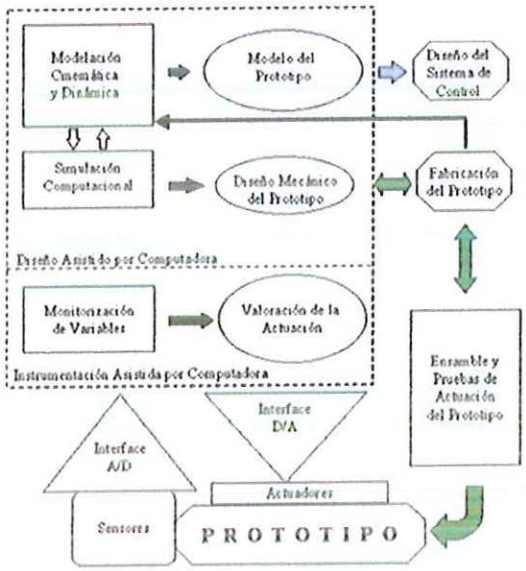


Ilustración 2. Diagrama de actividades generales

Fuente:https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcQuFepnjn3dwteefBV940xEwsolfCmAD5Hvu9yERHfluRhtbOlv

La ilustración 2, nos indica de forma general las actividades asociadas al desarrollo de una máquina diseñada bajo el concepto de la mecatrónica. En esta metodología, el punto de partida es la modelación cinemática y dinámica asociada al mecanismo que se desea analizar. Todas las actividades se encuentran en su conjunto integradas para obtener resultados que permitan una evolución hacia la creación del prototipo. Por lo general, se utilizan diversas herramientas o técnicas computacionales para lograr resultados de diseño, manufactura y control que permitan una reducción de tiempo y costo de prototipo, así como un aseguramiento de su funcionamiento.

El uso de estas herramientas y técnicas dependerán del tipo de problema a resolver, en otros casos, de la infraestructura con la que se cuenta para realizar el proyecto, o bien de la experiencia de los participantes en el proyecto, principalmente. Para cada uno de estos casos es fundamental justificar de forma objetiva la utilización de las técnicas que se aplicarán, así como la forma en que se integrarán en las actividades al proyecto.

5. CAPITULO 1: CONCEPTOS BÁSICOS

5.1 Inmótica

La inmótica es la incorporación al equipamiento de edificios de uso terciario o industrial (oficinas, edificios corporativos, hoteleros, empresariales y similares) de sistemas de gestión técnica automatizada de las instalaciones, con el objetivo de reducir el consumo de energía, aumentar el confort y la seguridad de los mismos (MILLARES).

5.1.1 Características

Las características que debe cumplir un buen sistema inmótico son (MILLARES):

- Integración: Es la propiedad fundamental de un edificio inteligente. Es lo que diferencia un edificio inteligente de un edificio automatizado. En una instalación automatizada, los diversos autómatas actúan de forma aislada. Al integrar el conjunto de sensores, controles, actuadores, el edificio es capaz de detectar lo que ocurre en su interior y en su alrededor y actuar en consecuencia.

- Flexibilidad: El sistema debe ser capaz de adaptarse con facilidad a la incorporación de nuevos subsistemas en su arquitectura. Resulta fundamental que tras una inversión inicial que puede resultar importante, se pueda actualizar de forma rápida y cómoda el sistema con tecnologías futuras.

- Fiabilidad: El número de funciones que controla el sistema será elevado, por lo que es necesario reducir los errores al mínimo para que las consecuencias ocasionadas sean irrelevantes.

- Manejo sencillo: El sistema será controlado por más de un empleado y, generalmente, será personal no calificado. Por ello, es necesario que el funcionamiento que permite controlar el sistema sea de fácil uso y rápida compresión a la hora de aprender a usarlo.

5.1.2 Beneficios

Los beneficios que se obtienen son (MILLARES):

- Reduce el consumo de energía. El edificio inteligente controla de forma óptima el uso de la energía, provocando un ahorro económico considerable. Además, contribuye a proteger el medio ambiente.

- Aumenta el confort. Un edificio inteligente proporciona a los ocupantes del mismo un ambiente más confortable, lo que provoca mejores condiciones de trabajo y favorece la producción de los empleados.

- Aumenta la seguridad. Una de las áreas a la que más importancia da un sistema inmótico es la seguridad. Generalmente, el edificio contará con un equipamiento caro y con información que deberán ser protegidos ante intrusiones y alarmas técnicas (inundaciones, incendios, etc.). El edificio incluirá un sistema que protejan los recursos de forma óptima.

- Gestión remota. Disponiendo de un acceso a Internet, desde cualquier rincón del mundo se puede controlar y variar cualquier parámetro del sistema.

- Buena impresión. La introducción de tecnología en edificios de oficinas provoca buena imagen ante los clientes.

5.1.3 Arquitectura

La Arquitectura de los sistemas de domótica hace referencia a la estructura de su red. La clasificación se realiza en base de donde reside la "inteligencia" del sistema domótico(PONCE).

Las principales arquitecturas son(PONCE):

- Arquitectura centralizada: Un controlador centralizado, envía la información a los actuadores e interfaces según el programa, la configuración y la información que recibe de los sensores, sistemas interconectados y usuarios.

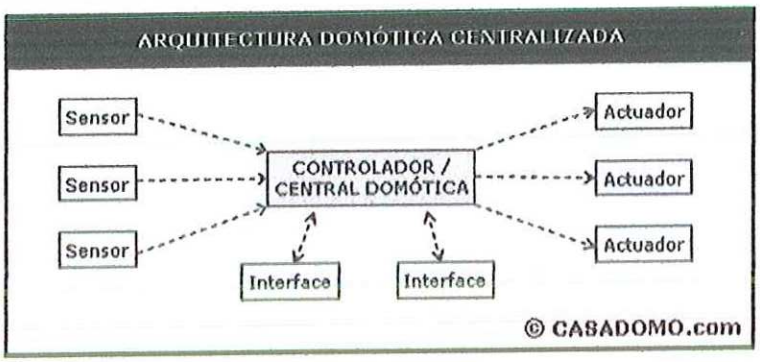


Ilustración 3. Arquitectura Centralizada

Fuente: www.casadomo.com

- Arquitectura descentralizada: Hay varios controladores, interconectados por un bus, que envía información entre ellos y a los actuadores e interfaces conectados a los controladores, según el programa, la configuración y la información que recibe de los sensores, sistemas interconectados y usuarios.

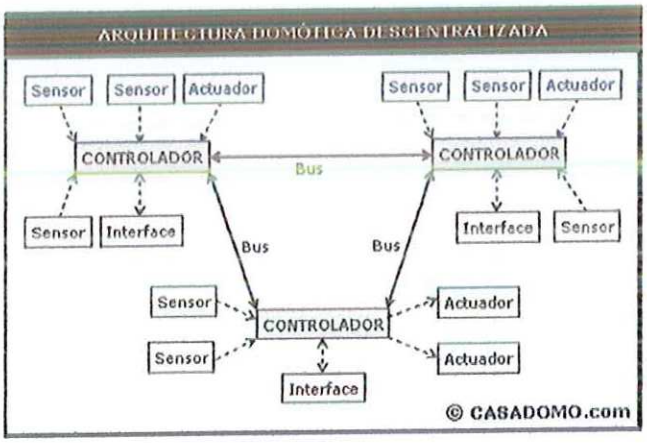


Ilustración 4. Arquitectura Descentralizada

Fuente: www.casadomo.com

- Arquitectura distribuida: Cada sensor y actuador es también un controlador capaz de actuar y enviar información al sistema según el programa, la configuración, la información que capta por si mismo y la que recibe de los otros dispositivos del sistema.

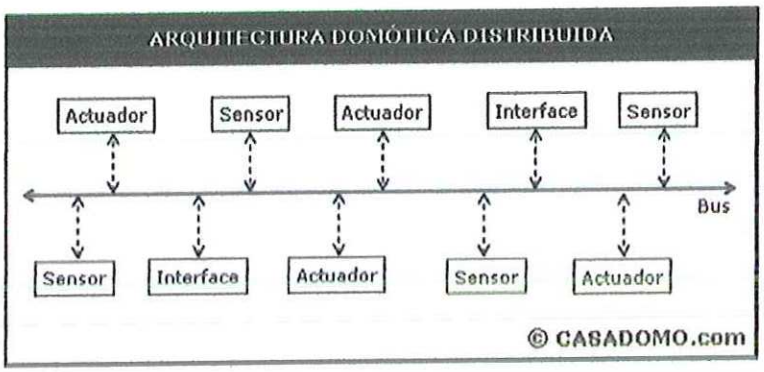


Ilustración 5. Arquitectura Distribuida

Fuente: www.casadomo.com

- Arquitectura híbrida/mixta: Se combinan las arquitecturas de los sistemas centralizadas, descentralizadas y distribuidas. A la vez que puede disponer de un controlador central o varios controladores descentralizados, los dispositivos de interfaces, sensores y actuadores pueden también ser controladores (como en un sistema "distribuido") y procesar la información según el programa, la configuración, la información que capta por si mismo, y tanto actuar como enviarla a otros dispositivos de la red, sin que necesariamente pasa por otro controlador.

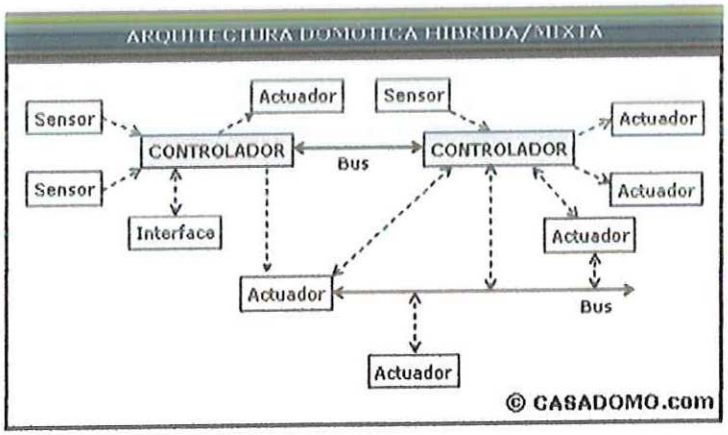


Ilustración 6. Arquitectura Híbrida/Mixta

Fuente: www.casadomo.com

5.1.4 Aplicaciones

Debido a su gran versatilidad y en función del objetivo del sistema inmótico podemos definir más funcionalidades ALVARADO et Al, 2007).

- ❖ Centro de ocio y restauración (ALVARADO et Al, 2007).

La implantación de un sistema de control en un centro comercial tiene cuatro objetivos principales:

- Seguridad del edificio: Mantener la seguridad del edificio ante intrusiones ajenas y alarmas técnicas, inundaciones o escapes de gas.
- Mantenimiento del complejo: El sistema de control supervisa todos los cuadros eléctricos, las horas de funcionamiento de las luminarias, y las alarmas técnicas. De este modo se ahorra y se ayuda al servicio de mantenimiento a tener las instalaciones controladas.
- Ahorro energético: El derroche de energía es algo muy común en este tipo de complejos, con una buena gestión de la iluminación y climatización se puede ahorrar una gran cantidad del gasto energético, amortizando la inversión anual.
- Ayuda a la gestión del edificio: Una de las mayores ventajas es la facilidad y ahorro de personal que reporta un sistema de control. Facturación de gasto energético.
- Control de zonas verdes y regadío de las mismas en función de parámetros atmosféricos.

- ❖ Balneario y gimnasios (ALVARADO et Al, 2007).

Los sistemas de control gestionan los parámetros fundamentales en estas instalaciones que son la:

- Climatización.
- El control de la calidad del aire.
- La temperatura del agua, la composición de la misma.
- Control de accesos, facturación.
- Iluminación.

- Control de audio y video de las distintas salas a través de pantallas táctiles en cada sala o desde el punto de control central, mejorando la confortabilidad de los usuarios finales.

❖ Zonas Educativas (ALVARADO et Al, 2007).

En una zona educativa los parámetros fundamentales para garantizar el bienestar de las personas y el correcto funcionamiento del centro son:

- Climatización.
- Iluminación.
- Salas comunes.
- Estores y persianas.
- Control de accesos y ausencias.
- Seguridad.

❖ Hoteles (ALVARADO et Al, 2007).

En las instalaciones hoteleras, existe la integración de sistemas de control de las zonas comunes del hotel y cada una de las habitaciones.

- En las zonas comunes se puede realizar el control de:

  ✓ Cuadros eléctricos.
  ✓ Control de iluminación.
  ✓ Control de sistemas de ventilación y climatización.
  ✓ Alarmas en el hotel.
  ✓ Integración con ascensores.
  ✓ Medición de consumos.

- En las habitaciones, el control de:

  ✓ Control de acceso.
  ✓ Control de presencia.
  ✓ Control del sistema de televisión.
  ✓ Control del clima.
  ✓ Control de servicios (limpieza).

❖ Parkings (ALVARADO et Al, 2007).

- Sistemas de ayuda al aparcamiento a través de señales luminosas en las zonas de paso de los vehículos y en cada plaza individualmente.

- Sistemas de reconocimiento de matriculas.

❖ Centros para personas mayores (ALVARADO et Al, 2007).

- Localización de personas.
- Detección de comportamientos extraños.
- Control remoto de la iluminación, persianas y climatización.
- Supervisión de habitaciones.
- Seguridad.
- Alarmas individuales por paciente de pánico.
- Control del personal del recinto.
- Control de accesos y de permanencia

❖ Comunidades de vecinos (ALVARADO et Al, 2007).

- Gestión de zonas comunes.
- Reservas de pistas comunes.
- Iluminación inteligente en zonas comunes.
- Seguridad. CCTV.
- Sitio Web comunitario
- Control de accesos a zonas comunes.
- Control eficiente de riego e iluminación en jardines.

5.2 Ventajas y desventajas

Como toda nueva tecnología, la inmótica es una gran alternativa para la comodidad y el beneficio de grandes edificaciones, pero también trae consigo inconvenientes de los que día a día se trata de solventar con nuevas ideas (ALVARADO et Al, 2007).

5.2.1 Ventajas de la Inmótica

Las principales ventajas se basan en racionalización de la energía, la reducción de los costos de mantenimiento, reducción de fallas imprevistas, seguridad de los bienes y por sobre todas las cosas la seguridad de las personas que lo habitan.

Por ellos la gestión técnica de este tipo de instalaciones cobra una máxima relevancia, tanto en la optimización de los recursos del centro, como en el bienestar y la comodidad de los usuarios y sus trabajadores.

Las ventajas de un sistema en edificios y grandes instalaciones son muy numerosas, las más destacables son (ALVARADO et Al, 2007):

- Ahorro energético.
- Ahorro en servicios de mantenimiento.
- Gestión eficaz de los parámetros principales de un edificio.
- Gestión del personal del edificio.
- Supervisión en tiempo real de eventos.
- Gestión de históricos y tiempos de funcionamiento.
- Aviso de averías.
- Avisos de mantenimiento preventivo.
- Alarmas técnicas.
- Telegestión remota.

5.2.2 Desventajas de la Inmótica

Como es de imaginarnos, en la Inmótica y Domótica, no todo son cosas a favor. Si bien no se considera que la implementación en una edificación lleve consigo alguna problemática, hay algunas debilidades en el sistema debido fundamentalmente al nuevo de la tecnología y, por lo tanto, la inexperiencia en la entrega de los servicios (ALVARADO et Al, 2007).

Dentro de estas debilidades están algunos puntos que hay que considerar, siendo algunos de ellos (ALVARADO et Al, 2007):

- El alto precio de los aparatos inmóticos (instalación, equipos), siendo Latinoamérica la zona más cara para adquirirlos, aunque se espera que con el tiempo estos valores disminuyan debido a la competencia entre empresas.

- El uso de la Internet (fundamental en el uso de la Domótica) en las personas hace que disminuyan su vida social.

- La vulnerabilidad de acceso al sistema informativo, pudiendo desactivar el sistema de seguridad de nuestro hogar lo cual podría provocar un gran caos.

5.3 Normativa

5.3.1 Ámbito europeo

- Reglamento Nº 2887/2000. Reglamento sobre acceso desagregado al bucle local.

- Paquete TELECOM (Marzo 2000):

1. Directiva 2002/21: "Directiva marco".
2. Directiva 2002/19: "Directiva acceso e interconexión".
3. Directiva 2002/20: "Directiva de autorizaciones".
4. Directiva 2002/22: "Directiva Servicio Universal".
5. Decisión 676/2002: "Decisión espectro radioeléctrico".

5.3.2 España

- Ley 32/2003.Ley General de Telecomunicaciones.
- Ley 38/1999. Ley Ordenación de la edificación.
- Ley 8/1999. Reforma la Ley 49/1960 sobre propiedad horizontal.
- Real Decreto 8421/2002. Reglamento Electrotécnico para Baja Tensión.

5.3.3 Telecomunicaciones en edificios

- Real Decreto-Ley 1/1998. Sobre infraestructuras comunes para el acceso a servicios de telecomunicaciones en edificios.

- Real Decreto 401/2003. Aprueba el Reglamento regulador de las infraestructuras comunes de telecomunicaciones para el acceso a los servicios de telecomunicación en el interior de los edificios y de la actividad de instalación de equipos y sistemas de telecomunicaciones.

- Orden CTE/1296/2003. Desarrolla el Real Decreto 401/2003.

5.3.4Seguridad y gestión de la energía

- ITC-BT-51: Instrucción Técnica Complementaria para Baja Tensión. Establece los requisitos específicos de la instalación de los sistemas de automatización, gestión técnica de la energía y seguridad para viviendas y edificios.

- Real Decreto 1942/1993. Reglamento de instalaciones de protección contra incendios.

- Real Decreto 1853/1993. Reglamento de instalaciones de gas en locales destinados a usos domésticos, colectivos o comerciales.

- Real Decreto 1751/1998. Reglamento de instalaciones técnicas de edificios.

5.4 Organismos de normalización y normas técnicas

Los organismos dedicados a la normalización de servicios, dispositivos o infraestructuras del sector son: ISO e ITU a nivel internacional, CELENEC y ETSI a nivel europeo y AENOR en el ámbito nacional.

5.4.1 ISO

La principal iniciativa de ISO en el sector domótico es el desarrollo de un estándar a nivel mundial: HES (ISO/IEC 10192). Se trata de un trabajo elaborado por el grupo ISO/IEC JTC1/SC25/WG1 en el que han colaborado expertos de Asia, Europa y Norte América.

Por otra parte, trabaja para la aceptación como normas ISO de distintos protocolos domóticos. Ejemplo de este trabajo es ISO 16484 donde se aprueba BACnet como norma ISO.

5.4.2 ITU

Entre los trabajos relacionados con la domótica, desarrollados por la ITU destaca la elaboración de unos estándares internacionales para redes telefónicas recogidos en las normas G.989.1, G.989.2 y G.989.3, basados en la segunda versión de HomePNA.

5.4.3 CELENEC

EN 50090 (Home & BuildingElectronicSystems) se trata de una norma europea desarrollada por el comité CLC/TC205 "Sistemas electrónicos para viviendas y edificios" de CENELEC (Comité Europeo de Normalización Electrotécnica). Está constituida por diversas partes y se incluye el estándar KNX como parte integrante de las mismas.

La aprobación de las distintas partes no supone obligado cumplimiento mientras que un documento legislativo nacional no haga referencia a la misma. Sin embargo, las empresas fabricantes de productos que deseen adoptar el sistema KNX deberán cumplir: ISO 9000-1, EN 50090-2-2 y Certificación Konnex.

5.4.4 ETSI

El Instituto Europeo de Normas de Telecomunicaciones (ETSI) es un organismo dedicado a la elaboración de las normas de telecomunicación que faciliten la estandarización del sector. En el ETSI participan como miembros no sólo las Administraciones, sino también los operadores de red, la industria, los centros de investigación y los usuarios de los servicios de telecomunicación.

En lo referente a edificios y viviendas inteligentes, el ETSI ha creado, junto con CELENEC y CEN, la iniciativa ICTSB (Information and Communications Technologies Standard Board) que se encarga, entre otras tareas, de los trabajos de normalización en este terreno. Dentro de ICTSB el grupo de trabajo destinado al sector es el SHSSG (Smart House Standards Steering Group).

Por otra parte, los comités técnicos de la ETSI, ETSI/AT y ETSI/HF, están desarrollando trabajos en este campo.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, junto con la Asociación Española de Normalización y Certificación (AENOR), participa en la elaboración y transposición de las normas técnicas e informes procedentes del ETSI, convirtiéndolos en normas nacionales.

5.4.5 AENOR

El Comité Técnico de Normalización 133 "Telecomunicaciones" se encarga de la normalización de las tecnologías, los equipos, los productos, las infraestructuras, las redes, los medios, los servicios y otros aspectos en el ámbito de las telecomunicaciones. Además, realiza un seguimiento de cualquier tema desarrollado por el Instituto Europeo de Normas de Telecomunicación (ETSI).

6. CAPÍTULO 2: ESTÁNDARES MUNDIALES EN DOMÓTICA E INMÓTICA

6.1 Estándar X-10

El protocolo X-10 es un estándar para la transmisión de información por corrientes portadoras. Fue desarrollado entre 1976 y 1978 por los ingenieros de Pico Electronics Ltd, en Glenrothes, Escocia.

El objetivo de esta tecnología fue la de transmitir datos por las líneas de baja tensión (tanto monofásica como trifásica) a muy baja velocidad (60 bps en EEUU y 50 bps en Europa) y costes muy bajos. Al usar las líneas eléctricas de la vivienda, no es necesario tender nuevos cables para conectar dispositivos.

Gracias a su madurez (más de 20 años en el mercado) y a la tecnología empleada, los productos X-10 tienen un precio muy competitivo, lo que les convierte en líderes del mercado norteamericano residencial y de pequeñas empresas (para instalaciones realizadas por los usuarios finales o electricistas sin conocimientos en automatización) (MARTIN et Al, 2008).

6.2 Estándar CEBus

En 1984 varios miembros de la EIA norteamericana (Electronics Industry Association) llegaron a la conclusión de la necesidad de un bus domótico que aportara más funciones que las que aportaban sistemas de aquella época (ON, OFF, DIMMER xx, ALL OFF, etc.). Especificaron y desarrollaron un estándar llamado CEBus (Consumer Electronic Bus).

En 1992 fue presentada la primera especificación. Se trata de un protocolo, para entornos distribuidos de control, que está definido en un conjunto de documentos (en total unas 1000 páginas).

Como es una especificación abierta cualquier empresa puede conseguir estos documentos y fabricar productos que implementen este estándar, tras obtener la autorización de la CIC (CEBus Industry Council).

La CIC es una asociación de diferentes fabricantes de software y hardware que certifican que los nuevos productos CEBus que se lancen al mercado cumplan toda la especificación. Una vez que el producto pase todos los ensayos, el fabricante paga una tasa y es autorizado a poner el logo CEBus en ese producto.

En Europa una iniciativa similar en prestaciones, y en el mercado al que va dirigido, es el protocolo EHS (European Home System) (MARTIN et Al, 2008).

6.3 Estándar Lonworks

Echelon presentó la tecnología LonWorks en el año 1992, desde entonces multitud de empresas vienen usando esta tecnología para implementar redes de control distribuidas y automatización. Aunque está diseñada para cubrir los requisitos de la mayoría de las aplicaciones de control, sólo ha tenido éxito de implantación en edificios de oficinas, hoteles o industrias, debido a su coste.

El éxito que ha tenido LonWorks en instalaciones profesionales, en las que importa mucho más la fiabilidad y robustez que el precio, se debe a que desde su origen ofrece una solución con arquitectura distribuida, extremo a extremo, que permite distribuir la inteligencia entre los sensores y los actuadores instalados en el edificio y que cubre desde el nivel físico de aplicación de la mayoría de los proyectos de control.

En algunos aspectos, una red LonWorks se asemeja a una red de datos de ordenador LAN (Local Area Network). Las redes de datos consisten en ordenadores unidos a varios medios de comunicación, conectados por medio de routers, los cuales se comunican con otros ordenadores usando un protocolo común tal como el TCP/IP. Las redes de datos están optimizadas para el movimiento de grandes cantidades de datos, y el diseño de los protocolos de estas redes de datos prevé retrasos ocasionales a la hora de enviar o recibir la información.

Las redes de control contienen piezas similares optimizadas para los requisitos de coste, realización, tamaño y respuesta de control. El control de red permite a estos sistemas llegar a un tipo de aplicación que la tecnología de redes de datos no puede alcanzar. Los fabricantes de sistemas de control y aparatos pueden acortar el tiempo de desarrollo incluyendo componentes LonWorks. El resultado es un coste más ajustado en el desarrollo y mantenimiento, permitiendo que aparatos de diferentes fabricantes puedan comunicarse.

La sofisticación de una red LonWorks puede variar desde pequeñas redes integradas en máquinas, hasta grandes redes controlando cientos de aparatos. Las redes LonWorks son usadas en edificios, trenes, aviones, fábricas y muchos otros procesos (MARTIN et Al, 2008).

6.4 Estándar EHS

El estándar EHS (European Home System) ha sido otro de los intentos de la industria europea (año 1984), auspiciada por la Comisión Europea, de crear una tecnología que

permitiera la implantación de la domótica en el mercado residencial de forma masiva. El resultado fue la especificación del EHS en el año 1992.

Desde su inicio han estado involucrados los fabricantes europeos más importantes de electrodomésticos de línea marrón y blanca, las empresas eléctricas, las operadoras de telecomunicaciones y los fabricantes de equipamiento eléctrico. La idea fue crear un protocolo abierto que permitiera cubrir las necesidades de interconexión de los productos de todos estos fabricantes y proveedores de servicios.

Tal y como fue pensado, el objetivo de la EHS es cubrir las necesidades de automatización de la mayoría de las viviendas europeas cuyos propietarios que no se pueden permitir el lujo de usar sistemas más potentes pero también más caros (como LonWorks, EIB o BatiBUS) debido a la mano de obra especializada que exige su instalación.

El EHS viene a cubrir, por prestaciones y objetivos, la parcela que tienen el CEBus norteamericano y el HBS japonés y rebasa las prestaciones del X-10 que tanta difusión ha conseguido en EEUU.

La asociación EHSA (EHS Association) es la encargada de emprender y llevar a cabo diversas iniciativas para aumentar el uso de esta tecnología en las viviendas europeas. Además se ocupa de la evolución y mejora tecnológica del EHS y de asegurar la compatibilidad total entre fabricantes de productos con interface EHS (MARTIN et Al, 2008).

6.5 Estándar Batibus

El estándar BatiBUS fue desarrollado por MERLIN GERIN, AIRLEC, EDF Y LANDIS & GYR.

En 1989 se fundó el BCI (BatiBUS club international) con el propósito de extender las aplicaciones basadas en este bus. Hoy en día este club tiene más de 80 socios en muchos países, incluyendo fabricante líderes en aire acondicionado, sistemas de seguridad, equipamiento eléctrico, sistemas de automatización, etc.

BatiBUS ha conseguido la certificación como estándar europeo CENELEC. Existen una serie de procedimientos y especificaciones que sirven para homologar cualquier producto que use esta tecnología como compatible con el resto de productos que cumplen este estándar. A su vez, la propia asociación BCI ha creado un conjunto de herramientas para facilitar el desarrollo de productos que cumplan esta especificación (MARTIN et Al, 2008).

6.6 Estándar EIB

El European Installation Bus o EIB es un sistema domótico desarrollado bajo los auspicios de la Unión Europea con el objetivo de contrarrestar las importaciones de productos similares que se estaban produciendo desde el mercado japonés y el norteamericano donde estas tecnologías se han desarrollado antes que en Europa.

El objetivo era crear un estándar europeo, con el suficiente número de fabricantes, instaladores y usuarios, que permita comunicarse a todos los dispositivos de una instalación eléctrica como: contadores, equipos de climatización, de custodia y seguridad, de gestión energética y los electrodomésticos.

El EIB está basado en la estructura de niveles OSI y tiene una arquitectura descentralizada.

Este estándar europeo define una relación extremo-a-extremo entre dispositivos que permite distribuir la inteligencia entre los sensores y los actuadores instalados en la vivienda.

Aunque en un principio sólo se contempló usar un cable de dos hilos como soporte físico de las comunicaciones, se pretendía que el nivel EIB.MAC (Médium Access Control) pudiera funcionar sobre los siguientes medios físicos:

- EIB.TP: sobre par trenzado a 9600 bps. Además por estos dos hilos se suministra 24 VDC para la alimentación de los dispositivos EIB. Usa la técnica CSMA con arbitraje positivo del bus que evita las colisiones evitando así los reintentos y maximizando el ancho de banda disponible.

- EIB.PL: Corrientes portadoras sobre 230 Vac/50 Hz (powerline) a 1200/2400 bps. Usa la modulación SFSK (Spread Frequency Shift Keying) similar a la FSK pero con las portadoras más separadas. La distancia máxima que se puede lograr sin repetidor es de 600 metros.

- EIB.net: usando el estándar Ethernet a 10 Mbps (IEC 802-2). Sirve de backbone entre segmentos EIB además de permitir la transferencia de telegramas EIB a través del protocolo IP a viviendas o edificios remotos.

- EIB.RF: Radiofrecuencia: Usando varias portadoras, se consiguen distancias de hasta 300 metros en campo abierto. Para mayores distancias o edificios con múltiples estancias se pueden usar repetidores.

- EIB.IR: Infrarrojo: Para el uso con mandos a distancia en salas o salones donde se pretenda controlar los dispositivos EIB instalados.

En la práctica, sólo el par trenzado ha conseguido una implantación masiva mientras que los demás apenas han conseguido una presencia testimonial.

A continuación se muestra una tabla sobre los estándares de control en sistemas de gestión de edificios. Se resumen los protocolos o estándares más utilizados en estos sistemas en particular (MARTIN et Al, 2008).

Tipo	Usabilidad	Características y requerimientos
Estándares americanos		
X-10	Muy fácil implantación	Utiliza la red eléctrica instalada del edificio, pensado para mercado domestico.
CEBus	Mediana implantación	Utilizado en instalaciones de tipo medio
LON	Mucha implantación	Utilizado ampliamente en climatización. Apto para grandes instalaciones.
Estándares Europeos		
EHS	Poca implantación	Pensado para utilidades domesticas.
Batibus	Sencillo	Instalaciones de tipo medio.
EIB	Gran implantación	Complejo y útil en instalaciones de tipo medio-alto

Tabla 1. Estándares de control en Sistemas de gestión de edificios

Fuente: http://isa.uniovi.es/docencia/AutomEdificios/transparencias/Generalidades2.pdf

7. CAPITULO 3: CONTROL DE ACCESO

7.1 Generalidades

El manejo de acceso a recursos está adquiriendo una importancia cada vez mayor para organizaciones en todas partes del mundo, desde pequeñas compañías hasta grandes empresas corporativas y cuerpos gubernamentales de todos los tamaños, hasta la organización más neutral ahora reconoce el peligro de fallas en la seguridad (SCALA).

La administración de acceso a recursos significa controlar tanto el acceso físico como el acceso lógico, ya sea como un esfuerzo independiente o a través de un abordaje integrado. El control de acceso físico protege contra robo o usurpación tanto de bienes tangibles como intelectuales. El control de acceso lógico permite a las empresas y organizaciones limitar el acceso a los datos, a las redes y las estaciones de trabajo solamente para aquellos que están autorizados para tener dicho acceso(SCALA).

El sistema de control de acceso físico es una red coordinada de tarjetas de identificación, lectores electrónicos, bases de datos especializadas, software y computadoras diseñadas para monitorear y controlar el tráfico a través de puntos de acceso(SCALA).

7.2 Componentes del Sistema de Control Acceso

Un sistema de control acceso típico está compuesto de los siguientes componentes(SCALA).

- Una credencial de identificación (tarjeta inteligente).
- Un lector de puerta de acceso (lector de tarjeta inteligente).
- Cerradura de Puerta.
- Panel de Control.
- Servidor de control de acceso.
- Software.
- Base de Datos.

A continuación, en la ilustración 7 se muestra la interconexión entre los componentes de un sistema de control de acceso.

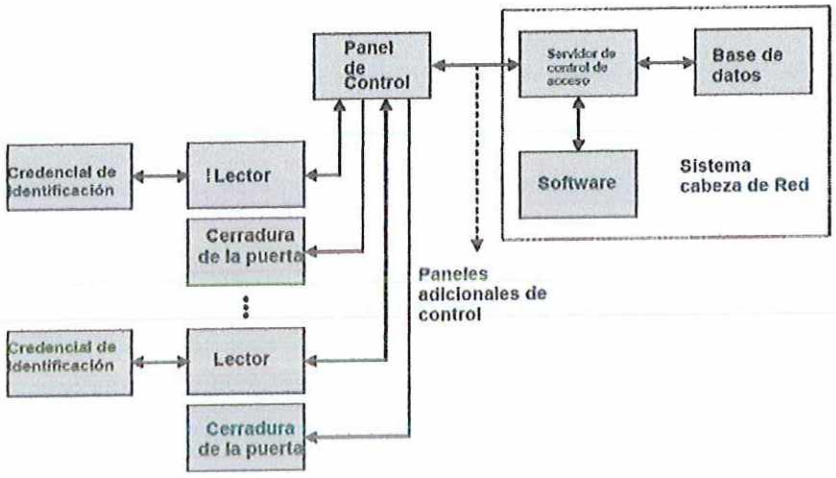


Ilustración 7. Esquema de un sistema de control de acceso

Fuente: http://www.smartcardalliance.org/

A la hora de controlar la entrada y salida de individuos del recinto existen diversas técnicas que proporcionarán distintos grados de control(J. A. ALVARADO).

Uno de los sistemas más empleados se basa en tarjetas magnéticas. En este tipo de instalación, los usuarios del edificio deben pasar o introducir sus tarjetas de identificación en los lectores situados en las puertas donde se quiere controlar el acceso. Otro método similar es el de lectores de proximidad, en ellos, el usuario sólo debe acercar su tarjeta al lector para poder acceder al lugar deseado. Estos sistemas presentan el problema de la pérdida o robo de la tarjeta, que podría permitir el acceso a personas no autorizadas(J. A. ALVARADO).

Si se desea un grado mayor de seguridad, se puede optar por sistemas dotados con teclados numéricos que permitan introducir una clave de usuario. En este caso el usuario deberá teclear la contraseña cuando desee acceder al recinto. Problemas que presenta: la memorización y olvido de una clave por parte del usuario y el craqueo de claves(J. A. ALVARADO).

Si se requiere de un método más sofisticado que proporcione un mayor nivel de seguridad se pueden incluir lectores biométricos de huella digital. En este caso las huellas digitales del personal autorizado están registradas y cuando uno de ellos desea acceder a una zona de la instalación tendrá que poner el dedo encima del lector, que comprobará que el usuario está autorizado a pasar(J. A. ALVARADO).

Dentro del ámbito de la tecnología de identificación, aplicado al control de acceso, se pueden encontrar diversas tecnologías como: sistemas biométricos, tarjetas magnéticas, código de barras, RFID y memorias de contacto(J. A. ALVARADO).

7.3 Tecnologías de autoidentificación

- Acceso con Sistemas Biométricos

Este tipo de identificación se realiza a través del análisis y/o medición de características físicas. Algunas de las técnicas biométricas que existen son(J. A. ALVARADO):

- Reconocimiento de iris.
- Reflexión retinal.
- Geometría de la mano.
- Geometría facial.
- Termografía mano, facial.
- Huellas dactilares.
- Patrón de la voz.

La identificación biométrica ofrece una ventaja significativa, dado que bajo este sistema, se identifica explícitamente a la persona, no así a alguna credencial u otro objeto. La razón por la cual no es aplicable para ciertos problemas una tecnología de este tipo es porque no existen sistemas que ofrezcan una confiabilidad cercana al 100 por ciento. La mayoría de los sistemas de este tipo tienen una eficiencia menor a lo deseable. Otra desventaja de este tipo de sistemas es que son más costosos(J. A. ALVARADO).

- Acceso con Tarjetas magnéticas

Estos sistemas se basan en la lectura de una banda magnética. Utilizan señales electromagnéticas para registrar y codificar información en una banda que puede ser leída por una máquina para identificación instantánea. La aplicación más difundida es la de las tarjetas de crédito.

Sus ventajas son proporcionar agilidad en el acceso, dar identificación única al poseedor, bajo costo, además de que no son fácilmente falsificables. Sin embargo, su uso continuo las deteriora físicamente como consecuencia de la fricción al momento de la lectura. Además si alguna tarjeta es acercada a alguna fuente electromagnética,

relativamente fuerte, puede modificar la información que contiene, perdiendo con ello su utilidad(J. A. ALVARADO).

- Acceso con Tarjetas de Código de Barras

El código de barras se inventó hace más de 25 años y durante este tiempo, ha sido la tecnología más utilizada por los comercios para identificar los productos en venta. Este tipo de identificación se realiza codificando datos en una imagen formada por combinaciones de barras y espacios. Las imágenes son leídas por equipos especiales de lectura óptica a través de los cuales se pueden comunicar datos a la computadora(J. A. ALVARADO).

- Acceso con Tarjetas de RFID (Identificación por Radio Frecuencia)

La tecnología de radiofrecuencia se desarrolló en 1940, como medio para la identificación de los aviones aliados y enemigos durante la Segunda Guerra Mundial. Años más tarde evolucionó, logrando así ser utilizada en la industria ferroviaria para el seguimiento de los coches del ferrocarril y para los años 60´s y 70´s, su uso se enfocó en la seguridad de materiales nucleares.

Es un método electrónico que consiste en asignar un código de información a un producto, proceso o persona y usar esta información para identificar o acceder a información adicional al respecto. Se utiliza principalmente en el rubro de seguridad, como es el caso de los cruces fronterizos, credenciales de identidad, en el control vehicular, identificación de ganado, envío de paquetes, control de equipaje en los aeropuertos y de artículos para renta o préstamo (películas y libros) en videoclubes y bibliotecas, en la industria automotriz, para los procesos de automatización y seguimiento, en el sector agrícola y en el de administración de flora y fauna, para rastrear al ganado y a los animales, así como en el mercado minorista como dispositivo antirrobo(J. A. ALVARADO).

- Acceso con Memorias de Contacto

Tipo específico de tecnología de autoidentificación que requiere un contacto físico con el botón para leer los datos de la etiqueta. La adopción ha sido muy limitada, comparada con la pequeña inversión a realizar y las innovaciones que ha habido en esta área.

La memoria de contacto no ha tenido una amplia adopción como solución de autoidentificación. Una de las principales preocupaciones al respecto es que los tres mayores sistemas conocidos de esta tecnología en la actualidad son propietarios. Y si cualquiera de estos es descontinuado, será complicado encontrar un sustituto.

Pero entre sus ventajas están la de ser dispositivos de múltiples lecturas y escrituras, además de ser muy resistentes, ya que pueden ser empleados en entornos hostiles y con vibraciones propias de aplicaciones de manufactura(J. A. ALVARADO).

A continuación en la Tabla 2, se muestra una comparación entre las tecnologías de control de acceso que fueron descritas anteriormente.

Los parámetros evaluados para dicha comparación son los siguientes: modificación de la información, seguridad de los datos, capacidad de almacenamiento de los datos, precio, estándares, ciclo de vida, distancia de lectura e interferencia potencial.

	Código de Barras	Banda Magnética	Memoria de Contacto	Sistemas Biométricos	RFID Pasivo	RFID activo
Modificación de la información	No Modificable	Modificable	Modificable	No Modificable	Modificable	Modificable
Seguridad de los Datos	Mínima	Media	Alta	Alta	Variable (baja a alta)	Alta
Capacidad de Almacenamiento de datos	-Lineales(8-30 caracteres) - 2D hasta 7.200 caracteres	Hasta 128 bytes	Hasta 8MB	No aplica	Hasta 64 KB	Hasta 8MB
Precio	Bajo	Medio-Bajo	Alto (cerca de US$1 por memoria)	Alto	Medio (menos de US$0.50 por tag)	Muy Alto (US$10 a US$100 por tag)
Estándares	Estables	Estables	Propietarios, no estándar	No estándar	Evolucionando hacia estándar	Propietario y en evolución hacia estándar
Ciclo de Vida	Corto	Mediano	Largo	Indefinido	Indefinido	Depende de la batería (3 a 5 años)
Distancia de Lectura	Línea de vista y (hasta 1.5m)	Requiere contacto	Requiere contacto	Depende del biométrico	No requiere línea de vista ni contacto Hasta 10m.	No requiere línea de vista ni contacto Hasta 100 m. y mayores
Interferencia Potencial	Cualquier modificación en las barras y objetos entre el código y el lector	Bloqueo del contacto	Bloqueo del contacto	Puede ser bloqueo del contacto, o bloqueo de línea de vista e inclusive el ruido.	Ambientes o campos que afecten la transmisión de radio frecuencia	La interferencia es muy limitada, debido a la potencia de transmisión.

Tabla 2. Tecnologías de Control de Acceso

Fuente: Jorge Alvarado

7.4 Dispositivos utilizados para el control de acceso

7.4.1 Dispositivos para la seguridad

Los detectores de intrusión se clasifican en dos grandes grupos: volumétricos para la detección de presencia o movimiento y perimetrales para la detección de rotura o forcejeo de puertas de acceso o ventanas(MILLARES).

La vigilancia volumétrica permite señalizar la presencia de individuos en el interior del recinto o en una determinada estancia del mismo, activando la alarma cuando detecta el movimiento de las personas. Los detectores volumétricos deben colocarse en una esquina de la estancia, asegurando una orientación que logré la máxima cobertura. A la hora de seleccionar un detector se debe tener en cuenta los siguientes aspectos(MILLARES):

- Ángulo de detección: Existen detectores que van desde los 110º a los 360º.
- Distancia máxima de detección: Desde los 5 a los 50 metros.

Los sensores de presencia se agrupan en tres grandes grupos(MILLARES):

a) Infrarrojos: Son los más usados y existen dos variantes: activos y pasivos, aunque en el mercado se pueden encontrar también detectores infrarrojos combinados con tecnología microondas o con ultrasonido. El de tipo activo, se basa en la creación, mediante infrarrojos, de una barrera invisible que al ser rota activa la alarma. Está formado por un emisor de infrarrojos, un receptor (fototransistor), un convertidor de señal y un amplificador. Los pulsos de luz recibidos son convertidos a señales eléctricas, que se analizan para determinar si se corresponden con una transmisión de luz.

   En los de tipo pasivo, se programa el aparato para que detecte variaciones de temperatura con respecto a una de referencia, normalmente la temperatura ambiente; como la temperatura corporal suele ser mayor, la presencia de personas activa el dispositivo (pasiva). Entre sus limitaciones destacan la mala sensibilidad del dispositivo cuando el objeto se acerca directamente al sensor y su reducción en el rango de alcance cuando se dan temperaturas altas.

   Existen distintas formas de detección, y las características del objeto a ser detectado determinarán el método de detección que se adapta mejor.

b) Ultrasonidos: Emiten ondas de ultrasonido y se basan en el efecto Doppler, que provoca que varíe la frecuencia de la onda al rebotar en el objeto en movimiento. El receptor detecta los sonidos procedentes de las reflexiones en el área vigilada, que estarán en fase si no hay ningún objeto en movimiento. Su alcance

es de muy pocos metros (0.25 a 13 metros). Son susceptibles al ruido acústico y al viento pero su acción es muy rápida.

c) Microondas. Estos sensores emiten ondas electromagnéticas. Trabajan en la banda de los 10 GHz y poseen gran sensibilidad al ser capaces de detectar movimientos muy pequeños en distancias de 50 metros.

Las actuales cámaras IP o de red suelen incorporar detectores de presencia y por tanto, si se tiene una instalación con este tipo de cámaras no sería necesario incorporar este tipo de dispositivos, en las zonas donde estén situadas las mismas(MILLARES).

Para la detección de roturas de cristales o forcejeo de puertas y ventanas por parte de intrusos, se emplean dos tipos de sensores(MILLARES):

a) Sensores de contacto. También denominados electromecánicos, son los primeros detectores que se utilizaron y se caracterizan por ser simples, robustos y económicos. Su funcionamiento se basa en la apertura o el cierre de un circuito cuando se actúa sobre el sensor al abrir una puerta o una ventana. Estos sensores suelen constar de dos partes, una fija que se colocará en el marco de la puerta o la ventana y la otra, móvil, que se instalará en el lado contrario a las bisagras en la puerta o la ventana para lograr detección con mínima apertura.

b) Sensores de vibración. Se trata de sensores piezoeléctricos, capaces de detectar las vibraciones del objeto al que están adheridos y transformarlas en variaciones de tensión eléctrica.

7.4.2 Cámaras de vigilancia

Un elemento tradicional y eficiente para la protección de cualquier edificio es la cámara de seguridad. En este campo se pueden distinguir dos tipos(MILLARES):

a) Cámaras en circuito cerrado de televisión (CCTV): Es el sistema típico de vigilancia, requiere de personal para su observación y permite grabar lo que sucede en la zona para la identificación de posibles intrusos. Estas cámaras se situarán estratégicamente tanto en el exterior como en las zonas interiores y se podrá controlar remotamente para modificar el ángulo de visión. Las imágenes de vídeo procedentes de las distintas cámaras se mostraran en uno o varios monitores de televisión al personal encargado y podrán ser grabadas para un posible análisis posterior.

b) Cámaras IP: Se conocen también como cámaras Web o de red y están diseñadas para enviar las señales de vídeo a través de Internet o a través de un concentrador en una red de área local. Este tipo de cámaras permite la

visualización de imágenes tanto desde cualquier navegador de Internet en PC como desde una PDA o un teléfono con el software adecuado. Además, podría ser capaz de enviara un e-mail o un mensaje corto si detecta presencia. Una cámara IP está constituida de los elementos típicos de una cámara de vídeo tradicional, un sistema de compresión de imagen y un sistema de procesamiento que se encargará de la gestión de las imágenes, del envío al módem, de la detección de movimiento, etc.

Las ventajas que aporta una cámara IP frente al sistema tradicional CCTV son(MILLARES):

- Posibilidad de acceder desde cualquier sitio del mundo. Para visualizar las imágenes de un CCTV es necesario estar en el lugar donde se encuentra el sistema.

- Más económico. Instalar un sistema de cámaras IP resulta sencillo ya que es como montar una red local, mientras que las instalaciones de un CCTV resultan caras y complicadas.

- Escalabilidad. Resulta más sencillo añadir nuevas cámaras IP al sistema que en CCTV.

Por otro lado, es posible conectar a la cámara IP sensores convencionales o relés que permitan la actuación de dispositivos de forma remota. Generalmente, estas cámaras llevan un mecanismo de detección de movimiento incorporado y no sería necesario dotar al sistema de detectores de movimientos externos(MILLARES).

El principal problema de las cámaras IP es el relacionado con el tema de la seguridad. Al existir conexión a Internet existe la posibilidad de que individuos no autorizados puedan acceder a la configuración de las cámaras de manera más fácil que cuando se tiene un sistema de televisión cerrado. Como medida de seguridad, las cámaras IP disponen de un software interno que permite establecer varios niveles de acceso (administrador y usuario), a los que se tiene entrada mediante un nombre y una contraseña(MILLARES).

Para visualizar las cámaras IP desde un PC lo único que será necesario es tener instalado un navegador web, mediante el cual se tendrá acceso a la dirección propia de la cámara y se mostrará al usuario imágenes de lo que está sucediendo en tiempo real. Además, existe en el mercado software específico que permitirá una visualización simultánea de varias cámaras, control y administración de las mismas y la reproducción de vídeos grabados mediante una grabación programada o como consecuencia de alarmas(MILLARES).

Si se dispone ya de un sistema CCTV se pueden disponer de imágenes del mismo a través de Internet gracias al denominado servidor de vídeo IP. Este servidor se compone de conversores analógico-digital, de sistema de compresión y de un sistema de procesamiento que se conecta por un lado al sistema CCTV y por otro al router que da la conexión a Internet (MILLARES).

8. CAPITULO 4: DOCUMENTACIÓN CÓDIGOS QR

QR Code o Quick Response Code (Código de Respuesta Rápida), es un estándar de "código de barras bidimensional". Fue creado en Japón en el año 1994 por la empresa *Denso Wave. Esta empresa japonesa distribuye las especificaciones del mismo* de manera libre y aunque posee una patente sobre el QR Code, no ejerce los derechos sobre la misma. Existen dos estándares de los QR Code, el japonés JIS X 0510, creado por la JIS y distribuido en enero de 1999; y el correspondiente estándar de la ISO, ISO/IEC 18004 aprobado en junio de 2000 y revisado en 2006 (ISO/IEC 18004:2006) (FERNÁNDEZ. G.).

El éxito probado del QR Code se debe precisamente a su estándar abierto y a que su decodificación puede realizarse con cualquier teléfono móvil con cámara sin ser importante la calidad de ésta. En Japón está muy extendido su uso y es raro que los móviles no vengan con software incorporado para decodificarlos (FERNÁNDEZ. G.).

Ventajas del QR Code

El QR Code es capaz de contener información en ambas direcciones (verticalmente y horizontalmente) a diferencia de los tradicionales códigos de barra (de una dimensión), que tan sólo son capaces de almacenar información en una dirección. Precisamente por este motivo, la capacidad de almacenamiento es mayor en el caso del QR Code (así es posible almacenar 7089 caracteres numéricos o 2953 bytes). La unidad de información de un código unidimensional es la barra, en uno bidimensional es el módulo o cuadrado (FERNÁNDEZ. G.).

Además aporta otras características muy interesantes (FERNÁNDEZ. G.):

- Los QR Code tiene la capacidad de corregir errores. Se pueden restaurar los datos si parte del código está dañado o manchado. Existen varios niveles de corrección de errores, pudiendo llegar a restaurar hasta el 30% de la información pérdida debido a la suciedad, deterioro del código, etc. El sistema de corrección de errores se basa en Reed Solomon.

- Los QR Code pueden ser leído a alta velocidad (Quick Response) desde todas las orientaciones (en 360º). Esto es debido a que posee unos patrones (patrones localizadores) que permiten detectar la posición del código. Así, aunque es necesario mantener una línea de visión directa entre el código y el lector la posición de la etiqueta no es crítica, a diferencia de los códigos de barras. Si la imagen no esta recta se detecta su orientación y se rota.

El uso del QR Code se ha popularizado (sobre todo en países como Japón) gracias a la combinación de tres factores (FERNÁNDEZ. G.):

- La publicación de las especificaciones del código. Esto ha permitido la proliferación de lectores de QR Code de muy bajo coste o incluso gratuitos. Además, se han desarrollado aplicaciones de software que permiten descifrar el QR Code. Muchas de ellas son gratuitas.

- La integración con dispositivos móviles (teléfonos y PDAs). Esto ha permitido que la mayoría de los teléfonos puedan leer los QR Code, puesto que sólo necesitan tener una cámara de fotos para la captura de los códigos y una aplicación (que en muchos casos es gratuita) para descifrar la información contenida en los mismos. Muchos de los principales fabricantes de telefonía móvil incorporar de serie en algunos de sus dispositivos aplicaciones para leer QR Code.

- Además QR Code soporta los caracteres del alfabeto japonés Kanji y viene preparado para poder soportar cualquier otro lenguaje.

8.1 Características principales

Los símbolos QR Code tienen 40 versiones y 4 grados de corrección de error (L, M, Q, H). Un símbolo 40-H sería un símbolo de versión 40 y corrección de errores H. Cada versión tiene un tamaño, siendo la 1 de 21x21 módulos y la 40 de 177x177 módulos, creciendo en 4 módulos el tamaño de cada versión (FERNÁNDEZ. G.).

Hay 4 modos de codificar los caracteres de datos (FERNÁNDEZ. G.):

1) Datos numéricos (0-9).
2) Datos alfanuméricos (0-9, A-Z y otros 9 caracteres: espacio, $, %, *, +, -, ., /, :).
3) Bytes (por defecto ISO/IEC 8859-1).
4) Caracteres Kanji, compactados en 13 bits (caracteres de la escritura japonesa).

Para un símbolo 40-L el número máximo de datos que puede contener es (FERNÁNDEZ. G.):

- Datos numéricos: 7089 caracteres.
- Datos alfanuméricos: 4296 caracteres.
- Bytes: 2953 caracteres.
- Caracteres Kanji: 1817 caracteres.

El sistema corrección de errores se basa en Reed Solomon y tiene 4 niveles (FERNÁNDEZ. G.):

1) L (low) bajo, puede corregir hasta el 7% de los codewords del símbolo.
2) M (médium) medio, puede corregir hasta el 15% de los codewords del símbolo.
3) Q (quality) calidad, puede corregir hasta el 25% de los codewords del símbolo.
4) H (high) alto, puede corregir hasta el 30% de los codewords del símbolo.

Los módulos del símbolo QR Code pueden ser blancos o negros y representan respectivamente el 0 y el 1 binario. Sin embargo existe un modo de reflectancia inversa donde es al revés. QR Code puede soportar el que la imagen con el símbolo esté rotada o transpuesta lateralmente (mirror image), tiene independencia de orientación (FERNÁNDEZ. G.).

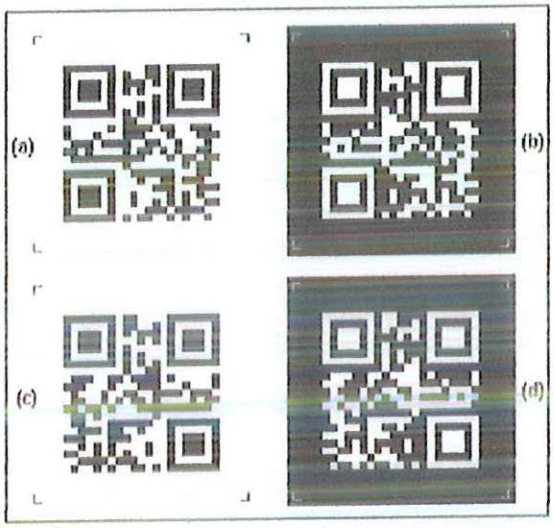


Ilustración 8. Ejemplos de QR Codes: a) orientación y reflectancia normal. b) orientación normal y reflectancia invertida. c) orientación transpuesta y reflectancia normal d) orientación transpuesta y reflectancia invertida.

Fuente: Fuente: Ginés Miguel Fernández Ordóñez

8.2 Estructura del símbolo

Los QR Code 2005 están formados por módulos colocados en una estructura cuadrada. Ésta estructura contiene la región de codificación y los patrones de función, que son: localizador, separador, temporizador y de alineamiento. El símbolo debe estar rodeado en sus cuatro lados por una zona de silencio (FERNÁNDEZ. G.).

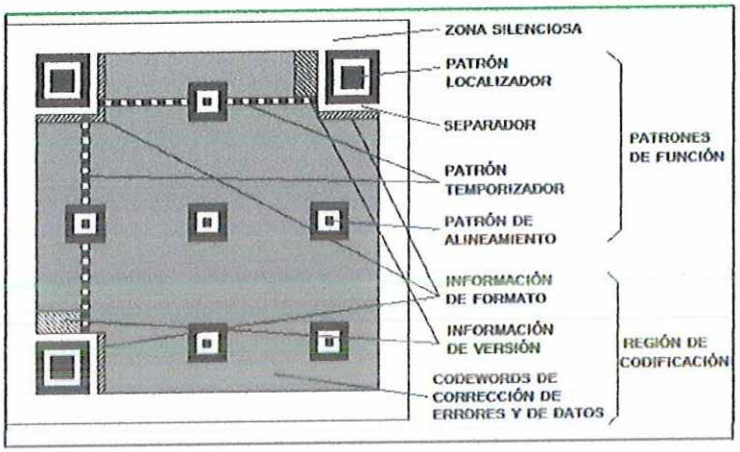


Ilustración 9. Estructura de un símbolo QR Code versión 7

Fuente: http://qrcode.es/wp-content/uploads/2007/12/structure-of-qrcode.gif

Hay 40 versiones cada una con un número de módulos, la versión 1 tiene 21x21módulos y la 40 177x177; el número de módulos se incrementa de 4 en 4 de una versión a otra. Las versiones también se diferencian en el número de codewords que contienen y el de patrones de alineamiento, algunas tienen bits de relleno pero otras no. Las versiones anteriores a la 7 no tienen información de versión, la versión 1 no tiene ningún patrón de alineamiento. Todas tienen tres patrones localizadores, dos patrones temporizadores, tres separadores y la información de formato por duplicado (FERNÁNDEZ. G.).

El patrón localizador se sitúa en las esquinas superior izquierda, superior derecha e inferior izquierda del símbolo QR Code. Está formado por un cuadrado relleno de 3x3módulos negros, rodeado de un cuadrado de 5x5 módulos blancos que a su vez está rodeado por otro cuadrado de 7x7 módulos negros. Será muy difícil encontrar un patrón de módulos similar a este en otras partes del símbolo (FERNÁNDEZ. G.).

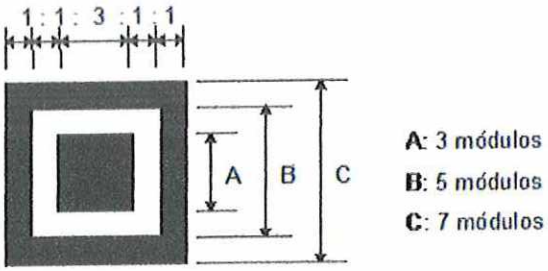


Ilustración 10. Patrón Localizador

Fuente: Ginés Miguel Fernández Ordóñez

Los separadores están formados por módulos blancos y rodean los bordes de los patrones localizadores que dan a la parte interior del símbolo (FERNÁNDEZ. G.).

Los patrones temporizador son dos, uno vertical y otro horizontal. Están formados por una línea o columna de módulos blancos y negros alternados, comenzando y terminando en un módulo negro. Posibilitan que la versión del símbolo y las coordenadas de los módulos puedan ser determinadas. El temporizador horizontal cruza la fila número 6 entre los separadores superiores y el vertical igual pero cruzando la columna 6 (FERNÁNDEZ. G.).

Los patrones de alineamiento están formados por un módulo negro, rodeado de un cuadrado de 3x3 módulos blancos que a su vez está rodeado por otro cuadrado de5x5 módulos negros. Su número en el símbolo varía según la versión (FERNÁNDEZ. G.).

La región de codificación contiene los codewords que representan los datos, también contiene codewords de corrección de errores, la información de formato y la información de versión en la mayoría de casos (FERNÁNDEZ. G.).

La zona de silencio debe tener un grosor de 4 módulos rodeando los cuatro bordes del símbolo (FERNÁNDEZ. G.).

9. CAPITULO 5: TARJETAS CONTROLADORAS

9.1 Sistemas Embebidos

9.2 BEAGLEBOARD XM

Es un sistema que permite tener un procesador de alto poder con todos los periféricos necesarios para hacer aplicaciones tan avanzadas como correr un sistema operativo. Integra un procesador ARM Cortex-A8 y memoria con 512 MB RAM DDR de bajo consumo de energía, permitiendo a los aficionados, los innovadores y los ingenieros para ir más allá de su imaginación usando todas las capacidades que tiene esta board.

El diseño de esta board incluye salidas a video, entradas y salidas de audio, conexiones USB, entre otras, además el diseño de hardware abierto mejora el rendimiento permitiendo que se tenga prácticamente un ordenador portátil con capacidad de expansión y bajo consumo de energía.

Al igual que con las versiones anteriores de BeagleBoard, la BeagleBoard-XM no esta diseñada para ser un entorno de desarrollo, sino más bien una plataforma apoyada por la comunidad que puede ser utilizada como base para la construcción de sistemas de desarrollo más completo y aplicaciones especificas donde el factor de procesamiento unidas con sistemas operativos sencillos sean claves.

9.2.1 Características

- Super-escalar ARM Cortex-A8.
- 512 MB RAM LPDDR.
- USB 2.0 de alta velocidad.
- Puertos de alta velocidad USB 2.0 con 10/100 Ethernet.
- DVI-D (monitores de ordenador digital y televisores de alta definición).
- S-video (salida de TV).
- Salida de audio estéreo.
- Alta capacidad ranura microSD de 4 GB y tarjeta microSD.
- JTAG

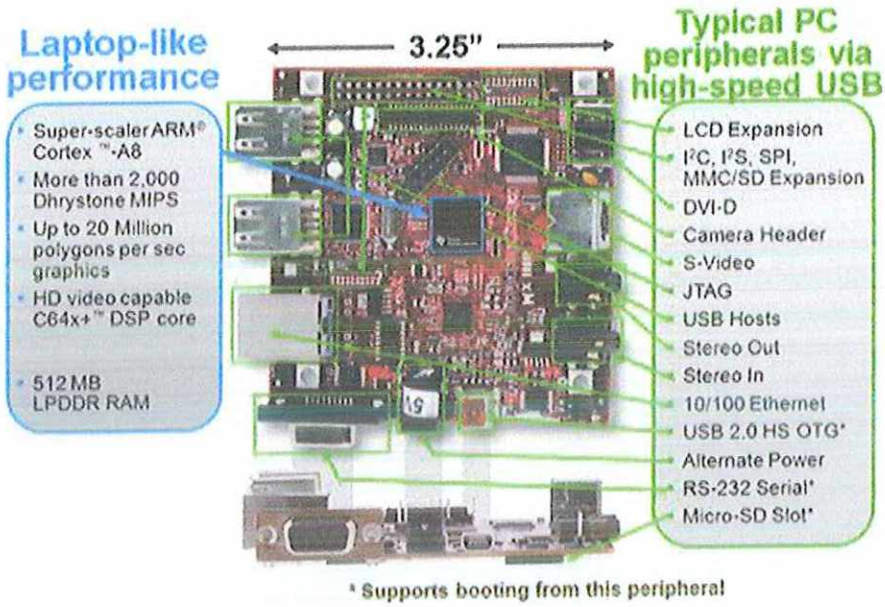


Ilustración 11. Tarjeta Beagleboard XM

Fuente: http://farm5.static.flickr.com/4068/4644432552_2fb4280336.jpg

9.3 ALIXD2D

9.3.1 Características

- CPU: 500 MHz AMD Geode LX800
- DRAM: 256 MB DDR DRAM
- Almacenamiento: CompactFlash socket, 44 pin IDE cabecera.
- Alimentación: Min. 7 V, max 20V
- 3 Leds en el panel frontal.
- Expansión: 2 MiniPCI slots, LPC Bus.
- Conectividad: 2 Canales Ethernet (Vía VT6105M 10/100).
- E/S: Puerto Serial DB9, Puerto Dual USB.
- Tamaño de la board: 6X6" (152.4 x 152.4 mm)
- Firmware: tinyBIOS
- Opciones del cliente: Bus I2C, buzzer, batería RTC.

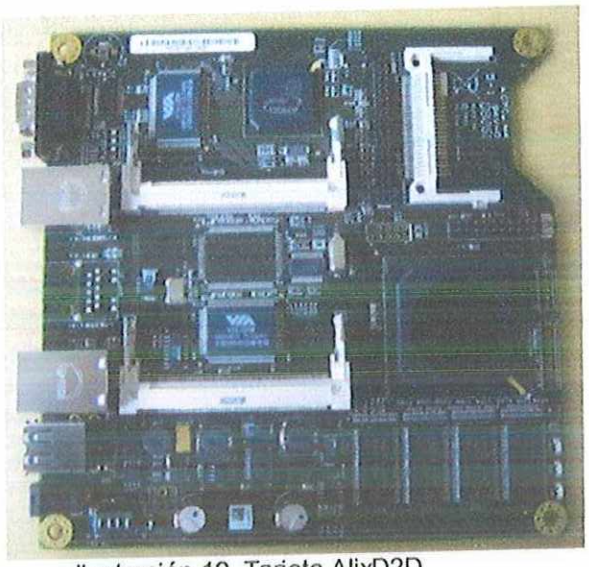


Ilustración 12. Tarjeta AlixD2D

Fuente: http://www.pcengines.ch/pic/alix2d2.jpg

9.4 ODROID U2

9.4.1 Características

- Procesador: Samsung Exynos4412 Prime Cortex-A9 Quad Core 1.7GHz with 1MB L2 cache.
- Memoria RAM: 2048MB (2GB) DDR2 880MHz.
- Tarjeta Gráfica: aceleradora 3D Mali-400 QuadCore 440MHz con drivers libres para Linux.
- Vídeo: 1080p HDMI codec H.264+AAC.
- Salida de Vídeo: conector micro HDMI.
- Salida de Audio:

  -Tipo jack de 3.5mm para auriculares estándar.

  -HDMI Digital.

- Entrada Audio: Micrófono digital incluido en placa base.
- Tarjeta de red: Ethernet 10/100Mbps conexión RJ-45 Jack USB:
  - 2 entradas USB 2.0 de tamaño estándar para conectar periféricos y almacenamiento. Tipo USB Host.
  - 1 entrada USB 2.0 de tamaño micro USB para conectar la ODROID-U2 como si fuera un periférico externo en modo ADB o Massstorage. Tipo USB Device.
- Almacenamiento: ranura tipo micro SD.

- Alimentación: conexión tipo jack de 5V y 2A.
- Sistemas Operativos oficialmente soportados: Android 4.x, Linaro Ubuntu 12.10.
- Caja: incluida de serie caja de aluminio con funciones de disipador.
- Tamaño de la placa base: 48 x 52 mm.
- Precio: 89$ + 30$ por gastos de envío + 25% aprox. aduanas = 148.75$.

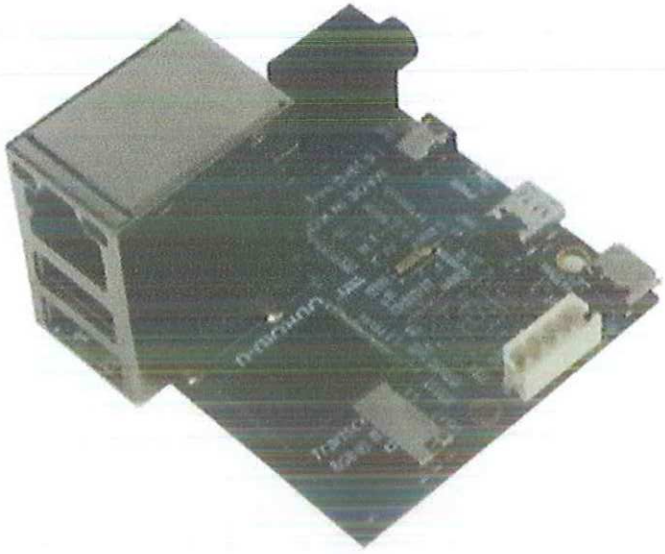


Ilustración 13. Tarjeta Odroid U2

Fuente: http://raspberryparatorpes.net/wp-content/uploads/2013/03/289x237x030713_1600_Rivalesdela1.jpg.pagespeed.ic.dfNUvPGtyX.jpg

9.5 PANDABOARD

Son Single Board Computers y consisten en una placa madre de tamaño reducido basada en la plataforma ARM, ampliamente utilizada en sistemas embebidos y últimamente en Smartphones y tablets.

9.5.1 Especificaciones técnicas

- Memoria
  - 1GB low power DDR RAM.
  - Full size SD/MMC card cage with Support for High-Speed & High-Capacity SD cards.

- Display

- HDMI v1.3 Connector (Type A) to drive
- HD displays.
- DVI-D Connector (can drive a 2nddisplay in simultaneous) .
- LCD expansion header.

- Conectividad
  - Onboard 10/100 Ethernet.
- Debug
  - JTAG.
  - UART/RS-232.
  - 2 status LEDs (configurable).
  - 1x GPIO button.

- Distribuciones admitidas
  - Android.
  - Ubuntu.
  - Angström minimal filesystem

- Procesador
  - OMAP4430 applications processor.

- Expansion
  - 1x USB 2.0 High-Speed On-The-Go port.
  - 2x USB 2.0 High-Speed host ports.
  - General purpose expansion header (I2C, GPMC, USB, MMC, DSS, ETM).
  - Camera expansion header.
- Audio
  - 3.5" Audio in/out.
  - HDMI Audio out.

- Conectividad Inalámbrica
  - 802.11n (based on Wi Link™ 6.0)
  - Bluetooth® (based on Wi Link™ 6.0)

- Dimensiones
  - Altura: 4.5" (114.3 mm).
  - Ancho: 4.0" (101.6 mm).
  - Peso: 2.6 oz (74 gr).

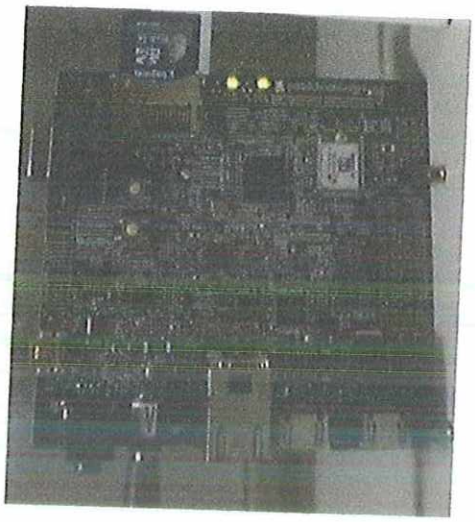


Ilustración 14. Tarjeta Pandaboard

Fuente: http://upload.wikimedia.org/wikipedia/commons/7/7e/Beadaframe.jpg

9.6 LNL 2220

Los controladores Lenel de la serie NGP-2200 se han diseñado para aplicaciones integradas de intrusión y control de acceso. Estos controladores son el motor del ambiente híbrido de Lenel y proporcionan el poder y la capacidad necesaria para ambientes extensivos de intrusión y control de acceso. Diseñados originalmente para funcionar como controladores basados en Ethernet redundante, estos controladores pueden soportar también la transmisión de eventos a receptores de estación central para reporte de intrusión. Al utilizar las comunicaciones redundantes Ethernet y un avanzado procesador basado en linux, la serie NGP-2200 de controladores Lenel puede comunicarse upstream a la computadora anfitrión con rendimiento protegido con respaldo hasta 8 veces mayor que las conexiones en serie más rápidas. La serie NGP-2200 puede soportar hasta 250,000 tarjeta habientes, 512 puntos de entrada tipo intrusión o estándar, 256 salidas y 66 puertas (Lectoras de entrada/salida por puerta). Cuatro puertos de comunicación SNAPP pueden usarse para conectar combinaciones múltiples de teclados LCD, módulos de control de entrada, módulos de control de salida, módulos de interfaz de lectora de tarjeta y fuentes de alimentación (hasta 96 dispositivos) dando a este set de controlador la capacidad para administrar instalaciones a nivel Enterprise.

Basados en una plataforma de hardware común (compartida con la Serie de Seguridad NGP-2200), los controladores pueden actualizarse por medio de una licencia para proporcionar niveles múltiples de sets de características. La serie NGP-2200 puede comprarse con una interfaz redundante en bordo o en una configuración de control de acceso solamente. Los controladores se proporcionan con un gabinete y el transformador de alimentación adecuado para la región.

9.6.1 Características

- Soporta hasta 250,000 tarjetas habientes (credenciales).
- Soporte para 1000 perfiles de permisos (autoridades).
- Soporte para 130 áreas (intrusión y anti-passback).
- 512 puntos de entrada/256 puntos de salida.
- Buffer de 50,000 eventos (memoria no volátil respaldada por batería).
- Soporte para 66 puertas (lectoras entrada/salida para cada puerta).
- Soporte para hasta 32,000 niveles de acceso (hasta 128 por credencial).
- 255 feriados con agrupamientos, 255 zonas horarias (cada una con seis intervalos).
- Soporte para formato de tarjeta (magnética, Wigand, inteligente) hasta 245 bits.
- Supervisión (fin de línea) de 4 líneas personalizadas (circuito).
- Comunicaciones al anfitrión red (10/100) puerto dual en bordo.
- Comunicaciones al anfitrión en serie y por modem basadas en USB.
- Estación central y monitoreo con capacidad de reporte redundante.
- Encriptación de AES 128 bit - anfitrión a controlador.
- Diagnósticos locales y remotos.
- Soporte de alimentación en bordo.
- Firmware flash actualizable.
- Flash en bordo y RAM con respaldo de batería.
- Gestión de alimentación avanzada.

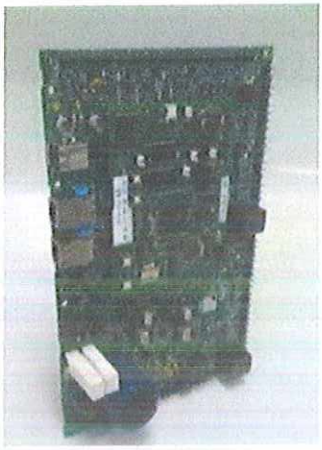


Ilustración 15. Tarjeta LNL 2220

Fuente: http://cdn.lenel.com/collateral/HW_NGP-2220_ESP.pdf

9.7 Comparación entre las diferentes tarjetas controladoras

Para facilitar la selección de la tarjeta de desarrollo que realizará la integración del sistema, se plantea un cuadro comparativo entre las opciones estudiadas, evaluando principalmente siete criterios; consumo de energía, procesador, velocidad de puertos, expansión, conectividad, memoria RAM y costo. A continuación, se muestra en la tabla 3 la comparación entre los diferentes sistemas embebidos.

Criterios de Comparación	 Beagleboard	 Alix D2D	 Odroid U2	 Pandaboard	 LNL 2220
Consumo de energía	Bajo	Medio	Medio	Alto	Alto
Procesador	ARM Cortex-A8	AMD Geode LX800	Samsung Exynos4412	ARM Cortex-A9 MPCore	32 Bits
Velocidad de puertos	Alta	Baja	Media	Baja	Media
Expansión	Si	Si	No	Si	Si
Conectividad	Ethernet	Ethernet	Ethernet	Ethernet	Ethernet
Memoria RAM	512MB	256MB	2048MB	1024MB	6MB
Costo	Medio	Medio	Medio	Medio	Alto

Tabla 3. Comparación entre cinco sistemas embebidos

Fuente: Autor

10. CAPITULO 6: DESCRIPCIÓN DEL SISTEMA DE CONTROL DE ACCESOS

10.1 Generalidades

A la hora de plantear la selección óptima del sistema domótico y su implantación se han de tener en cuenta una serie de variables relacionadas con el tipo y características del edificio, así como sus condiciones de uso.

Las características de la edificación se refieren al uso residencial o no del mismo, la ubicación, el régimen de uso, si es o no de nueva construcción y al carácter público y/o privado. Con una vivienda nueva, por ejemplo, siempre es más sencillo poder utilizar cualquier tipo de tecnología dada la posibilidad de realizar cuantas canalizaciones sean precisas.

El uso o utilización al que se destina el edificio que se pretende automatizar aporta detalles significativos; no es lo mismo plantear el diseño para un restaurante, que para una cafetería o negocio en general, un edificio industrial, una instalación deportiva o dedicada al trasporte de personas o mercancías, un edificio administrativo, un hospital, etc. Cada uno de ellos determina un conjunto de variables que requieren de un tratamiento especial al que el sistema tiene que dar respuesta.

Por último, detalles constructivos y característicos de la edificación como el número de plantas, estancias por planta, tipo de paramentos horizontales y verticales, número de metros cuadrados, disposición de puertas y ventanas, etc., apuntan nuevos datos para el correcto desarrollo del proyecto.

10.2 Distribución física en puntos estratégicos

10.2.1 Plano de distribución Laboratorio Automatización

En la ilustración 16, podemos apreciar la distribución física del Laboratorio de Automatización, ubicado en el sexto piso del edificio de ingenierías. Se cuenta con una puerta doble, la cual permite el acceso a los estudiantes. Todo lo que se encuentra dentro es de gran importancia y por ende se debe garantizar la seguridad para que solo el personal autorizado pueda ingresar a dicho laboratorio.

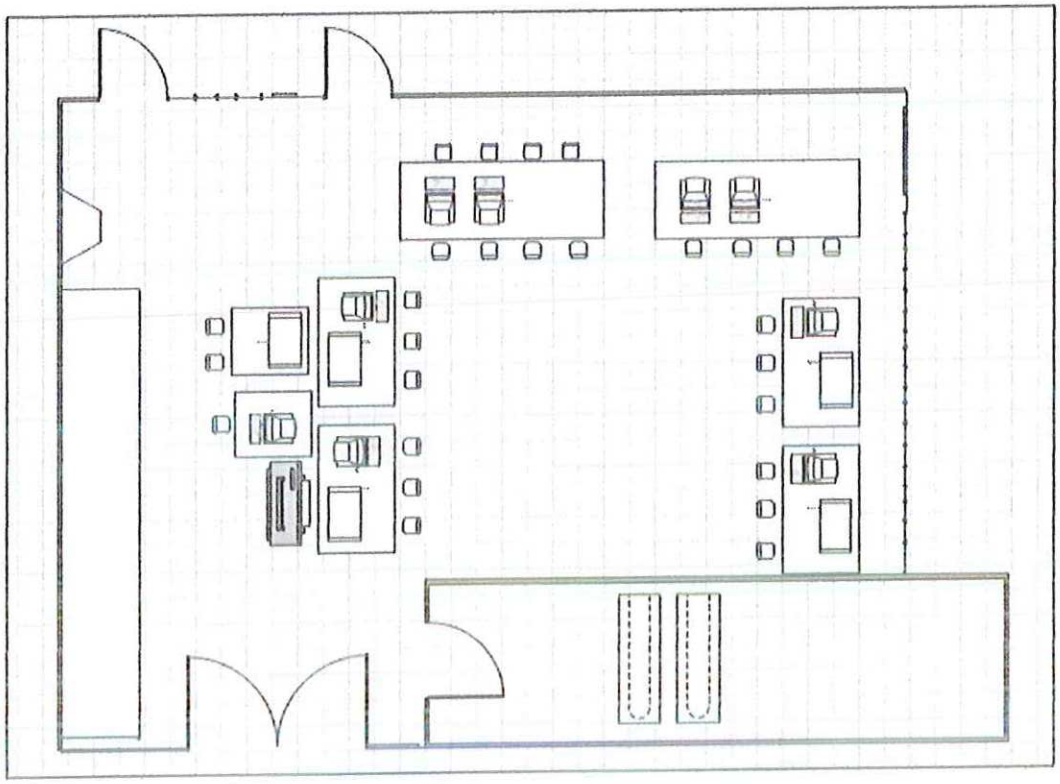


Ilustración 16. Plano Laboratorio Automatización

Fuente: Autor

10.2.2 Plano de distribución Laboratorio CIM

A continuación, en la ilustración 17 podemos observar el plano la distribución física del Laboratorio CIM, ubicado en el sexto piso del edificio de ingenierías. Se cuenta con una puerta doble, la cual permite el acceso a los estudiantes. De igual forma, que en el laboratorio de automatización, todos los elementos, máquinas, computadores, etc., son de gran importancia y relevancia para prestar un correcto servicio a los estudiantes, por tal razón se debe garantizar la seguridad en dicho laboratorio.

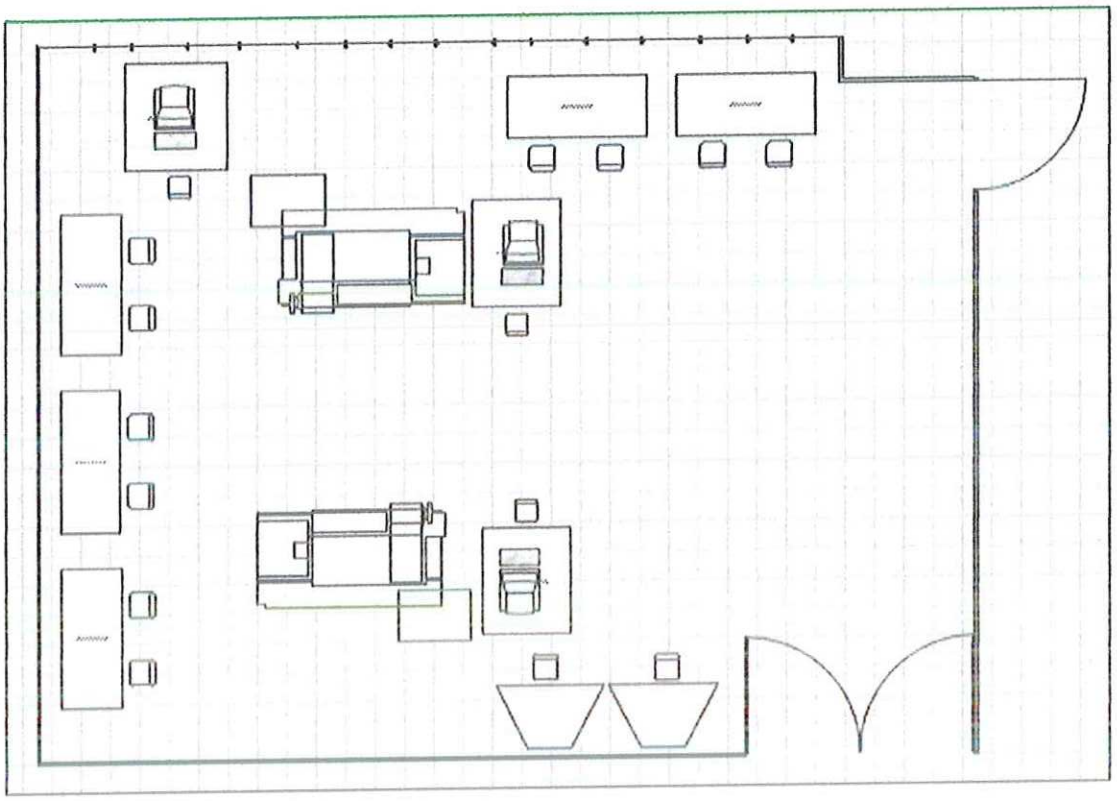


Ilustración 17. Plano Laboratorio CIM

Fuente: Autor

10.2.3 Plano de distribución Centro de estudios

En el plano de la ilustración 18, se puede apreciar la distribución física del Centro de estudios de ingeniería mecatrónica, ubicado en el séptimo piso del edificio de ingenierías. Se cuenta con una puerta doble, la cual permite el acceso a los estudiantes. Todo lo que se encuentra dentro es de gran importancia y por ende se debe garantizar la seguridad para que solo el personal autorizado pueda ingresar a dicho laboratorio.

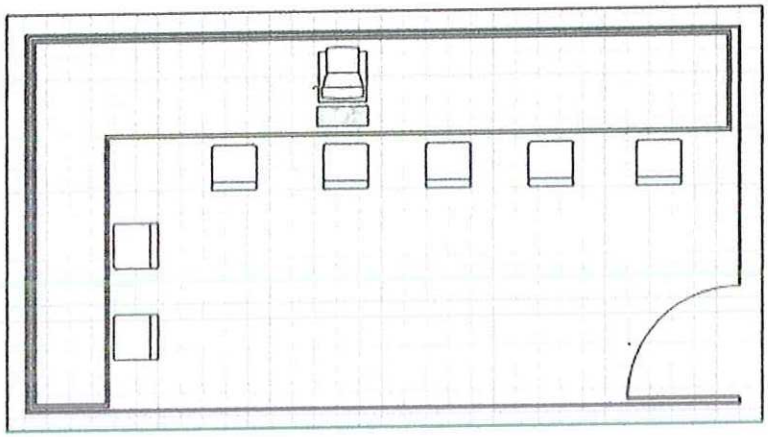


Ilustración 18. Plano Centro de estudios

Fuente: Autor

10.3 Requerimientos de usuarios

Se realiza una encuesta de diez preguntas puntuales que tiene como objetivo identificar los requerimientos necesarios para el diseño de un sistema de control de acceso en tres áreas específicas del edificio de ingenierías.

La muestra se destina para treinta personas, entre profesores y estudiantes de diferentes semestres de ingeniería mecatrónica (Anexo 1).

10.4 Proceso de control de acceso

El proceso de control de acceso empieza cuando el usuario presenta la credencial al lector, que normalmente está próximo a la puerta o portal de entrada. El lector extrae los datos de la tarjeta lo procesa y lo envía al panel de control(SCALA).

En primera instancia el panel de control valida el lector y luego acepta los datos transmitidos por el lector. Lo que ocurre luego depende si el sistema es centralizado o distribuido(SCALA).

En un sistema centralizado, el panel de control transmite los datos al servidor de control de acceso. El servidor de control de acceso compara los datos recibidos de la tarjeta con la información sobre el usuario que está almacenado en la base de datos. El programa de control de acceso determina los privilegios de acceso del usuario y su

autorización, la hora, la fecha y la puerta a la que se va a ingresar y cualquier otra información que se requiera para garantizar la seguridad dentro del área. Cuando se autoriza el acceso, el servidor de control de acceso envía una señal al panel de control para abrir la puerta: el panel de control envía dos señales, una a la cerradura de la puerta correspondiente, que abre la puerta y una al lector de la puerta, que emite un sonido audible u otro tipo de señal que indica al usuario que puede entrar(SCALA).

En un sistema distribuido, el panel de control permite o niega la entrada. El servidor de control de acceso periódicamente provee datos al panel de control, que habilita al software del panel de controla determinar si el usuario está autorizado o no para tener acceso. El panel de control, entonces, realiza las funciones del servidor de control de acceso descrito arriba y toma la decisión de permitir o negar la entrada. El habilitar el panel de control para realizar la función de decisión tiene la ventaja de requerir menor comunicación entre los paneles de control y el servidor de control de acceso central, *mejorando el desempeño y la confiabilidad del sistema como un todo*(SCALA).

10.5 Identificación de elementos

El sistema de control de accesos representa el conjunto de dispositivos que permiten monitorear, registrar, validar y generar señales de notificación de un evento en particular relacionado con el registro, reporte ingreso o egreso de personas a ciertas áreas, en este caso son los laboratorios CIM, Automatización y Centro de estudios.

A partir de las sugerencias y respuestas obtenidas de la encuesta, se puede dar una idea de qué elementos, dispositivos, sensórica, y demás se necesitan para garantizar la seguridad y controlar el acceso en las áreas críticas mencionadas anteriormente.

El sistema estará conformado por una credencial o tarjeta de identificación con el código QR, una interfaz de usuario, la base de datos, una cerradura electromagnética, una cámara, una Beagleboard-XM Rev C. A continuación, se realiza una breve descripción de cada componente del sistema de control de acceso.

10.5.1 Credencial o tarjeta de identificación

Se utiliza una tarjeta que incluya un código QR en su superficie, el cual debe ser leído por la cámara. La información del usuario está contenida en la base de datos y dependiendo del estado en que se encuentre le será permitido o no acceder al laboratorio.

10.5.2 Lector de puerta de acceso

Para leer o interpretar un código QR es necesario usar una cámara o un dispositivo que cuente con esta.

10.5.3 Base de datos

Es un componente de alta importancia, pues se requiere para almacenar toda la información de los usuarios que se beneficiarán del control de acceso en los respectivos laboratorios. Se estudian cuatro motores de base de datos y finalmente se escoge el que mejor se adapte a las necesidades del problema.

10.5.4Cerradura de puerta

Corresponde al actuador del sistema; se propone trabajar con una cerradura electromagnética, que será instalada en cada puerta de acceso.

10.5.5 Tarjeta controladora

Se propone utilizar la tarjeta de desarrollo Beagleboard-Xm como elemento central que integre todo el sistema.

10.5.6 Interfaz de usuario

Se requiere diseñar y desarrollar una interfaz gráfica que permita acceder al sistema, donde se visualice un menú principal y se accedan a todas las opciones que este contemple.

10.5.7 Otros

Dentro de este grupo se encuentran posibles componentes de menor "jerarquía" pero con igual relevancia que los anteriores, ya que garantizarán el correcto funcionamiento del sistema. Tal es el caso de los cables de conexión, componentes electrónicos diversos, conectores y demás elementos.

10.6 Selección de dispositivos

10.6.1 Credencial o tarjeta de identificación

Se propone el diseño de la tarjeta, teniendo en cuenta que debe llevar en su superficie el código QR para proporcionarle el acceso a los usuarios de la facultad. Como bien se muestra en la figura 19, para evitar el texto sobre la tarjeta se incluye el código bidimensional (QR Code). La apariencia final de la tarjeta puede verse en la ilustración 20, donde se tendrá la foto del usuario y el código qr respectivo.

Ilustración 19. Ejemplo de Tarjeta de acceso

Fuente: http://www.internetpronto.com/images/stories/ban_acredita.jpg

Ilustración 20. Credencial o tarjeta de acceso

Fuente: http://www.ultramagicard.es/tecnologia/codigo-de-barras/

10.6.2 Base de datos

Para elegir el servidor de base de datos, se estudiaron diferentes características y parámetros, sin embargo los principales se relacionan con: la independencia de los datos, seguridad, visualización de la información y la integridad de los datos.

En la tabla 4, se muestran seis columnas; la primera contiene los criterios de evaluación, la segunda el porcentaje, y las otras cuatro corresponden a los motores de bases de datos estudiados previamente.

Se le asignan un peso o un porcentaje a cada criterio y se les da una calificación según el grado de cumplimiento o satisfacción del parámetro evaluado. El rango de dicha evaluación está entre 1 (uno) y 5 (cinco). Finalmente, se promedian los valores y la opción con la calificación más alta será la elegida.

Criterios de Selección	Porcentaje (%)	MySQL	Microsoft Office Access	Oracle	SQL Server
Independencia de los datos	20	5	4.2	4	4.5
Seguridad	30	4	4	4.2	4
Visualización de la información	20	5	3.6	3.8	4.3
Integridad de los datos	30	5	4	4	4
Total	100	4.7	3.9	4	4.2

Tabla 4. Evaluación de parámetros entre cuatro motores de base de datos

Fuente: Autor

10.6.3 Cerradura de puerta de acceso

En la tabla 5, se muestran los resultados de la evaluación realizada teniendo en cuenta cuatro criterios importantes a la hora de seleccionar la cerradura electromagnética.

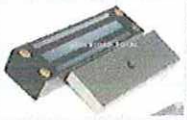
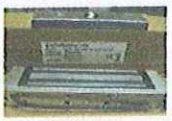
Criterios de Selección	Porcentaje (%)	 E-941SA-600	 Cerradura electromagnética universal 150 Kilos	 Cerradura Electromagnética de 1200 Lbs. YM-500	 EM-291
Facilidad de instalación	30	3.5	4.2	3.2	3
Mantenimiento	20	4	4.3	4	4
Consumo de energía	20	2	4.5	2.5	2.5
Costo	30	2	4	1.5	2.5
Total	100	2.9	4.2	2.7	3

Tabla 5. Evaluación de parámetros entre cuatro cerraduras electromagnéticas

Fuente: Autor

En el Anexo 6, puede verse el circuito electrónico para la activación de dicho componente.

10.6.4 Cámara

Para este caso, usamos la cámara del laptop, la cual es la encargada de realizar la lectura del código desde la interfaz de usuario diseñada.

10.6.5 Tarjeta de desarrollo

A continuación, se observa en la tabla 6 los resultados de la evaluación realizada teniendo en cuenta siete criterios importantes a la hora de seleccionar la tarjeta de desarrollo; consumo de energía, procesador, velocidad de puertos, expansión, conectividad, memoria RAM y costo.

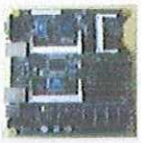
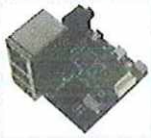
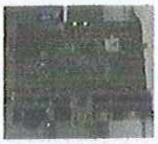
Criterios de Selección	Porcentaje (%)	 Beagleboard	 Alix D2D	 Odroid U2	 Pandaboard	 LNL 2220
Consumo de energía	15	5	3.5	3.5	2.5	2.5
Procesador	20	4.5	3.7	4	4	4
Velocidad de Puertos	5	5	2.5	3.6	2.4	3.7
Expansión	10	5	4.5	1	4.5	4.5
Conectividad	15	5	4.6	4.6	4.6	4.6
Memoria RAM	20	3.5	1.5	4	4	1.5
Costo	15	3.5	4	4	4	1
Total	100	4.4	3.5	3.7	3.9	2.9

Tabla 6. Evaluación de parámetros entre cuatro tarjetas controladoras

Fuente: Autor

10.6.6 Interfaz de usuario

Se diseñó una interfaz en PHP; lenguaje de programación de uso general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico. El código es interpretado por un servidor web con un módulo de procesador de PHP que genera la página Web resultante.

Cuenta con un menú principal, el cual presenta tres opciones; iniciar lector de códigos qr, panel de usuarios y panel bitácora. De allí, se despliega una pantalla que solicita al usuario el uso de la cámara para iniciar lectura del código, se debe dar click a la opción de permitir.

En el panel de usuarios, podemos visualizar parámetros del usuario existente en la base de datos, tales como: ID, nombre, código, email, código qr, estado y acciones.

Además, permite visualizar el código qr del usuario en una sola pantalla.

En relación a las acciones que realiza, la interfaz permite visualizar la forma como se crea, edita y elimina cualquier parámetro del usuario.

Finalmente, en el panel bitácora se aprecia una tabla que muestra parámetros importantes del usuario tales como; ID, código qr, nombre, fecha de ingreso y autorización, con el fin de llevar el control y registro de las personas que ingresan a los laboratorios.

10.7 Planteamiento de la solución

Una vez son identificados y seleccionados los elementos necesarios para el desarrollo del prototipo, nacen incógnitas sobre cómo, de qué manera, bajo que software o sistema se va a trabajar y como se van a enlazar dichos elementos.

Algo claro e inmodificable en el diseño del prototipo, se relacionaba con la inclusión de los códigos qr y la tarjeta de desarrollo Beagleboard-XM Rev C.

A partir de la investigación previa sobre esta tarjeta de desarrollo, se estableció la estructura del sistema de control de accesos; se estudiaron dos parámetros importantes como el funcionamiento y sistema operativo que soporta para establecer la solución.

A continuación, se muestra en la tabla 7 los parámetros evaluados para escoger el sistema operativo a trabajar con la beagleboard-XM.

Criterios de Selección	Porcentaje (%)	XBMC	Ubuntu	Angstrom Linux	Android
Facilidad de instalación	15	3.2	4	5	3
Entorno Amigable	15	2	5	3.5	3.2
Drivers	30	3	3.5	5	3
Disponibilidad de información	40	3	5	1	3
Total	100	2.8	4.4	3.6	3.1

Tabla 7. Compatibilidad de software Beagleboard-XM

Fuente: Autor

Como se observa, la calificación mas alta la recibió Ubuntu, por lo que se decidió instalarlo en la Beagleboard-XM.

Seguido a esto, fue indispensable preguntarse, analizar, pensar e imaginar la forma en que se iba a procesar la información, cómo se iba a leer y decodificar el qr, cómo se iba a conectar la cámara, para lo cual se plantearon dos opciones:

1) Utilizar una Beagleboard-XM que integre los tres laboratorios, tres cámaras, tres cerraduras electromagnéticas, interfaz de usuario, base de datos, bitácora (Ilustración 21).

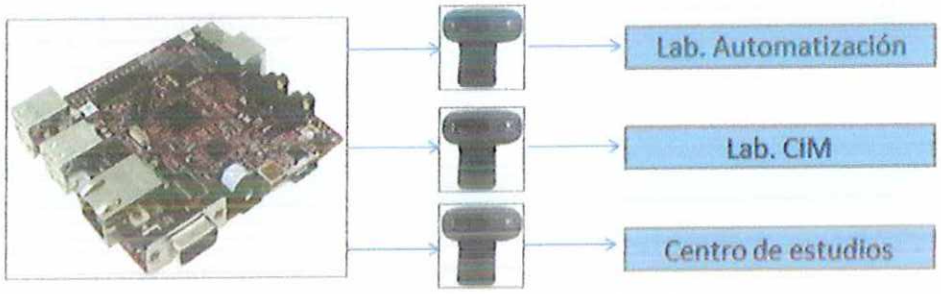


Ilustración 21. Estructura centralizada para control de acceso

Fuente: Autor

2) Utilizar tres Beagleboard-XM para cada laboratorio, tres cámaras, tres cerraduras electromagnéticas, interfaz de usuario, base de datos, bitácora (Ilustración 22).

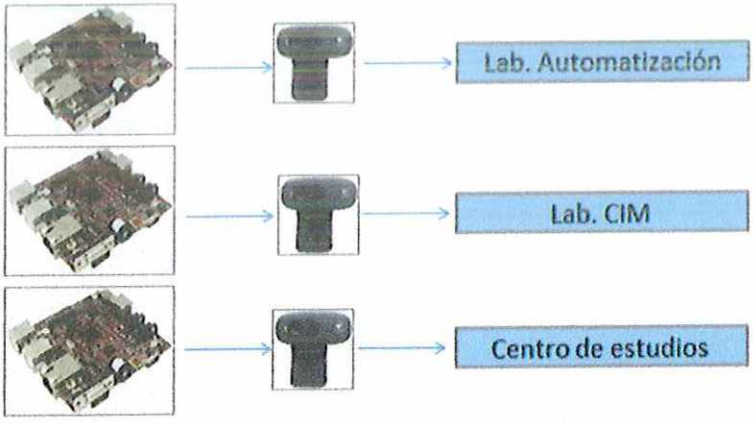


Ilustración 22. Estructura distribuida para control de acceso

Fuente: Autor

La opción elegida fue la primera, ya que permite reducir el hardware y software, lo que se traduciría en mayor eficiencia y confiabilidad para el usuario.

Teniendo en cuenta lo anterior, el paso a seguir fue crear una base de datos que almacenara algunos parámetros de los usuarios y permitiera llevar el registro de entrada a los laboratorios.

Finalmente, se diseña una interfaz de usuario que visualice la información almacenada en la base de datos indispensable para el control de acceso en los laboratorios.

10.8 Descripción del sistema de control de acceso

- En la ilustración 23, se evidencia el esquema general del prototipo desarrollado para el control de acceso en los laboratorios Automatización, CIM y Centro de estudios.

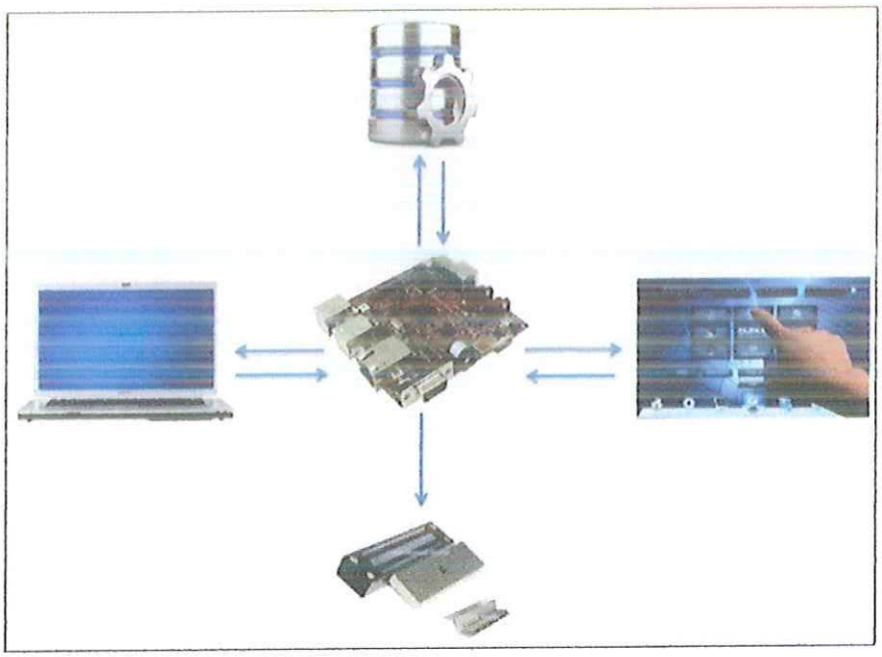


Ilustración 23. Diagrama general de control de acceso

Fuente: Autor

Como se ha mencionado anteriormente, la beagleboard-XM fue utilizada para controlar todo el sistema de control de accesos, para este caso se utilizó como un servidor encargado de almacenar los datos y procesar la información que allí se guardó.

La forma como se logró esta estructura se describe en los siguientes pasos:

1) Se instaló el sistema operativo Ubuntu 12.04 para iniciar la beagleboard- XM y correr los archivos y carpetas necesarios para el correcto funcionamiento del prototipo.

2) Se instaló el servidor APACHE para acceder por IP a la interfaz de usuario diseñada.

3) Para manejo de la base de datos y registro de usuarios se utilizó MySQL.

4) Se utilizó un framework de PHP denominado Laravel, el cual permite agilizar la programación.

5) Se utiliza la tecnología CSS para estilizar el diseño web de la interfaz (módulos de la bitácora, panel de usuarios, base de datos, etc).

6) Para la lectura del código QR se utilizó la librería HTML5- QRCode, se programa en JavaScript que tiene soporte en HTML5, para activar la cámara dentro del navegador del servicio que para este caso es GoogleChrome (Es obligatorio que el navegador tenga soporte en HTML5).

7) La forma como se planteó la lectura del código QR hace que sea un servicio que siempre está escuchando o corriendo, en espera de leer y decodificar un qr.

8) En relación a la verificación de ingreso a los laboratorios, se realizó una comparación entre el código qr de cada usuario almacenado en la base de datos y la cadena que me genera la libreríaHTML5-QRCode. Si existe el código QR, busca en la base de datos el qr almacenado y dependiendo de la concordancia envía un "0" ó "1", esto se guarda en la bitácora.

9) La beagleboard-XM se clasifica como una "single board computer", es decir un ordenador de placa reducida; se centra en un sólo microprocesador con la RAM, E/S y todas las demás características de un computador funcional. Cuenta con una interfaz de GPIO, visto en carpetas con fácil acceso. Normalmente, la ruta que se sigue para hacer modificaciones o activaciones es: sys/class/GPIO.

   Para visualizar la autenticación o no de un usuario se utilizan dos Leds. Se hace necesario escribir las instrucciones de High y Low a las carpetas que se generan una vez escogidos los GPIO (Para este caso se escogieron el 132 y 133) (Anexo 7).

10.9 Diagrama de flujo del funcionamiento del sistema

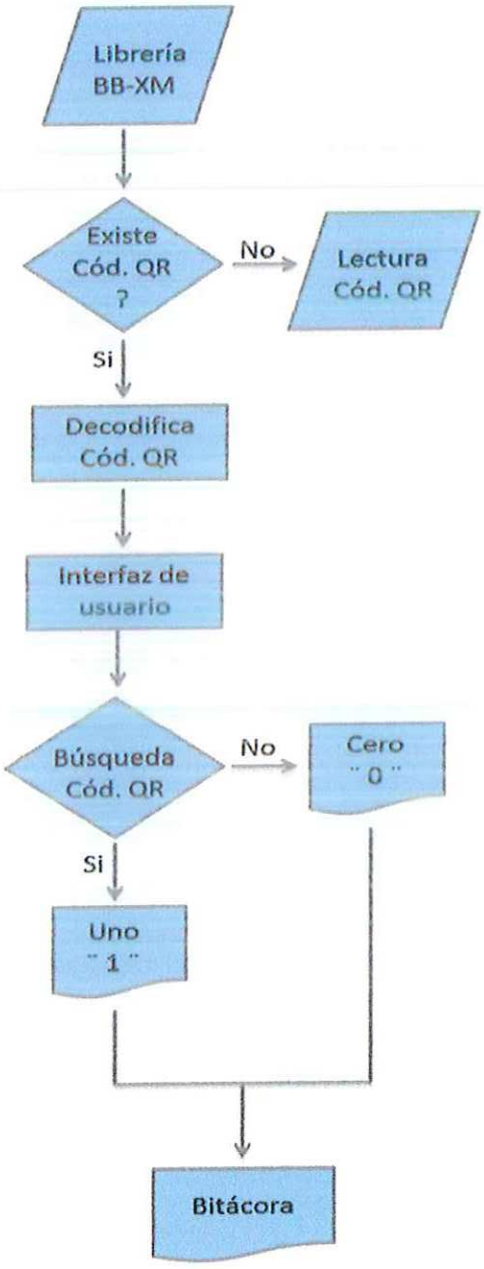


Ilustración 24. Diagrama de flujo del funcionamiento del sistema

Fuente: Autor

En la ilustración 24, se aprecia el diagrama de flujo del funcionamiento del sistema de control de acceso. Inicialmente, se tiene en la Beagleboard-XM la librería HTML5-QRCode, que es la encargada de identificar el qr. Si el código se ubica frente a la cámara y es identificado por la librería, ésta pasa a decodificarlo. De lo contrario sigue leyendo hasta que encuentre un código qr válido.

Una vez decodificado, va a la interfaz de usuario e inicia la búsqueda del código almacenado en la base de datos (asignado previamente a cada usuario), si el usuario existe (Estado = Activo) asigna el valor ¨1¨, de lo contrario asigna un ¨0¨.

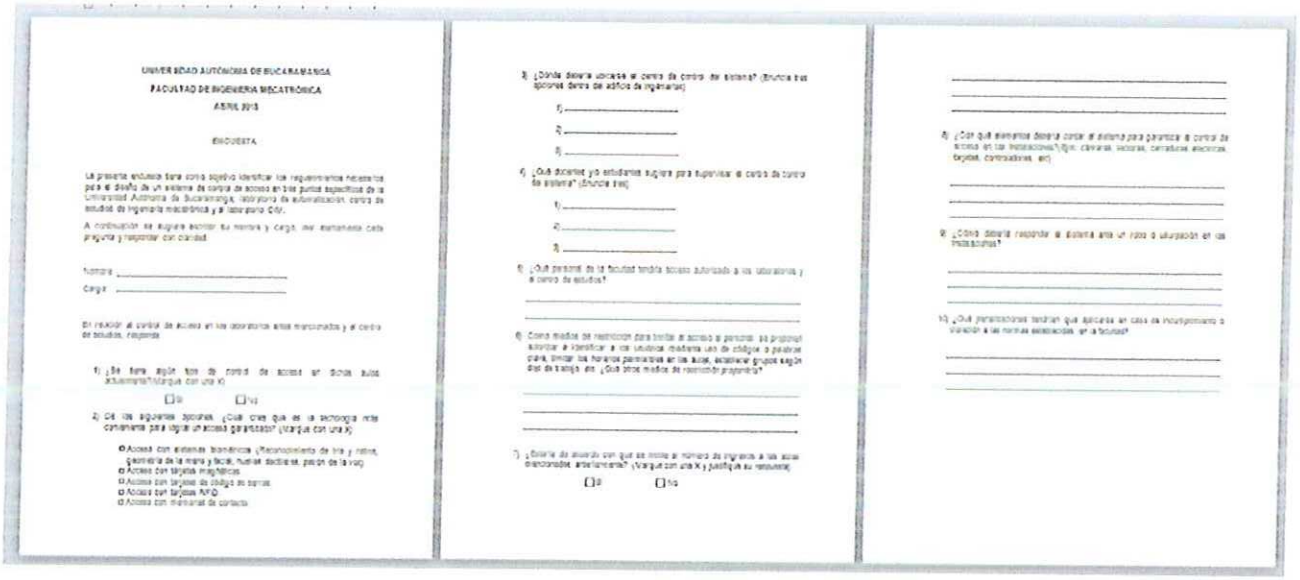
Finalmente, estos valores se guardan en el panel Bitácora para llevar el registro de usuarios que ingresaron o no a los laboratorios.

11. CAPITULO 7: ANEXOS

11.1 Anexo 1: Encuesta

- **Formato de la encuesta**

Encuesta realizada a estudiantes y docentes Facultad Ingeniería Mecatrónica.



UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA
FACULTAD DE INGENIERÍA MECATRÓNICA
ABRIL 2018

ENCUESTA

La presente encuesta tiene como objetivo identificar los requerimientos necesarios para el diseño de un sistema de control de acceso en tres puntos específicos de la Universidad Autónoma de Bucaramanga, laboratorio de automatización, cerca de estudio de ingeniería mecatrónica y el laboratorio CIM.

A continuación se solicita escribir su nombre y cargo, leer detenidamente cada pregunta y responder con claridad.

Nombre _____

Cargo _____

En relación al control de acceso en los laboratorios antes mencionados y el cerca de estudios, responda:

1) ¿Se tiene algún tipo de control de acceso en dichos sitios actualmente?(Marque con una X)

☐Si ☐No

2) De las siguientes opciones ¿Cuál cree que es la tecnología más conveniente para regular un acceso garantizado? (Marque con una X)

- Acceso con sistemas biométricos (Reconocimiento de iris y retina, geometría de la mano y facial, huellas dactilares, patrón de la voz)
- Acceso con tarjetas magnéticas
- Acceso con tarjetas de código de barras
- Acceso con tarjetas RFID
- Acceso con teléfonos de contacto

3) ¿Dónde debería ubicarse el cerco de control de sistema? (Enuncie tres opciones dentro de edificio de ingeniería)

1) _____
2) _____
3) _____

4) ¿Qué docentes y/o estudiantes sugiere para supervisar el cerco de control de sistema? (Enuncie tres)

1) _____
2) _____
3) _____

5) ¿Qué personal de la facultad tendría acceso autorizado a los laboratorios y al cerco de estudios?

_____
_____
_____

6) Como medios de restricción para brindar el acceso al personal se propone autorizar e identificar a los usuarios mediante uso de código o palabra clave, limitar los horarios permitidos en las aulas, establecer grupos según días de trabajo etc. ¿Qué otros medios de restricción propondría?

_____
_____
_____

7) ¿Estaría de acuerdo con que se lleve el número de ingresos a las aulas mencionadas anteriormente? (Marque con una X y justifique su respuesta)

☐Si ☐No

_____
_____
_____

8) ¿Con qué elementos debería contar el sistema para garantizar el control de acceso en las instalaciones?(Ejm: cámaras, lectores, cerraduras electrónicas, tarjetas, contraseñas, etc)

_____
_____
_____

9) ¿Cómo debería responder el sistema ante un robo o situación en las instalaciones?

_____
_____
_____

10) ¿Qué penalizaciones tendrían que aplicarse en caso de incumplimiento o violación a las normas establecidas en la facultad?

_____
_____
_____

Anexo 1. Encuesta aplicada

*Tamaño de la muestra: 20

*Número de estudiantes encuestados: 16

*Número de docentes encuestados: 4

*Número de preguntas realizadas: 10

- ***Objetivo de la encuesta***

Identificar los requerimientos necesarios para el diseño de un sistema de control de acceso en tres puntos específicos de la Universidad Autónoma de Bucaramanga;

laboratorio de automatización, centro de estudios de ingeniería mecatrónica y el laboratorio CIM.

- **Preguntas**

En relación al control de acceso en los laboratorios antes mencionados y el centro de estudios, responda:

1) ¿Se tiene algún tipo de control de acceso en dichas aulas actualmente?(Marque con una X)

   ☐ Si ☐ No

2) De las siguientes opciones, ¿Cuál cree que es la tecnología más conveniente para lograr un acceso garantizado? (Marque con una X)

   - ☐ Acceso con sistemas biométricos (Reconocimiento de iris y retina, geometría de la mano y facial, huellas dactilares, patrón de la voz)
   - ☐ Acceso con tarjetas magnéticas.
   - ☐ Acceso con tarjetas de código de barras.
   - ☐ Acceso con tarjetas RFID.
   - ☐ Acceso con memorias de contacto.

3) ¿Dónde debería ubicarse el centro de control del sistema? (Enuncie tres opciones dentro del edificio de ingenierías)

   1)_____

   2)_____

   3) _____

4) ¿Qué docentes y/o estudiantes sugiere para supervisar el centro de control del sistema? (Enuncie tres)

   1)_____

   2)_____

   3) _____

5) ¿Qué personal de la facultad tendría acceso autorizado a los laboratorios y el centro de estudios?

_____

_____

6) Como medios de restricción para limitar el acceso al personal se proponen autorizar e identificar a los usuarios mediante uso de códigos o palabras clave, limitar los horarios permisibles en las aulas, establecer grupos según días de trabajo, etc. ¿Qué otros medios de restricción propondría?

_____

_____

_____

7) ¿Estaría de acuerdo con que se limite el número de ingresos a las aulas mencionadas anteriormente? (Marque con una X y justifique su respuesta)

☐ Si ☐ No

_____

_____

_____

8) ¿Con qué elementos debería contar el sistema para garantizar el control de acceso en las instalaciones?(Ejm: cámaras, lectoras, cerraduras eléctricas, tarjetas, controladores, etc)

_____

_____

_____

9) ¿Cómo debería responder el sistema ante un robo o usurpación en las instalaciones?

10) ¿Qué penalizaciones tendrían que aplicarse en caso de incumplimiento o violación a las normas establecidas en la facultad?

11.2 Anexo 2: Cronograma de Actividades

En el anexo 2, podemos ver el cronograma semestral que se ha llevado a cabo para el desarrollo del proyecto.

- **Actividades**

1. Planteamiento de la solución: cómo, de qué manera, bajo que software o sistema se va a trabajar y como se van a enlazar dichos elementos.

2. Instalación de Ubuntu en la beagleboard-XM.

3. Analizar, pensar e imaginar la forma en que se iba a procesar la información, cómo se iba a leer y decodificar el qr, cómo se iba a conectar la cámara, para lo cual se plantearon dos opciones: 1) Utilizar una Beagleboard-XM que integre los tres laboratorios, tres cámaras, tres cerraduras electromagnéticas, interfaz de usuario, base de datos, bitácora. 2) Utilizar una Beagleboard-XM para cada laboratorio, tres cámaras, tres cerraduras electromagnéticas, interfaz de usuario, base de datos, bitácora.

4. Planteamiento de la estructura final del sistema de control de accesos.

5. Creación de la base de datos.

6. Lectura de la cámara web.

7. Lectura del código QR.

8. Diseño de la interfaz de usuario.

Cronograma desarrollo del proyecto						
ACTIVIDADES	SEMANA 1-4	SEMANA 5-8	SEMANA 9- 12	SEMANA 13-16	SEMANA 17-20	SEMANA 21- 24
1. Planteamiento de la solución: cómo, de qué manera, bajo que software o sistema se va a trabajar y como se van a enlazar dichos elementos.						
2. Instalación de Ubuntu en la beagleboard-XM.						
3. Analizar, pensar e imaginar la forma en que se iba a procesar la información, cómo se iba a leer y decodificar el qr, cómo se iba a conectar la cámara, para lo cual se plantearon dos opciones: 1) Utilizar una Beagleboard-XM que integre los tres laboratorios, tres cámaras, tres cerraduras electromagnéticas, interfaz de usuario, base de datos, bitácora. 2) Utilizar una Beagleboard-XM para cada laboratorio, tres cámaras, tres cerraduras electromagnéticas, interfaz de usuario, base de datos, bitácora.						
4. Planteamiento de la estructura final del sistema de control de accesos.						
5. Creación de la base de datos.						
6. Lectura de la cámara web.						
7. Lectura del código QR.						
8. Diseño de la interfaz de usuario.						

Anexo 2. Cronograma de actividades

11.3 Anexo 3: Panorama sistemas domóticos e inmóticos en Universidad Autónoma de Bucaramanga (UNAB)

- **Especificaciones solicitadas**

  - ✓ Implementación de un sistema de control para expandirse a 9 laboratorios de una Universidad.
  - ✓ Prototipo en dos laboratorios ubicados en el tercer y cuarto piso.
  - ✓ El centro de control quedará ubicado en el cuarto piso.
  - ✓ Sistema por tarjeta.
  - ✓ El sistema debe permitir que se asignen los horarios de ingreso por laboratorios, además debe permitir acceso por horas, franjas horarias o días.
  - ✓ La tarjeta debe deshabilitarse automáticamente luego de pasada la hora de préstamo.
  - ✓ Revisar opción para que en algunos laboratorios el acceso sea sin restricción en horario de oficina pero en horario nocturno si deba autorizarse el ingreso.
  - ✓ El sistema debe llevar estadísticas (ingreso y salida).
  - ✓ Opcional sistema de monitoreo con cámaras IP alámbricas.
  - ✓ 2 cámaras fijas para la entrada.
  - ✓ 4 internas de 360 grados.
  - ✓ Cotizar con cantonera o electroimán. (Un laboratorio se encuentra con cantonera).

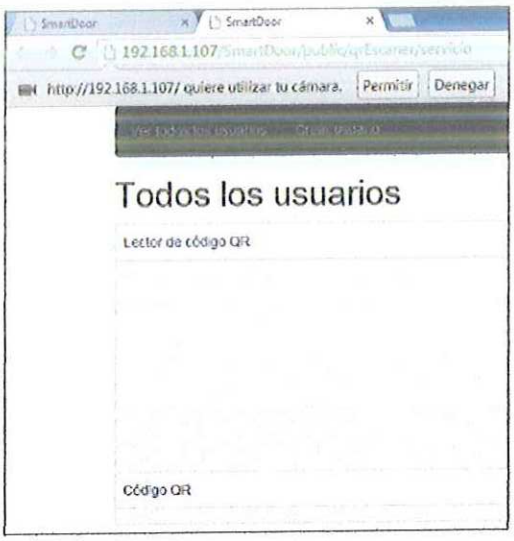
11.4 Anexo 4: Presupuesto

En la tabla 8, se muestran los dispositivos, elementos y lo necesario para la implementación del proyecto; la cantidad requerida y el precio de los mismos.

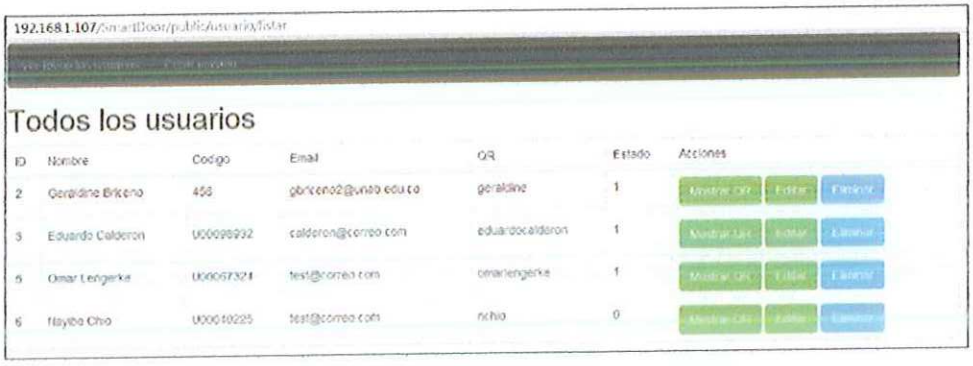
	Cantidad	Precio Individual	Precio final
Beagleboard- Xm	1	$450.000	$450.000
Cámara C270	3	$70. 000	$210.000
Cerradura electromagnética	3	$140.000	$420.000
Raspberry Pi	3	$130.000	$390.000
Instalación	--	$ A convenir	$ A convenir
Mantenimiento	--	$A convenir	$A convenir
Total	10	$790.000	$1.020.450

Tabla 8. Tabla presupuesto

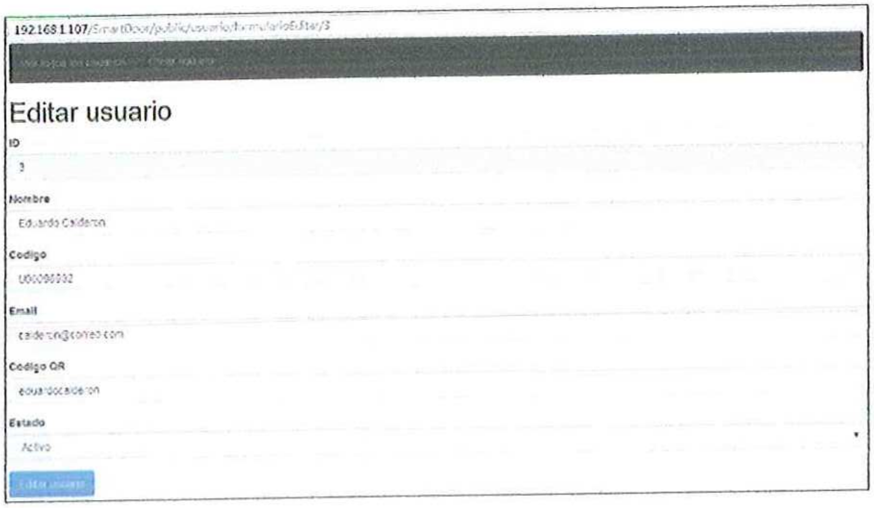
11.5. Anexo 5: Interfaz de usuario

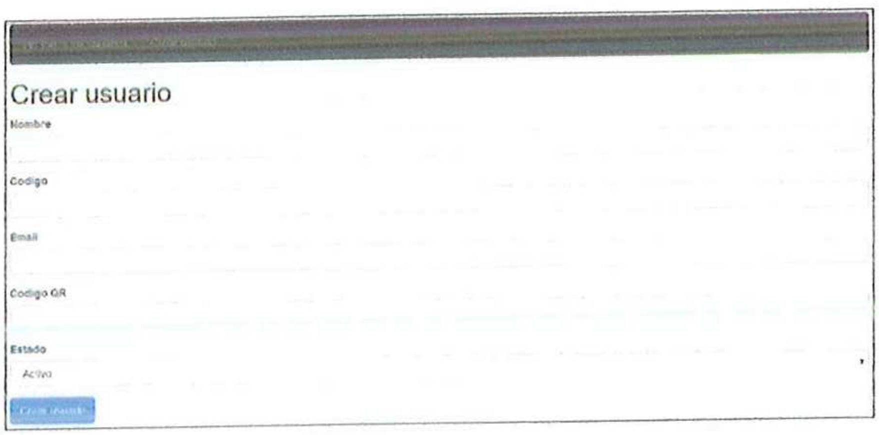



SmartDoor
SmartDoor
192.168.1.107/SmartDoor/public/qrEscaner/se
Todos los usuarios
Lector de código QR
Código QR


192.168.1.107/SmartDoor/public/usuario/listar
Todos los usuarios
ID Nombre Codigo Email QR Estado Acciones
2 Geraldine Briceno 456 gbriceno2@unab.edu.co geraldine 1
3 Eduardo Calderon U00099932 calderon@correo.com eduardocalderon 1
5 Omar Lengerke U00057321 test@correo.com omarlengerke 1
6 Hayibo Chio U00010225 test@correo.com nchio 0

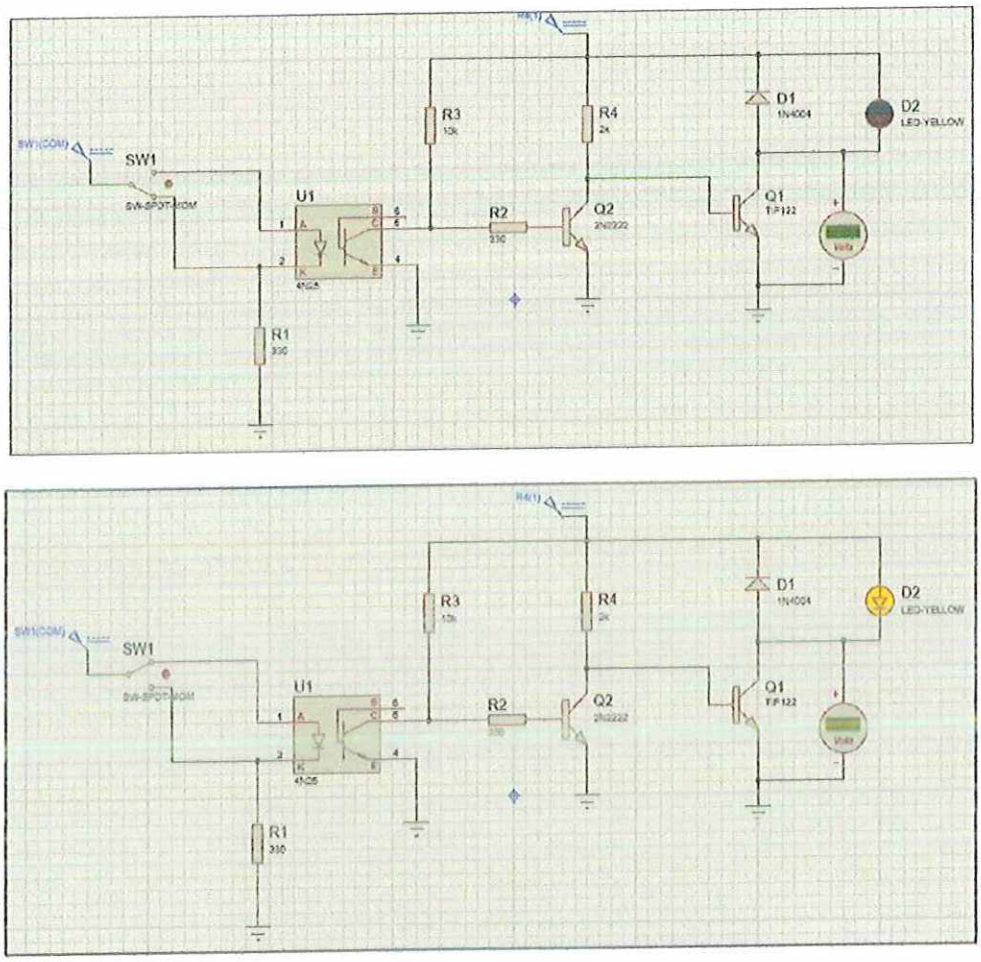

192.168.1.107/SmartDoor/public/usuario/mostrarQR/eduardocalderon
Codigo QR del usuario
Codigo QR
eduardocalderon



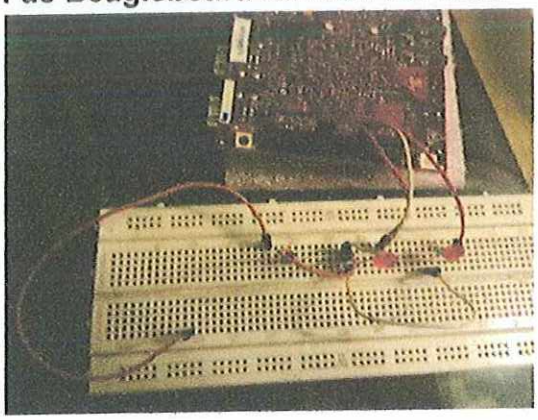


ID	Codigo QR	Usuario	Fecha de ingreso	Fue atorizado
1	sadglogsdfsoa454388	Geraldine Briceno	2014-01-15 00:00:00	1
2	saggndn6576678uzcx	Geraldine Briceno	2014-01-10 00:00:00	1
3	sdshgd657575	Omar Lengerke	2014-01-19 00:00:00	0
4	adar6456767565	Eduardo Calderon	2014-01-16 00:00:00	1
5	3167015953	Sin usuario registrado	2014-01-29 02:18:46	0
6	3167015953	Sin usuario registrado	2014-01-28 21:26:54	0
7	3167015953	Sin usuario registrado	2014-01-28 21:30:52	0
8	asdfghjmyikynn657ovacS	Sin usuario registrado	2014-01-28 21:31:21	1
9	asdfghjmyikynn657ovacS	Eduardo Calderon	2014-01-28 21:33:32	1
10	asdfghjmyikynn657ovacS	Eduardo Calderon	2014-01-28 21:33:33	1
11	asdfghjmyikynn657ovacS	Eduardo Calderon	2014-01-28 21:33:33	1
12	asdfghjmyikynn657ovacS	Eduardo Calderon	2014-01-28 21:34:13	1
13	asdfghjmyikynn657ovacS	Eduardo Calderon	2014-01-28 21:34:14	1
14	asdfghjmyikynn657ovacS	Eduardo Calderon	2014-01-28 21:34:15	1

11.6 Anexo 6: Circuito de activación Cerradura electromagnética



11.7 Anexo 7: Conexión de Beagleboard-XM con los Leds



12. GLOSARIO

Apache: Servidor web HTTP de código abierto, para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.12 y la noción de sitio virtual.

Beagleboard-XM: Tarjeta de bajo costo sin refrigeración por aire que presenta desempeño similar a un pc portátil (laptop), y capacidad de expansión sin la incomodidad por tamaño, el costo, o ruido típico de una máquina de escritorio.

CSS (Cascading Style Sheets): Lenguaje de hojas de estilos usado para describir la presentación semántica (el aspecto y formato) de un documento escrito en lenguaje de marcas. Su aplicación más común es dar estilo a páginas webs escritas en lenguaje HTML y XHTML, pero también puede ser aplicado a cualquier tipo de documentos XML, incluyendo SVG y XUL.

GPIO (General Purpose Input/Output, Entrada/Salida de Propósito General): Pin genérico en un chip, cuyo comportamiento (incluyendo si es un pin de entrada o salida) se puede controlar (programar) por el usuario en tiempo de ejecución.

HTML5 (Hyper Text Markup Language, versión 5): Quinta revisión importante del lenguaje básico de la World Wide Web, HTML. Especifica dos variantes de sintaxis para HTML: un «clásico» HTML (text/html), la variante conocida como HTML5 y una variante XHTML conocida como sintaxis XHTML5 que deberá ser servida como XML).1 2 Esta es la primera vez que HTML y XHTML se han desarrollado en paralelo.

Laravel: Framework de código abierto para desarrollar aplicaciones y servicios web con PHP 5. Su filosofía es desarrollar código PHP de forma elegante y simple, evitando el "código espagueti".

MySQL: Sistema de gestión de bases de datos relacional, multihilo y multiusuario.

PHP: Lenguaje de programación de uso general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico.

Ubuntu: Sistema operativo basado en Linux y que se distribuye como software libre, el cual incluye su propio entorno de escritorio denominado Unity.

13. CONCLUSIONES

- A partir del estudio de nuevas tecnologías, estándares y normativa se crearon las bases de conocimiento para plantear un prototipo de control de accesos en los laboratorios de la facultad de Ingeniería Mecatrónica.

- Mediante la evaluación de diferentes alternativas existentes en el mercado, se plantearon cuadros comparativos que ayudaron a la selección de los componentes y elementos del sistema.

- Gracias al desarrollo de una metodología de diseño mecatrónico, se estructuró el proyecto en general y se llegó a la mejor solución del problema.

- Para iniciar con la estimación de la cobertura que debía tener el sistema de control de accesos, se identificaron los diferentes accesos en las instalaciones del edificio de ingenierías mediante un plano usando Microsoft Visio 2010.

- Se implementa la Beagleboard-XM como un servidor para lograr el acceso desde diferentes locaciones.

- Se logró leer, identificar y procesar los códigos qr mediante la cámara web, permitiendo la autenticación del usuario de forma segura y práctica.

- Se logra diseñar una interfaz de administrador para gestionar el control de acceso en los laboratorios, permitiendo obtener información del usuario de forma rápida y práctica a la hora de llevar un registro o informe de ingresos por parte de las directivas de la facultad.

- Se consiguió diseñar el sistema Inmótico de control de accesos para los tres laboratorios; Automatización, CIM y Centro de estudios, siendo un prototipo de topología distribuida que ayuda a reducir costos de implementación.

- Con el presente proyecto, se genera un grado de confort para los estudiantes al ya no haber la necesidad de pasar carta para uso de los laboratorios de la facultad, simplemente con que sea autorizado el estudiante podrá acceder sin problema con su tarjeta.

14. BIBLIOGRAFIA

ALVARADO, J., A., *Sistema de control de acceso con RFID*. México, 2008.

ALVARADO, R., F., AYALA, G., A., CUEVA, W., E., *Plan piloto del diseño e implementación de un sistema de control de acceso de personal y seguridad para optimizar recursos de la facultad de arquitectura*. Ecuador, 2007.

COBOS, M., J., INTRIAGO, A., L., GARAY, F., LEYTON, E.,*Diseño inmótico para ahorro energético, seguridad y control de instalaciones para el nuevo edificio de la FIEC*. Ecuador, 2005.

FERNÁNDEZ. G., M., *Generador e intérprete QR Code*. Sevilla, 2009.

MARTIN, F., M., ARGUELLES, R., P., *Generalidades sobre domótica e inmótica*. España, 2008.

MILLARES, M., J., *Panoramica de los sistemas domóticos e inmóticos*. España, 2005.

PONCE, C., A.,*Implementación del sistema inmótico para el control de accesos en el Aeropuerto de Latacunga basado en la tecnología Lonworks*. Ecuador, 2011.

QUINTERO, J., M., LAMAS, J., SANDOVAL, J., D., *Domótica: sistemas de control para viviendas y edificios*. Madrid: Paraninfo, 2003.

RUBIO, G., REYES, P., J.,*Aplicación Inmótica De Control De Aulas Docentes de la E.T.S.I.T*. Málaga, 2007.

SCALA, *Uso de Tarjetas Inteligentes para un Control de Acceso Físico*. Clarksville, 2003.

VELAYOS, M., *Sistemas de control de accesos a edificios mediante tarjetas criptográficas y tarjetas RFID*. Madrid, 2007.

http://www.dynamoelectronics.com

http://beagleboard.org/hardware-xM

http://farm5.static.flickr.com/4068/4644432552_2fb4280336.jpg

http://www.pcengines.ch/alix2d2.htm

http://raspberryparatorpes.net/dudas/rivales-de-la-raspberry-odroid-u2/

http://csrg.inf.utfsm.cl/~rmujica/proyecto_arm.pdf

http://www.sourceaccesscontrol.com/product-profile/lenel-lnl-2220.html

http://cdn.lenel.com/collateral/HW_NGP-2220_ESP.pdf

http://www.logitech.com/es-es/webcam-communications/webcams

http://www.almacen-informatico.com/TRUST_InTouch-Chat-Webcam-16176_62397_p.htm

http://www.pixmania.com/es/es/9657065/art/soyntec/webcam-vga-joinsee-trade.html#pix-review

http://www.geniusnet.com/wSite/ct?xItem=19470&ctNode=1303&mp=3

http://code-two-qr-code-desktop-reader.softonic.com/

http://barcapture.softonic.com/

http://www.gratisprogramas.org/descargar/lector-de-codigos-qr-para-pc-mf/

http://cajondesastres.wordpress.com/2012/10/08/lector-de-codigos-qr-para-pc/

http://www.seco-larm.com/pdfs/Mi-E941SA_Sp.pdf

http://www.lcdtcorp.com/index.php/em-291.html

http://www.seco-larm.com/pdfs/Mi-E941SA_Sp.pdf

http://deloesteseguridad.com.ar/445,cerradura-electromagnetica-universal-150-kilos-ber-col-para-puertas-comunes-blindex-de-escape-emergencia-antipanico.html

http://www.seguridadpercol.com/cerraduras%20electromagneticas.html

http://s1.hipertextual.com/wp-content/blogs.dir/3/files/2008/07/sony-vaio-fw-frontal.jpg imagen pc

https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcSFVRnHaEsR9CDHv1YHVIRTyAQu2UT2arFVAMQo1BS-bM1djJlUSg

http://www.liquidware.com/system/0000/3754/BeagleBoard_xM_Angle_1.jpg

http://us.123rf.com/400wm/400/400/lcs813/lcs8131308/lcs813130800025/21616028-optimizacia-n-de-base-de-datos-y-el-concepto-de-configuracia-n-base-de-datos-con-cremallera-de-metal.jpg

http://www.arcapelectronica.com.ar//imagenes_misaplicaciones/domotica%20interfaz%20usuario%20empresa%20222.jpg

http://static.freepik.com/foto-gratis/hombre-usuario-icono-de-clip-art_421787.jpg

http://www.digitaltrends.com/wp-content/uploads/2012/10/samsung-series-5-ultra-touch.jpeg laptop

http://imagenes.pccomponentes.com/logitech_hd_webcam_c270_2.jpgcam

http://www.itespresso.es/wp-content/uploads/2010/04/laptop-webcam.jpg

http://www.sigmaelectronica.net/beagleboard-p-1529.html