UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:

INGENIERO EN ELECTRÓNICA DIGITAL Y TELECOMUNICACIONES

TEMA: SISTEMA DE SEGURIDAD AUTOMATIZADO DE VIDEOVIGILANCIA CON ARDUINO PARA LA UNIDAD EDUCATIVA “LUXEMBURGO”.

AUTOR: LUIS ALFREDO FLORES ROGEL

TUTOR: Ing. David Cando Garzón Mg.

AÑO: 2016

INFORME FINAL DE RESULTADOS DEL PIC

CARRERA:	Electrónica Digital y Telecomunicaciones
AUTOR/A:	Luis Alfredo Flores Rogel
TEMA DEL TT:	Sistema de seguridad automatizado de videovigilancia con Arduino para la Unidad Educativa “Luxemburgo”.
ARTICULACIÓN CON LA LÍNEA DE INVESTIGACIÓN INSTITUCIONAL:	Desarrollo de Sistemas Automáticos para la Mejora de Seguridad y Movilidad en la Ciudad de Quito
SUBLÍNEA DE INVESTIGACIÓN INSTITUCIONAL:	Sistema de Control Automático para la Seguridad y Movilidad Ciudadana
ARTICULACIÓN CON EL PROYECTO DE INVESTIGACIÓN INSTITUCIONAL DEL ÁREA	Sistema de Seguridad para instituciones Educativas
FECHA DE PRESENTACIÓN DEL INFORME FINAL:	22 de agosto del 2016

RESUMEN

El presente proyecto titulado Sistema de Seguridad Automatizado de Videovigilancia con Arduino se enfoca en mantener la seguridad en la institución educativa por medio del monitoreo de las cámaras y en control al ingreso del laboratorio de computación de la Unidad Educativa “Luxemburgo”.

Por medio de las cámaras de seguridad y el DVR ubicado en un lugar seguro lejos de la zona vulnerable, garantizará la grabación del video sobre lo que suceda dentro del laboratorio y a sus alrededores.

El control de acceso es un dispositivo capaz de permitir el acceso sólo a las personas que ingresen la contraseña de forma correcta y así evitará que personas ajenas ingrese al laboratorio de la institución sin ser autorizadas.

***Palabras claves**: sistema de seguridad, videovigilancia, grabación, control de acceso, contraseña, vulnerabilidad.*

ABSTRACT

This project called Automated Security System Video Surveillance with Arduino focuses on maintaining security in the educational institution with the implementation of monitoring cameras and entry control of computer lab Education Unit “Luxemburgo”.

Through the security cameras and the DVR located in a safe place away from the vulnerable zone, it will guarantee the video recording about what happens in the laboratory and its around.

Access control is a device capable of allowing access only to people who enter the password correctly and thus prevent outsiders from entering the laboratory of the institution without being authorized.

***Keywords:** security system, video surveillance, recording, access control, password vulnerability.*

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. Introducción

La Unidad Educativa Luxemburgo empieza sus labores en 1989 como Colegio Fiscal "Luxemburgo" y su anterior nombre era Carmen Calisto Ponce. Dicha institución realizaba sus actividades en la casa comunal de Carapungo y también en casas abandonadas del sector. Los alumnos llevaron bloques y tablas para improvisar pupitres.

En 1992 se realiza trámites con el banco "EBPODC" para que trabajara el ciclo básico hasta décimo año. Luego de ser admitido el proyecto se crea La RED Q5, la cual fue edificada en su mayoría por los alumnos y padres de familia. Se efectúa los trámites en el magisterio y crean la jornada vespertina en 1997. Cuenta con un distinguido grupo de maestros quienes dirigen sus actividades, imparten sus conocimientos y forman moralmente a sus estudiantes para que en su futuro se conviertan en profesionales líderes del cambio para el bien de la sociedad.

La Unidad Educativa “Luxemburgo” se encuentra ubicada en el sector de Carapungo en la calle Rumiñahui Oe11-251 e Isidro Ayora en la parroquia Calderón. En la actualidad la escuela posee dos laboratorios de computación que están dotados de equipos de última tecnología como proyector y computadoras donde se transmiten por medio de las TIC´s (Tecnologías de la Información y Comunicación), conocimientos de informática importantes en el aprendizaje de los estudiantes.

El bloque uno a pesar de tener en su laboratorio un número importante de computadoras y otras herramientas de las TIC´s, no posee un método de seguridad conforme a la necesidad del establecimiento educativo; debido al sector donde se encuentra ubicado, queda vulnerable de robos y cualquier acto ilícito que afecte al progreso de la institución, especialmente en las noches y fines de semana, donde un solo agente de seguridad no garantiza el cuidado de las instalaciones de esta institución.

1.1. Problema investigado

La unidad educativa “Luxemburgo” dispone de equipos de computación y herramientas de TIC´s que se usa para el aprendizaje de los estudiantes. Sin embargo el laboratorio de computación del bloque uno no cuenta con la seguridad conveniente e indispensable para salvaguardar los mismos. A pesar de las gestiones para

conseguir un número necesario de herramientas de TIC´s, el centro educativo no pudo adquirir estos equipos de seguridad, debido a su costo elevado y por motivo de su bajo presupuesto asignado a sistemas de seguridad para la institución.

1.2. Problema principal

No existe un sistema de seguridad automatizado con videovigilancia en la Unidad Educativa “Luxemburgo”, por lo tanto se encuentran en peligro de hurto los equipos de computación y herramientas de las TIC´s, que se localizan en el laboratorio de computación del bloque uno.

1.3. Problemas secundarios

- La Unidad Educativa Luxemburgo no posee un sistema adecuado para custodiar los equipos del laboratorio de computación del bloque uno.
- No hay un sistema adecuado que reúna las características necesarias para la automatización de la seguridad en el laboratorio.
- No existe un sistema en el establecimiento educativo que permita conectarse al internet para controlar la seguridad remotamente y mediante clave.
- La institución no consta de un sistema de seguridad automatizado para monitorear constantemente el laboratorio de computación y controlar el acceso al mismo remotamente y mediante contraseña.

1.4. Justificación

Este sistema de seguridad automatizado será apremiante para aplicar cada uno de los conocimientos adquiridos en la carrera de electrónica y telecomunicaciones y obtener experiencias de situaciones relacionadas a la investigación de este campo. Estos conocimientos serán implementados en el laboratorio de computación del bloque uno, de la institución educativa mencionada con anterioridad; con lo que se solucionará la falta de vigilancia en el lugar y un control de acceso Arduino que permitirá tener mayor control para el ingreso del laboratorio.

Implementado el sistema de seguridad automatizado de videovigilancia con Arduino, los docentes encargados de administrar el laboratorio, tendrán mejor control del ingreso y mantendrán vigilado el laboratorio y sus alrededores.

La utilización de nuevas tecnologías en el diseño e implementación son: Android que permitirá una interacción en tiempo real con las cámaras que cubren los puntos ciegos del lugar y se podrá observar desde cualquier dispositivo móvil o fijo que posea acceso a internet; y Arduino, dicha plataforma manejará el ingreso mediante una cerradura electromagnética controlada por clave y remotamente.

1.5. Objetivos

1.5.1. Objetivo general.

Implementar un sistema de seguridad de videovigilancia con Arduino en el laboratorio del bloque uno de la unidad educativa “Luxemburgo” ubicada en el Sector Carapungo perteneciente a la parroquia Calderón.

1.5.2. Objetivos específicos.

- Estudiar los diferentes sistemas de seguridad que se pueden implementar en la Unidad Educativa Luxemburgo.
- Analizar el sistema adecuado que reúna las características necesarias para la automatización de la seguridad en el laboratorio.
- Diseñar un sistema de seguridad que sea compatible en la red de internet con las cámaras de seguridad y un control de acceso Arduino.
- Implementar un sistema de seguridad automatizado para el monitoreo constante por medio de grabaciones respaldadas en un DVR y controlar el acceso remotamente por Internet y mediante contraseña.

2. Fundamentación Teórica

La Ley de Seguridad Pública y del Estado en el artículo 23, establece que “La seguridad ciudadana es una política de Estado destinada a fortalecer y modernizar los mecanismos necesarios para garantizar los derechos humanos, en especial el derecho a una vida libre de violencia y criminalidad” (Unidad de Planificación del Ministerio Coordinador de Seguridad, 2015).

El entorno de las personas y algunos sucesos acontecidos a través de la historia marca un antecedente de debilidad e incertidumbre. Por tal motivo el hombre construye continuamente herramientas y dispositivos aptos para reducir el peligro al que se compromete. Al pasar de los años, estos dispositivos de seguridad se perfeccionaron y mecanizaron hasta lograr efectivos métodos, por lo tanto se logra un alto desempeño y confianza de los mismos.

Los sistemas de videovigilancia son muy utilizados en la sociedad con fines de garantizar la seguridad de los bienes y las personas en diferentes ámbitos. Son instrumentos ventajosos al momento de detectar posibles amenazas, persuasión de delincuentes y busca evitar robos, agresiones y vandalismo. De ésta forma, el uso de sistemas de seguridad en tiempo real está desarrollándose a pasos agigantados y se debe conocer cómo utilizar toda la tecnología disponible adaptándola a las necesidades para brindar servicios de seguridad óptimos y eficaces (Rengel Rivera & Jimbo Jérez, 2015).

Para el esquema e implementación del sistema de seguridad automatizado de videovigilancia con Arduino en el laboratorio de computación del bloque uno de la unidad educativa “Luxemburgo” ubicada en el Sector de Carapungo perteneciente a la parroquia de Calderón cantón Quito. Es indispensable contar con varios conceptos y aspectos básicos. Los dispositivos electrónicos utilizados tanto para hardware y software se emplearán para configurar el sistema de seguridad y realizar las pruebas respectivas que garantizarán el correcto funcionamiento del sistema tanto de la videovigilancia como el control de acceso, ya que es un mecanismo importante para la seguridad de la institución educativa.

2.1. Generalidades de los sistemas de seguridad

Etimológicamente, el término seguridad se deriva del latín SECURITAS, dicha palabra nace del verbo SECURUS que significa “sin temor”. Donde las personas

pueden ser capaces de sentir miedo. La seguridad mantiene una analogía continua con las personas y también con los bienes materiales, con estas circunstancias se puede consumar que el período de ausencia de miedo o seguridad es la incorporación de operaciones orientadas a la protección, defensa y preservación de las personas y el medio que las rodea frente a circunstancias externas que violenten contra su integridad (Cevallos M., 2011)**.**

Por lo tanto, el ser humano vio la necesidad de crear diferentes métodos para reducir el riesgo de la inseguridad que vive las tres cuartas partes de la población mundial. Efectivamente, la delincuencia perceptible disminuye en medida que se garantice la igualdad social de todas las personas, o por lo menos que consten medidas orientadas a este sentido, mientras se propenda una sociedad más justa donde reinen los derechos y la paz. De igual manera, las diferencias sociales en los sectores urbanos (estratos con ingresos asimétricos y un volumen considerable de grupos de personas con necesidades básicas insatisfechas) se asocian diferentemente y, con ella, incrementan los índices de delincuencia. A consecuencia de este acontecimiento y en vista que la tecnología avanza se crean sistemas tecnológicos que puedan, en gran parte, contrarrestar estos índices de delincuencia y ofrecer seguridad de mejor calidad para las personas.

2.2. Sistema de videovigilancia CCTV

Un CCTV (Circuito Cerrado de Televisión), es un sistema de videovigilancia planteada para vigilar local y/o remotamente una variedad de lugares y actividades. La información es captada por una o más cámaras que pueden ser analógicas e IP's. Se menciona circuito cerrado, porque todos sus elementos están enlazados, todo lo contrario que ocurre con el sistema de difusión. Adicionalmente, en oposición de la televisión convencional, este sistema es limitado para un determinado número de espectadores (García Mata, 2011).

Sin importar los mecanismos que se utilicen para esquematizar y elaborar un sistema de seguridad CCTV, constan parámetros que se toma en cuenta en el instante de elegir el sistema a continuación se describe los siguientes:

2.2.1. Ambientes interiores y exteriores.

Se refieren a las cámaras del sistema que se utilizarán para custodiar ambientes interiores y exteriores de acuerdo a la estructura física y los materiales, de

los cuales se fabricaron las cámaras. Para ambientes hóstiles (humedad, polución, exposición al sol y condiciones climáticas extremas) corresponden las cámaras fabricadas con carcasas metálicas y de forma más robusta. Las interiores se elaboran en plástico y su diseño es más afable (Macroquil, 2015).

2.2.2. Cobertura.

Para cada zona es preciso establecer el número de áreas de interés, de las cuales se requieren cubrir y definir si se localizan respectivamente cerca unas de otras o si están muy separadas. El área es lo que determinará el tipo y número de cámaras necesarias (Macroquil, 2015).

2.2.3. Funcionalidades de Día/Noche.

La mayoría de ambientes o entornos delimitan la utilización de luz artificial, por lo cual hacen que las cámaras de infrarrojos (IR) sean especialmente rentables. Éstas manejan un mecanismo que se llama IR Cut Filter, usual en las hojas de especificaciones de las cámaras día noche. La función específica es remover el filtro infrarrojo usado básicamente por las cámaras de color en la noche o en circunstancias de baja intensidad de luz en el ambiente. Por este motivo las cámaras día noche son preferibles en ambientes de baja iluminación. Pero existe un mecanismo aún más sofisticado de las que poseen las cámaras de día noche, y son las cámaras IR. Las cámaras perceptibles a infrarrojos, que logran usar luz infrarrojo visible (Macroquil, 2015).

Estas cámaras poseen un iluminador de infrarrojos que se activa a sensar la ausencia de luz. El alcance que tiene el IR en la mayoría de cámaras es de 15 mts, a diferencia de las HD que tienen un alcance de 50 mts y las PTZ HD que poseen un alcance de hasta 120 mts. Se pueden usar en zonas residenciales, puesto que en la noche, no se incomoda a los habitantes con la utilización de lámparas u otras fuentes de iluminación (Universidad de Zaragoza, 2006).

2.2.3.1. Percepción de la luz.

La luz es una radiación que se propaga en el vacío en forma de ondas electromagnéticas. No obstante, el ojo humano logra observar sólo una parte (entre longitudes de onda de ~400-700 nm). Por debajo del color azul se puede percibir,

correspondiente a la luz ultravioleta y por encima del rojo se encuentra la luz infrarroja. En la figura 1 se observa los tipos de luz visible y no visible con las longitudes de onda que poseen.

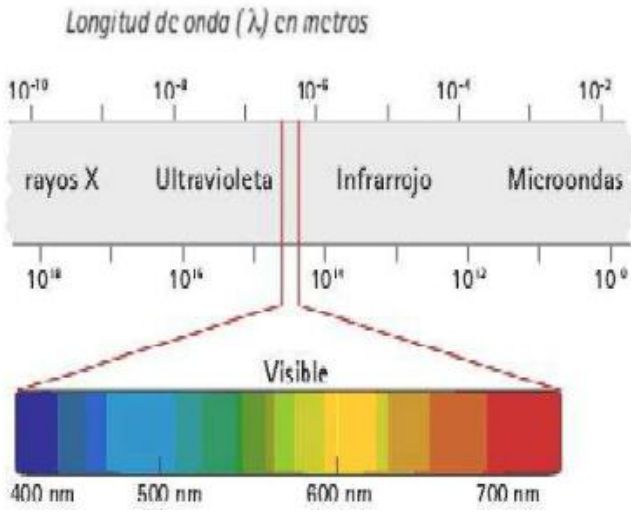


Figura 1. Descripcción de la luz visible y no visible por el ojo humano y la longitud de onda característica.
Fuente: (Universidad de Zaragoza, 2006).

La luz infrarroja es producida por todos los objetos vivos o inertes. Los objetos que desprenden más calor, reflejan fondos más fríos (personas, animales). Por lo tanto el ojo humano no puede percibir todos los colores, solo fondos blancos, negros y matices de gris (Universidad de Zaragoza, 2006).

2.2.4. **Disponibilidad de presupuesto**.

El presupuesto, es muy importante al elegir el sistema CCTV adecuado para la implementación. Al momento la institución no cuenta con un respaldo económico para adquirir estos sistemas. Por lo tanto se aportará con un presupuesto de $ 380 para implementar este sistema (incluye sólo sistema fuera del cableado estructurado y la instalación). Con la descripción de aporte se puede adquirir sistemas con cámaras analógicas conectadas a un DVR donde se almacenen los videos. Las cámaras IP son las más adecuadas en estos sistemas, sin embargo su costo es muy elevado para adquirirlas. Para contrarrestar esta situación se considera adquirir un sistema que posea un DVR con puerto Ethernet, si su requerimiento es conectarse al internet (Villegas, 2012).

2.2.5. Gama.

La gama baja, media y alta es un aspecto también muy importante en las aplicaciones que se utilice. Las cámaras CCTV de gama baja son muy utilizadas para control de tránsito donde solo es necesario verificar por donde recorre el sujeto con su automóvil. Las cámaras de gama media son muy utilizadas para la videovigilancia del hogar, con la necesidad de ver que ingresa al hogar y que actividad realizan. En cambio las cámaras de gama alta son las más demandadas en el mercado ya que su uso principal es de reconocimiento, por tal motivo, la aplicación se la realiza en accesos, cajas y manejo de valores. A continuación la tabla 1, refleja es estudio de las marcas de sistemas CCTV con gama baja, media y alta y sus aplicaciones (Telefonía Total, 2014).

Tabla 1. Estudio de las marcas de sistemas CCTV por gama y sus aplicaciones.

Gama	Rango de Líneas de televisión(TVL)	Marca	Aplicaciones
Baja	420 - 480	SONY HIKVISION SHARP APOSONIC C301 ZTV	Videovigilancia en sitios de desarrollo deportivo, control de tráfico vehicular, sala de reuniones. Sala de recepciones, funerales y escaleras de emergencia.
Media	500 – 600	HIKVISION SONY HECKER	Oficinas, Call Center, bodegas, hogares, transporte de pasajeros.
Alta	700 - 1000	HIKVISION LG SONY ZMODO ISMART ASDK LONGSE	Centros comerciales, bancos, cooperativas, instituciones del sector público y privado. Custodia de valores (vehículos).

Fuente: (Videovigilancia.com, 2006).

Al hablar de estos parámetros, se generan los requerimientos de información que pueden proporcionar los sistemas de CCTV. Por lo tanto, surgen esta pregunta, ¿Qué información necesita que los componentes visualicen? Existen tres respuestas posibles:

• **Detección** – determina la existencia de alguna acción en el área de vigilancia.

• **Reconocimiento** – estipula puntualmente, ¿qué ocurre en el área de monitoreo?

• **Identificación** – establece quién está implicado en la acción captada por las cámaras.

En la figura 2, se observa y diferencia los casos descritos anteriormente

Figura 2. Fines de un sistema de CCTV.
Fuente: (Cumbajín Alférez, 2012).

2.2.6. Estudios de los sistemas CCTV

Hay muchas clases de sistemas CCTV que se manejan para implementar la seguridad en cada sitio que lo amerite. Para elegir el sistema CCTV adecuado, se debe realizar una serie de estudios según las necesidades y el ambiente. Las cámaras de seguridad en las instituciones educativas es una gran herramienta, tanto para las autoridades como para los padres.

Además ayudan a vigilar la seguridad en los exteriores de dichos lugares para impedir y controlar las malversaciones e intimidaciones por parte de personas extrañas a la institución. Contar con cámaras de vigilancia ayuda a realizar una evacuación en caso de emergencia, al momento que el personal de seguridad de las instituciones

esté dotado con sistemas de cámaras, puede ver en tiempo real lo que sucede y tomar acciones rápidas para evacuar a los alumnos, profesores y personal al momento de emergencias referentes con incendios u otras condiciones latentemente peligrosas.

Para instalar un sistema de cámaras CCTV se debe considerar la eficacia de la imagen de la cámaras (se mide en TVL: *Televisión Line*) y el sistema de protección para la encandilación de la imagen cuando se refleja la luz del sol, la funcionalidad del DVR (*Digital Video Recorder*: Grabador de video digital) para administrar el sistema con el control de alarmas y demás. También se considera la ubicación de las cámaras si son interiores o exteriores, de esto depende su fabricación para soportar ambientes hostiles. Al momento de considerar todos los aspectos, a continuación se explican algunos sistemas CCTV que se pueden utilizar.

2.2.6.1. Sistema CCTV analógico con la utilización de un VCR.

Los sistemas CCTV formados por cámaras analógicas con salidas coaxiales conectadas a un VCR (Video Cassette Recorder: Grabador de video cassette) donde se procesan los videos y se almacenan en un casete de cinta. Eran muy usados en la antigüedad, en vista que el casete de VetaMax era el dispositivo del almacenamiento más utilizado en esos tiempos, antes que aparecieran los CD y se utilizaran con mayor frecuencia los Disco Duros que su finalidad era el almacenamiento en los ordenadores. A continuación en la figura 3, se observa un esquema de conexión del sistema CCTV con un VCR (Rengel Rivera & Jimbo Jérez, 2015).

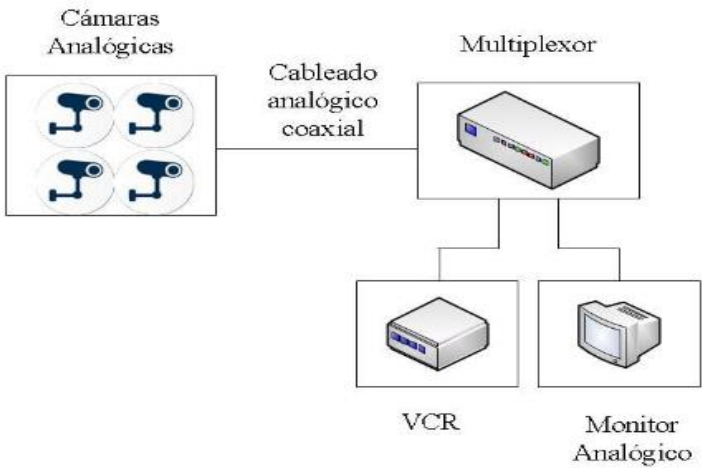


Figura 3. Esquema de un sistema CCTV analógico con la utilización de un VCR.
Fuente: (Rengel Rivera & Jimbo Jérez, 2015).

2.2.6.2. Sistema de CCTV analógico con la utilización de un DVR.

Este sistema CCTV conformado todavía por cámaras analógicas ya contaba con un DVR (Digital Video Recorder: Grabador de video digital) para el procesamiento y almacenamiento de los videos. La comunicación de las cámaras es analógico, sin embargo, ya no se utiliza los casetes de VetaMax para el almacenamiento. Para la grabación de los videos se utiliza un Disco Duro. Al aparecer este sistema, la evolución del almacenamiento se hizo presente con el aumento de la capacidad de los Discos Duro y los fines de utilización. Una de las ventajas más importantes es la calidad de imagen constante. Por lo tanto el DVR utilizaba un Disco Duro a partir de los 120 MB. A continuación se observa en la figura 4, el esquema de conexión de un sistema CCTV con un DVR (Rengel Rivera & Jimbo Jérez, 2015).

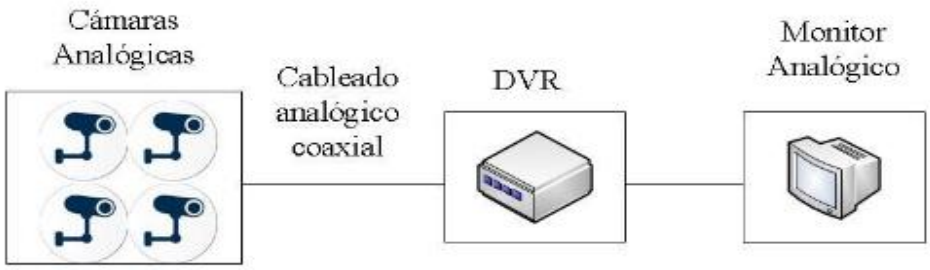


Figura 4. Esquema de conexión de un sistema CCTV con el uso de un DVR.
Fuente: (Rengel Rivera & Jimbo Jérez, 2015).

2.2.6.3. Sistema CCTV analógico con la utilización de un DVR de red.

Este sistema tiene una peculiaridad en su funcionamiento, al momento de utilizar un DVR de red. En primera instancia, sigue desarrollándose como un sistema analógico, ya que, la conexión de las cámaras con el DVR es por cable coaxial. Sin embargo, el DVR tiene una función adicional, la cual usa un puerto de red (Ethernet) para conectarse al internet y ver los videos captados por las cámaras en tiempo real, por medio de una aplicación, ya sea de escritorio o una móvil. El DVR IP añade las siguientes ventajas: Monitoreo y funcionamiento remoto del sistema. En la figura 5 se observa, el sistema CCTV conformado por las cámaras y el DVR conectado a internet (Rengel Rivera & Jimbo Jérez, 2015).

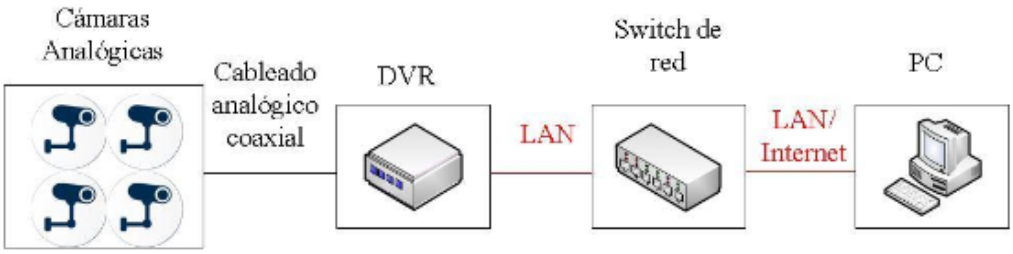


Figura 5. Esquema de conexión del sistema CCTV analógico que utiliza un DVR de red.

Fuente: (Rengel Rivera & Jimbo Jérez, 2015).

2.2.6.4. Sistema de video IP que utiliza servidores de video.

Este sistema todavía utiliza una conexión de video analógico de las cámaras, pero incorpora un servidor de video con las características para conectarse por medio de cable coaxial a las cámaras. También se incorpora en el sistema un Switch de red que proporciona conexión del servidor con un computador, el cual posee el software que administra el sistema. El sistema es escalable, por lo tanto, se consigue incrementar el número de elementos del sistema (computadores de administración, cámaras y servidores de video). El video se graba remotamente y si se logra utilizar cámaras IP el sistema ampliará la vigilancia. Este sistema se conoce como hibrido ya que combina el funcionamiento de cámaras analógicas e IP conectadas al servidor (si es que se ejecuta esa opción). En la figura 6, se observa el esquema de conexión del sistema de video IP con el servidor y el computador administrador del mismo (Rengel Rivera & Jimbo Jérez, 2015).

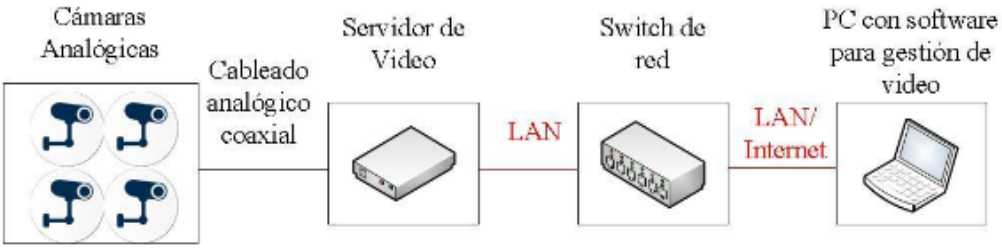


Figura 6. Esquema de conexión del sistema de video IP que utiliza seridores de video.

Fuente: (Rengel Rivera & Jimbo Jérez, 2015).

2.2.6.5. Sistema de video IP que utiliza cámaras IP.

Como se mencionó anteriormente se puede agregar cámaras IP en un sistema de video IP por la facilidad de conexión a la red y la utilización del mismo hardware

para la interconexión de los elementos dentro del sistema. Es decir, en este sistema ya no se necesita un dispositivo acoplador de conectores coaxiales a el servidor de video, al contrario, basta con utilizar un Switch con los puertos suficientes para conectar las cámaras necesarias del sistema. Una ventaja es que permite la digitalización y compresión del video al conectarse directamente a la red, y ya no pasaría por una etapa de conversión analógico-digital. Mantiene el mismo principio del sistema anterior cuenta con un ordenador que posee un software para administrar el sistema (Rengel Rivera & Jimbo Jérez, 2015).

Algunas características que se presentan en el sistema es que, utilizan cámaras de alta resolución, la calidad de la imagen se mantiene constante, la alimentación eléctrica es a través del mismo cable de Ethernet (PoE). Se incorpora también la funcionalidad inalámbrica, si existieran cámaras WiFi. Con este funcionamiento el sistema se flexibiliza y posee su escalabilidad completa. En la figura 7 se muestra el esquema de conexión del sistema de video IP en conjunto con las cámaras IP y el Switch (Rengel Rivera & Jimbo Jérez, 2015).

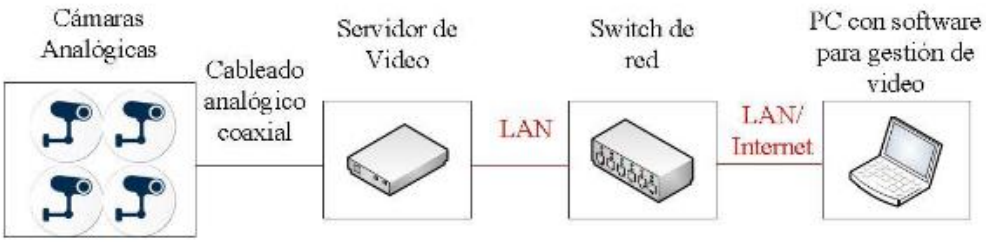


Figura 7. Esquema de conexión del sistema de video IP que utiliza cámaras IP. Fuente: (Rengel Rivera & Jimbo Jérez, 2015).

2.2.7. Estudio de marcas de sistemas CCTV.

Para la implementación del sistema CCTV en la Unidad Educativa Luxemburgo y en base a las anteriores descripciones de los sistemas existentes, se considera el circuito cerrado de televisión (CCTV) analógico que utiliza un DVR de red. En la actualidad la tendencia son los sistemas de video IP que utilizan servidores de video y cámaras IP. Sin embargo está implementación considera un costo muy elevado de inversión, ya que los servidores y las cámaras IP son excesivamente caras en comparación con el presupuesto que se cuenta para este proyecto.

Al utilizar cámaras analógicas se reduce el costo del sistema y se opta por la utilización de un DVR que realice el mecanismo de digitalización y almacenamiento de

video por medio de un Disco Duro. Además al realizar el estudio de marcas, se encuentra varias que poseen la opción de reflejar el video en tiempo real en un Smartphone u ordenador de escritorio por medio de su respectiva aplicación. Claro está que esta función se llevará a cabo, sólo cuando se conecte el sistema a un servicio de internet con IP pública. Si la institución contiene una red privada, sólo se podrá utilizar esta opción en un ordenador de escritorio que posea el software de visualización, ya que la red privada no permite el acceso remoto de un dispositivo conectado desde exterior de la red. Una desventaja de este sistema es el déficit en escalabilidad, puesto que si el DVR posee 4 canales de video analógico ya no se puede conectar más de 4 cámaras al sistema, esto limita el incremento de la vigilancia. Sin embargo, si con 4 cámaras se cubre los puntos ciegos del área a vigilar se cumpliría con el objetivo del sistema y los demás canales coaxiales estarían de más, si en el caso los hubiera.

A continuación se mostrará la investigación de las diferentes marcas de sistemas CCTV consideradas para este proyecto con sus respectivas funciones que apoyarán el desarrollo normal del sistema.

2.2.7.1. *Kit HIKVISION TURBO HD.*

Este sistema se recomienda para implementación en instituciones educativas por su mejor resolución y método convencional de conexión. El DVR de este sistema posee las siguientes características:

- Tiene una resolución de Grabación HD 720Pixeles/30fps (fotogramas por segundo)
- Cuenta con una compresión de video: H.264
- Compresión de audio: G.711U.
- Salidas de video VGA y HDMI
- Posee 2 entradas USB para conectar los periféricos de entrada (mouse y teclado).
- Posee 1 RS-485 para PTZ, que sirve también para conectarse a la red de internet.
- Contiene 4 entradas de video analógico (BNC).
- Contiene un mando inalámbrico (control remoto).
- Posee una comunicación TC/IP 10/100Mbps, para la comunicación con la red de internet para una velocidad de transmisión máximo de 100Mbps (TechResources, 2015).

Las cámaras que posee el sistema tienen las siguientes características:

- 1 cámara Domo Interior HD 720P: Salida de video HD, DNR (Digital Noise Reduction: Reducción digital de Ruido), Smart IR para visión nocturna, por lo tanto el alcance del infrarrojo (IR) es de 20 mtrs.
- 1 cámara Tubo Exterior HD 720P: con las mismas características de la de Domo, la única diferencia es que cuenta con un factor de protección de la intemperie de IP66.
- 2 cámaras Indoor / Outdoor HD 720P: con las mismas caracteristicas de la cámara de Tubo Exterior.
- Todas las cámaras manejar el sistema NTSC (*National Television System Committee*: Comisión nacional de sistemas de televisión): 1280(H) x 720(V).
- Poseen conectores tipo baluns (terminales de conversión BNC a RJ45) para el cambio de medio de transmisión de coaxial a UTP (*Unshielded Twister Pair*: Par trenzado sin apantallar) y viceversa (TechResources, 2015).

Este sistema se ajusta a la necesidad de la institución educativa, pero no al presupuesto previsto, ya que al sumar el precio del sistema y el Disco Duro de 320 Gb reúnen un precio de $ 450. Precio que al comparar con el presupuesto asignado se sobrepasa, por lo tanto no se considera utilizarlo.

2.2.7.2. Kit CCTV Zmodo.

El sistema mencionado es un muy buen aporte a la seguridad de las instituciones. Las cámaras consideradas en este sistema son:

- 4 cámaras de tipo Tubo Exteriores de 600 TVL.
- Poseen 24 LED's IR (*infrared*: Infrarrojo) con un alcance hasta los 30 metros de distancia.
- Considera estar en una gama alta, sin embargo su capacidad de fidelidad de colores mostrados es de nivel medio.
- Posee el mecanismo de protección de la intemperie IP66 (TechResources, 2015).

El DVR del sistema es:

- De 4 canales de video (conectores BNC; *Bayonet Neill-Concelman*: cierre en bayoneta)
- 4 canales de audio

- Un puerto HDMI (*High Definition MultiMedia Interface*: Interfaz multimedia de alta definición), un VGA (*Video Graphics Adapter*: adaptador gráfico de video) y un RCA (antigua compañía de electrónica estadounidense *Radio Corporation of America*).
- Posee 2 puertos USB (*Universal Serial Bus:* Bus universal en serie) para conectar los dispositivos de entrada y salida (teclado y mouse).
- Además posee un puerto Ethernet (RJ45) con el cual se enlaza a la red con o sin el suministro de una IP (*Internet Protocol*: Protocolo de internet) estática.
- Incluye un Disco Duro de 320 GB Para grabar se debe conectar un disco duro de acuerdo a la capacidad de grabación del lugar.
- También existe la opción de ver las 4 cámaras simultáneamente (Quads) (TechResources, 2015).

El sistema es adecuado e interesante para la implementación, sin embargo, para esta implementación se consideran sistemas con equipos de gama alta. Por poseer sólo 600 líneas de televisión y considerarse en el rango de gama baja no se tomará en cuenta. Su precio varía entre los $ 300 y $320, si cumple con el presupuesto pero la definición del video rechazó la utilización del mismo.

2.2.7.3. CCTV ISmart.

El sistema ISmart trabaja con una interface muy útil al momento de manejarla. El kit posee un DVR con las siguientes características:

- Salida de video de 720 TVL
- Una compresión de video: H.264 con doble flujo.
- Grabación de 4CIF a 30fps.
- Posee cuatro canales en tiempo real, vista en directo, grabación, reproducción.
- Soporta HDMI, CVBS (*Color, Video, Blanking, & Sync:* Color, Video, Borrado y Sincronismos), salida VGA.
- Detección inteligente de video: MD (Motion Detection), cámara en blanco, pérdida de video.
- Configuración de alarmas, timbre, PTZ (*Pan, Zomm y Tilt*: capacidades de las cámaras automatizadas y grabadoras de vídeo), e-mail, FTP (*File Transfer Protocol*: Protocolo de transferencia de archivos).
- Soporta NTP (*Network Time Protocol*: Protocolo de internet para sincronizar los relojes de los sistemas informáticos), DHCP, DDNS (***D****ynamic* ***D****omain* ***N****ame*

***S**erver*: Servidor de nombre de dominio dinámico), CMS (*Content Management System*: Sistema de gestión de contenidos), navegador web 2.0, P2P (*Peer-to Peer:* Par a par).

- Posee un canal de entrada de audio; un puerto de salida de audio;
- Soporta una conexión a un disco SATA HDD (*Serial Advanced Technology Attachment Hard Disk Drive:* Unidad de disco duro con tecnología avanzada adjunta serial) de hasta 2Tb.
- Posee 2 puertos USB 2.0.
- Tienen un puerto ethernet, con el cual se puede conectar a la red para poder realizar la vigilancia desde el celular o computadora de escritorio.
- Posee conexión a la aplicación IMSeye para Smartphone y la aplicación IMS200 para computadoras portátiles y de escritorio. El programa viene incorporado para configurar alarmas y notificaciones en tiempo real, sin embargo, no se puede acceder a las grabaciones que se encuentran almacenadas en el disco duro del DVR (Novicompu, 2014).

Las 4 cámaras son de la marca ISmart modelo C1030DP7 propias del sistema y las características son las siguientes:

- Tienen una resolución de 700 TVL
- Consta también de un sensor de imagen CMOS (*complementary metal-oxide-semiconductor*: semiconductor complementario de óxido metálico) LED 36pcs IR para visión nocturna. Mínimo de iluminación: OLux (distribución de la luz de forma homogénea, simétrica, precisa y eficiente) (IR encendido).
- Posee un lente 3.6 /6mm.
- Es resistente al agua: IP66 (acto de entrada: capacidad para impedir que la cámaras dejen ingresar objetos extraños; el primer digito 6, calificación de sólidos; el segundo dígito 6, calificación de líquidos) para uso interior y exterior.
- Además posee una fuente de poder que distribuye la energía hacia las diferentes cámaras y DVR con su respectivo voltaje de funcionamiento, de tal manera que no exista la conexión independiente de alimentación de cada dispositivo del sistema (Novicompu, 2014).

Esta marca se convierte en la más recomendable para la implementación del sistema, porque primero cuenta con una resolución óptima para el ambiente que se desea vigilar aunque no sea HD, pero tiene una buena resolución. Otra de las

opciones que califican al sistema como óptimo, es el precio de $ 370, ya incluido el Disco Duro del 320 Gb, por lo tanto se ajusta al presupuesto asignado al video vigilancia.

2.2.7.4. Kit CCTV Longse.

La marca cuenta con un DVR y 4 cámaras analógicas. Las características del DVR se detallan a continuación:

- Posee 4 canales Stand Alone (Todo en uno), en el frente con botones.
- 4 entradas de audio, 1 entrada bidireccional.
- 1 salida de audio.
- 4 entradas de alarma y 1 salida de alarma.
- Salida de video VGA y coaxial.
- Salida de audio y video a través de puerto HDMI.
- Grabación de 4 CIF a 25fps.
- Soporta un Disco Duro SATA de 4 Tb
- Soporta hasta 128 conexiones simultáneas (Impomax, 2015).

Las cámaras que trabajan en conjunto con el sistema cuentan con las siguientes características:

- Son 4 cámaras tipo Domo 600 TVL.
- Posee un sensor de imagen DIS 1/3”
- Trabaja con la señal en sistema PAL/NTSC.
- Sensor LED IR para visión nocturna con un alcance de 25 mtrs.
- Posee lentes de 3,6 mm con un angulo de visualización de 68,4° con un montaje M12.
- Una salida de video de 1Vp.p comuesta (75Ω/conexión BNC).
- Nivel de S/N más que 60 dB.
- Condiciones de temperatura operables del -40°C – 60°C.
- Fuente de poder de 12VCD.
- Protección a la intemperie IP66.
- Peso de cada cámara es de 400g.
- Posee la función de zoom digital Pan: 0 - 360°, Tilt: 0 - 75°, Rotation: 0 - 360° (Impomax, 2015).

Esta marca posee algunas características que superan a las demás tales como, la incorporación del zoom digital, las 4 cámaras son tipo Domo, soporta hasta 4Tb de Disco Duro, pero el problema es que las líneas de televisión corresponden al rango de gama media. Otro parámetro que deja afuera de consideración para la implementación del proyecto es el precio de $ 530,95 incluido un Disco Duro de 320 Gb. Precio que supera al presupuesto asignado a la implementación del sistema, por lo tanto, no se puede adquirir.

2.2.8. Componentes de un sistema de videovigilancia.

Un sistema de video vigilancia CCTV está formado por un gran número de elementos, desde una cámara que capture imágenes de un lugar determinado, y que se puede visualizar en un monitor que esté conectado al sistema, hasta complejos sistemas de video vigilancia para fábricas donde necesiten monitorear cada departamento a fin de salvaguardar la integridad de sus trabajadores. En esta instancia se elabora una descripción de los principales elementos que interceden en un sistema de video vigilancia:

2.2.8.1. Cámaras.

Es el componente del sistema de CCTV cuya función es la captura de imágenes y video que son transmitidas en forma de señales a un dispositivo con la capacidad de convertirlas en señales digitales (DVR) y a su vez puede administrarlas en diferentes aspectos como: enviarlas a un dispositivo de almacenamiento y trasmitirlos en un dispositivo para visualizar la imagen o video. Existen muchos tipos de cámaras en el ámbito comercial cada una con diferentes aplicaciones, especificaciones y funciones adicionales que las hacen más interesantes, como se observa en la Figura 8. En esta instancia se detallan algunas características que convierten a las cámaras propicias para el uso de vigilancia en algunos aspectos (Cruz, 2013).

Figura 8. Partes de una cámara de CCTV.
Fuente: (PC Componentes, 2015).

2.2.8.1.1. Características.

- **Alimentación:** 220 VCA, 24 VCA y/o 12 VCC.
- **Tipo de sensor:** CCD o CMOS y su respuesta espectral (color, blanco y negro y/o infrarrojo). El sensor de imagen de la cámara realiza el proceso de transformación de la luz en señales eléctricas. Para llevar a cabo la elaboración de una cámara se debe considera dos tipos de sensores: CCD (Dispositivo de acoplamiento de carga) y CMOS (Semiconductor de óxido metálico complementario). Los sensores CCD se elaboran con la implementación de una tecnología perfeccionada concretamente para las manufacturas de cámaras, en cambio, los sensores CMOS se apoyan en una tecnología estándar considerablemente usada en los chips de memoria (dentro de una PC) (Universidad de Zaragoza, 2006).
    - Tamaño del sensor: 1/2”, 1/3”,1/2”, 2/3”, 1”.
- Resolución: Es un aspecto de calidad de los cuales se reproducen los detalles más minuciosos del ambiente. Mientras la cantidad de pixeles del CCD sea mayor, la resolución de la cámara será más óptima. Las cámaras estándar poseen 380 líneas de resolución (TVL), en cambio, las cámaras profesionales van de las 420 a las 550 TVL. En la mayoría de las aplicaciones de CCTV se usan cámaras de resolución estándar (420TVL) (Universidad de Zaragoza, 2006).
- **Audio:** para escuchar el sonido del ambiente donde está instalada la cámara. Algunos ambientes lo requerirán, por lo tanto se considera cámaras con micrófono incorporado, o también se podría instalar micrófonos ocultos independientes de la cámara pero conectados al sistema CCTV.

- **Sensibilidad**: se entiende como la capacidad de reproducir imágenes de video en ambientes de baja iluminación. La sensibilidad se calcula en LUX. Las cámaras en blanco y negro comúnmente tienen una sensibilidad de 0,01 LUX. Por lo contrario las cámaras en color poseen una sensibilidad aproximada de 0,1 a 1 LUX (Universidad de Zaragoza, 2006).
- **Iris Electrónico:** es destacado como AES (Automatic Electronic Shutter), maneja de manera automática la luz que ingresa a la cámara. Mientras mayor sea la velocidad de conducción de la luz (varía entre 1/60 y 1/100.000 de segundo) mejor es la compensación de la imagen en esas condiciones (Universidad de Zaragoza, 2006).
- **Compensación de luz trasera**: Para observar un objeto que posee luz detrás del mismo se debe elegir una cámara que posea BLC (Back-Light Compensation: Compensación de luz trasera). Si la cámara se encuentra instalada en el interior de un ambiente debe poseer el BLC, de lo contrario, al momento que una persona ingrese por la puerta o asome por la ventana, la luz detrás se reflejará a la personas como una silueta negra. El trabajo que realiza el BLC es de alguna manera engañar a la cámara para que no registre la luz y poder observar al objeto en las peores condiciones, a través de un oscilador interno. Las cámaras que funcionan con corriente alterna se pueden sincronizar con la frecuencia de red (LLC – line lock control: control de bloqueo de línea). El ajuste del nivel de fase del sincronismo vertical, impide saltos indeseables al momento de la generación del video en vivo, también en la reproducción de la grabación guardada (Universidad de Zaragoza, 2006).
- **Relación Señal /Ruido (S/N - Signal Noise):** Esta relación calcula la inmunidad al ruido eléctrico que genera la fuente de alimentación. Lo normal es 46 dB de acuerdo a las normas de ética profesional (Universidad de Zaragoza, 2006).
- **AGC (Control Automático de Ganancia):** Posee un valor típico de 30dB. Conserva a la salida de la señal de video en un nivel de 1V pico a pico, con una carga de 75ohms.

2.2.8.1.2. Lentes.

De acuerdo a la iluminación del ambiente que se observa, se clasifican en:

- **Lentes de Iris Fijo:** Se usan en el momento que la iluminación es constante, por ejemplo un cuarto iluminado con focos o lámparas.

- **Lentes de Iris Variable Manual**: Se utilizan en ambiente de luz natural o artificial variable, por lo tanto se puede ajustar de acuerdo a las necesidades.
- **Lentes Autoiris:** Estos lentes manejan de forma automática la cantidad de luz que ingresa a la cámara. Mantienen una señal de video constante, es efectivamente superior a la del iris electrónico (AES), por lo cual logra una mayor profundidad del campo. Al observar un ambiente se mantiene la lente en la distancia focal determinada.
- **Lentes Fijas:** Esto ocurre cuando se define la lente adecuada para el área de vigilancia.
- **Lentes Varifocales:** Estos lentes permiten ajustar de forma manual la distancia focal, lo cual admite al instalador cambiar el campo de observancia en presencia del propietario de acuerdo al criterio del mismo. S lo usa en ambientes de campo de visión inseguro o definido en el momento de instalación.
- **Lentes Zoom**: Estos lentes permiten observar imágenes en diferente distancia focal, es decir, objetos cercanos o lejanos. Para realizar esta función se requiere un controlador que accione el motor de zoom cuando lo requiera (Higuera Angarita, 2015).

2.2.8.1.3. Clasificación de las cámaras por tecnología.

Existen amplios tipos de cámaras en el mercado, de acuerdo a la tecnología se fabrican distintos modelos, con varias funciones que las convierten en adecuadas para cada ambiente. Por lo tanto se presentan a continuación las tecnologías utilizadas y sus características.

2.2.8.1.3.1. Cámaras analógicas.

Son dispositivos que reciben la luz a través de un lente con las que logran la imagen. Poseen un obturador y un diafragma que cumplen la función de medir la luz con la dependencia de la sensibilidad del dispositivo. Una vez capturada la imagen es trasmitida en forma de señal de video compuesto analógico contiene lMMa (información de los pixeles) con todas las señales de sincronismo en un mismo cable, lo que hace que la conexión sea simple y barata (Cruz, 2013).

Al momento que la señal llega al DVR por el medio de transmisión asignado, ésta entra a un proceso de conversión de analógico-digital y podrá ser visualizada en algún dispositivo de salida de video (monitor). Todas las cámaras estándar son

analógicas, existen algunas cámaras de alta velocidad y de alta definición que también son analógicas. Las cámaras analógicas no contienen servidor Web, tampoco compresores, no demanda ningún mantenimiento a parte del físico (limpieza de polvo, lubricación de los elementos de sujeción y de traslación, etc.) (Cruz, 2013).

2.2.8.1.3.2. Cámaras IP.

Se puede definir como una cámara que digitaliza y procesa imágenes análogas, las comprime internamente y luego transmite la información del video a través de una conexión TCP/IP (*Transmission Control Protocol / Internet Protocol:* Protocolo de control de transmisión / Protocolo de internet). Una Cámara IP puede acoplar dos clases de sensores, el CMOS y el CCD (*Charge Coupled Device*: Dispositivo de carga acoplada). Suele ser frecuente que se pueda usar un navegador web para observarlas o una aplicación propietaria de la marca. Se configuran con su propia dirección IP de tal manera que son manipuladas virtualmente como cualquier otro medio de su red que logra la conexión tanto alámbrica como Inalámbrica. Estas cámaras demandan mantenimiento y configuración como cualquier dispositivo de red (Cumbajín Alférez, 2012).

2.2.8.1.4. Clasificación por modelo.

En el mercado existen varios modelos de cámaras, según su fabricación funcionalidad y ambiente. En esta instancia se habla de algunos modelos para el uso de sistemas CCTV en ambientes tanto interiores como exteriores, donde exista ausencia de luz o intensidad.

2.2.8.1.4.1. Domo.

Algunas cámaras se integra en el grupo de las PTZ, de hecho algunas domos son PTZ que integran funciones de Panning – Tilt. Existen otra cámaras que solo tienen un ángulo definido de visualización como se muestra en la figura 9. La principal función del Domo es de proveer la protección necesaria del ingreso de agentes exteriores a la cámara. A parte la protección suministra el espacio necesario para que una cámara pueda realizar el giro, ya sea de 180° o 360° (panning) y verticalmente hasta los 180° (Tilt). Existen cámaras de este tipo antivadálicas, el cual contiene una construcción mucho más fuerte de su estructura en el Domo y puede soportar golpes, pero al instalar hay que tomar en cuenta la fijación de la cámara, porque puede no romperse con un golpe, pero puedo desprenderse si no está fijada correctamente (Cruz, 2013).

Figura 9. Cámara tipo minidomo.
Fuente: (Cruz, 2013).

2.2.8.1.4.2. Bala o Tubular.

La cámara tipo bala es recomendable para detectar objetos y actividad en la más completa oscuridad como se observa en la figura 10. Si en el caso contara con tecnología IR adaptativa, esta cámara está facilitada para suministrar un ángulo de iluminación amplio y estrecho, la cual maximiza la calidad de la imagen independientemente de la condiciones del lugar. También añade capacidades como resistencia al vandalismo. La cámara tipo bala es apta para vigilar una variedad de ambientes que solicitan una discreta cobertura nocturna, tales como estacionamiento, las universidades y los parques industriales (Notiseg. S.A. de C.V., 2015).

Figura 10. Cámara tipo bala para exteriores.
Fuente: (Notiseg. S.A. de C.V., 2015).

2.2.8.1.4.3. Cámaras PTZ.

Las cámaras PTZ son cámaras con tres funciones principales de acuerdo a sus siglas Pan-Tilt-Zoom. Pan vigila en un plano horizontal (panning), Tilt vigilancia en un plano vertical y Zoom que permite acercarse o alejarse de forma manual o automática como muestra la figura 11. Estas cámaras son relacionadas con funciones como la ronda de vigilancia, la grabación de rondas, el audio, los puertos de E/S para mecanismos de alarma externos, la función Gatekeeper, el rastreo automático, poseen un sin número de funciones adicionales de acuerdo a las especificaciones del fabricante, tales como, seguimiento por generación de calor, movimiento, etc. Incluye accesorios como software o hardware donde destaca el joystick, para suministrar los movimientos, y los kits de montaje para instalaciones en interiores/exteriores (Axis Comunications, 2015).

Figura 11. Cámara PTZ con tecnología IP.
Fuente: (Axis Comunications, 2015).

2.2.8.1.4.4. Ojo de Pez.

Estas cámaras tienen el aspecto de una tipo domo, con la diferencia que es más pequeña y casi plana como se observa en la figura 12. Tiene un espectacular ángulo de visión de 360°. Posee varias características que se describen a continuación:

- La visualización completa de 360° en ojo de pez, muestra una sola imagen en 360° de todo el espacio vigilado.
- En la visión panorámica, muestra dos imágenes del espacio vigilado en un ángulo de 180°.

- Visualización en ojo de pez + PTZ, esta configuración muestra 4 imágenes simultaneas, la una muestra el espacio completo en 360° y las 3 muestras imágenes en diferentes panoramas como si se manejara 3 cámaras diferentes (Superinventos, 2000).

Figura 12. Cámara de videovigilancia tipo ojo de pez.
Fuente: (Superinventos, 2000).

2.2.8.2. Medios de transmisión utilizados por el sistema CCTV.

Por los ambientes donde se ubicarán los sistemas, los equipos de transmisión y las señales que se va a transmitir, se debe considerar los medios de transmisión más eficientes en el área. El más común, de precio módico y con una calificación buena en seguridad en el ámbito tecnológico es el cobre, pero este varía según las circunstancias ambientales, trayectos entre otras causas.

2.2.8.2.1. Cable coaxial.

El medio guiado más frecuente para transmitir video todavía es el coaxial. La eficacia de la señal de video obedece a la eficacia del cable. Este cable puede contener numerables diferencias entre los tipos. Los tipos RG-11, RG-59, RG-58 y RG-6 se consideran más usuales. En la figura 12 se observa el aspecto físico del RG-58U, que posee una impedancia baja con respecto a los demás tipos de cable.

Tabla 2. Distancias máximas para el uso de cable coaxial.

Tipo de cable	*Impedancia*	*Distancia*
RG-58	*50Ω*	250m
RG-59	75Ω	225m
RG-6	75Ω	400m
RG-11	75Ω	600m

Fuente: (Forouzan, 2007).

En la tabla 2, se exponen los tipos de cable coaxial, sus impedancias y distancias de utilización.

Figura 13. Aspecto físico de un cable coaxial RG-58.
Fuente: (Home: Hangzhou Yingbang Cable Co., Ltd, 2013)

2.2.8.2.2. Cable UTP.

El más común en transmisión de datos es el UTP Cat. 5e por sus diversas ventajas. Estos cables poseen cuatro pares de cobre cubiertos por aislante y trenzados a modo de evitar la diafonía. Estos pares permiten transmitir algunas señales por el propio cable (puede ser corriente, audio, video y datos) (Forouzan, 2007). Se saben usar a distancias mayores a diferencia del coaxial:

- Es más económico
- Es más plegable
- Es de espacio reducido y más estético que el coaxial.
- Para utilizar este cable se requiere de baluns, que constan como pasivos (en distancias cortas) y activos (para distancias más largas).

En la actualidad para la construcción del cableado estructurado de la red LAN (*Local Area Network* = Red de área local) se utiliza el cable UTP CAT6 como muestra la figura 14, en vista de que posee internamente un divisor de pares que ayuda a disminuir la diafonía.

Tabla 3. Categoria del Cable UTP con sus respectivas aplicaciones.

CATEGORÍA	ANCHO DE BANDA	APLICACIONES
Categoría 1	0,4 MHz	Líneas telefónicas y módem de banda ancha.
Categoría 2	4 MHz	Cable para conexión de antiguos terminales como IBM 3270.
Categoría 3	16 MHz	100BASE-T and 100BASE-T4 Ethernet.
Categoría 4	20 MHz	16 Mbit/s Token Ring
Categoría 5	100 MHz	100BASE-TX and 1000BASE-T Ethernet.
Categoría 5e	100 MHz	100BASE-TX and 1000BASE-T Ethernet.
Categoría 6	250 MHz	1000BASE-T Ethernet
Categoría 6a	250 MHz – 500 MHz	10GBASE-T Ethernet (en desarrollo)
Categoría 7	600 MHz	En desarrollo, aún sin aplicaciones.
Categoría 7a	1200 MHz	Para servicios de telefonía, Televisión por cable y Ethernet 1000BASE-T en el mismo cable.

Fuente: (Forouzan, 2007).

La tabla 3 demuestra los anchos de banda que soporta cada categoría y las aplicaciones en las que se usa esta clase de cable.

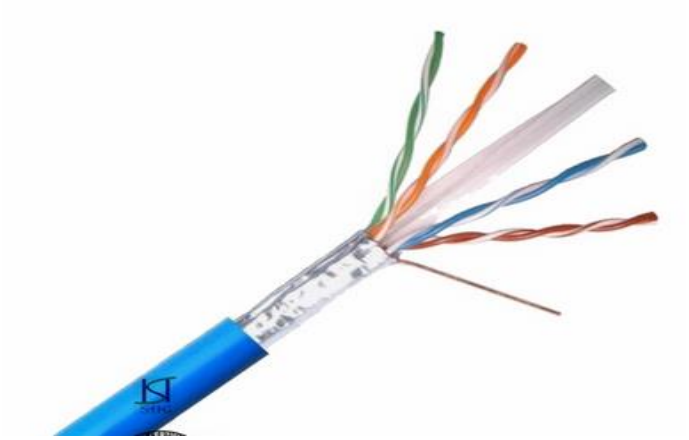


Figura 14. Cable UTP categoría 6 FTP.

Fuente: (Home: Hangzhou Yingbang Cable Co., Ltd, 2013).

2.2.8.2.3. Fibra óptica.

Son filamentos de vidrio (conformados por cristales naturales) o plástico (cristales artificiales), del espesor de un cabello (entre 10 y 300 micrones). Transporta señales digitales a modo de pulsos modulados de luz desde una fuente de luz (LED o láser) hacia un detector de luz (fotodiodo). Esta es una manera segura de transmitir datos mediante impulsos no eléctricos, a diferencia de un cable de cobre que envía señales eléctricas (Forouzan, 2007). Existen varias características que hacen a este medio como el más recomendado para la transmisión:

- Conforme a la atenuación en función de la longitud de onda, ofrece 3 ventanas de operación situadas en 850 nm, 1310 nm y 1550 nm.
- El ancho de banda se limita por la dispersión, por lo tanto, se puede alcanzar anchos de banda muy altos en comparación con los otros medios.
- Baja atenuación por Km, respecto a la tabla 4, se puede observar la atenuación por km de los tipos de fibra óptica más comunes.
- Permite separar repetidores a varias decenas de km.
- Inmunidad frente al ruido.
- Gran capacidad de transmisión.
- Usa señales de potencias muy bajas.
- El motivo que la fibra óptica no se considera mucho en estos circuitos, es el alto costo de la misma y sus equipos de transmisión en el mercado.

Tabla 4. Tipos de fibras más comunes en el mercado con sus respectivas atenuaciones, de acuerdo a las ventanas de operación.

TIPO	REGIÓN DE LONGITUD DE ONDA	VALOR TÍPICO DEL ENLACE
G.655	1530 nm – 1565 nm	0,275 dB/km
	1565 nm - 1625 nm	0,35 dB/km
G.652	1260 nm - 1310 nm	0,5 dB/km
	1530 nm – 1565 nm	0,28 dB/km
	1565 nm – 16XX nm	0,35 dB/Km

Fuente: (International Telecomunications Union, 2010).

Nota: Estos datos son determinados en un valor general de la atenuación en la tabla atributos del cable de tipo G652 y G655 (A, B, C, D) de las normas ITU – T (versión español).

La figura 15 muestra el cable de fibra que consta del núcleo que se encuentra recubierto por una capa de vidrio concéntrica conocida como revestimiento. Luego del revestimiento se encuentra el buffer (cubierta de plástico) que a veces contiene un gel que sirve para crear una capa oscura para que los rayos de luz no se dispersen hacia afuera de la fibra. El cable de fibra óptica también posee un grupo de fibras protectoras que sirven como elementos de tracción. Y el último elemento de protección es la chaqueta que se conforma de un material plástico e incluye una lámina de metal para los cables de fibra óptica canalizados (skynetgroup2005, 2014).

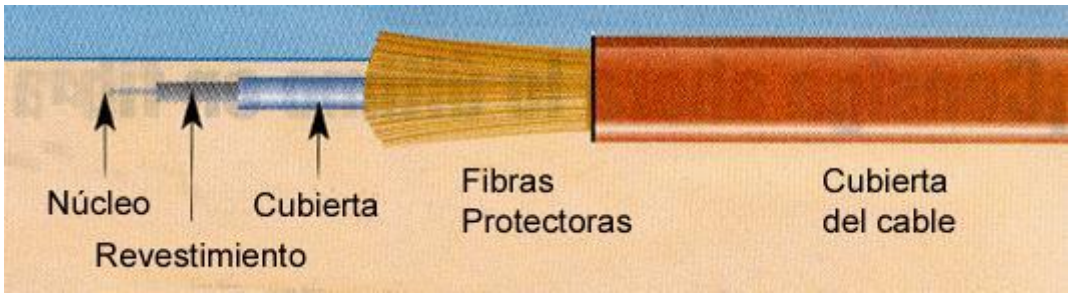


Figura 15. Cable de fibra óptica con sus respectivas partes.
Fuente: (skynetgroup2005, 2014).

2.2.8.2.4. Inalámbrico.

Se encuentran diversos ejemplos de transmisión inalámbrica: el WIFI (mecanismo de conexión de dispositivos electrónicos de forma inalámbrica) y el (WiMax; Worldwide Interoperability for Microwave Access: Interoperabilidad para el acceso a microondas) los más usados. Para un lugar cercano a la red se puede emplear una estándar de WIFI. Este estándar como otras tecnologías inalámbricas puede utilizar varias modulaciones y en la mayoría de equipos terminales estas modulaciones se ajustan de acuerdo a la velocidad que se recibe.

La modulación utiliza una frecuencia de portadora para transmitir información. Según la modulación que se utilice, se trasmiten datos en mayor o menor proporción, es decir, para mayor transmisión de información, mayor potencia en las señales. La tabla 5 visualiza la clase de modulación que se utiliza de acuerdo a la velocidad que se transmita la información. Los equipos actuales poseen la capacidad de ajustar

automáticamente la modulación y la velocidad de transmisión, para obtener la más alta posible y evitar la pérdida de información. Para distancias más amplias se requiere la integración de antenas especiales llamadas WiMax. En este servicio la técnica de modulación y el ajuste automático de la velocidad de transmisión es muy importante para tecnologías móviles, debido a que los usuarios se mueven constantemente y cambian las condiciones de conexión (Ubierna Yuvero, 2013).

Tabla 5. Tipos de modulación que utiliza el sistema de transmisión inalámbrico con su respectiva velocidad de transmisión.

MODULACIÓN	VELOCIDAD DE TRANSMISIÓN
BPSK	15 Mbps
QPSK	45 Mbps
16QAM	90 Mbps
64QAM	150 Mbps
256QAM	200 Mbps

Fuente: (Ubierna Yuvero, 2013)

Al inicio, la implementación de un medio inalámbrico parece sencillo y favorable para impedir el uso de cableado estructurado, sin embargo, se debe considerar las posibles interferencias en el lugar que puedan ocurrir y el riesgo de caída del enlace de comunicación.

2.2.8.3. Monitor.

La imagen y el video que es percibido por las cámaras necesitan ser visualizados en un dispositivo de salida donde se puedan interpretar las señales capturadas comprensibles por el ojo humano. Un monitor de CCTV, demostrado en la figura 16, es prácticamente el mismo dispositivo de recepción de televisión con la diferencia de que éste no tiene un circuito de sintonía. La característica principal es la durabilidad de su pantalla. Vale recordar que los sistemas de CCTV pasan 24 horas del día en operación de videovigilancia de ambientes difíciles y hostiles (Cruz, 2013).

En el mercado existen diferentes tipos de monitores que ofrecen una calidad de imagen nítida, desde los CRT (*Cathode Ray Tube*: Tubo de rayos catódicos) hasta los LED (*light-emitting diode*: Diodo emisor de luz), aunque ya existen pantallas táctiles, sin embargo, el táctil no se utiliza en los sistemas de CCTV.

Figura 16. Monitor CCTV.
Fuente: (Sunshine State Security, Inc., 2015).

2.2.8.4. DVR (Digital Video Recorder: Grabador de video digital).

Se lo considera como un dispositivo que almacena video en un medio digital. Generalmente poseen funciones similares de un VCR (*Video Cassette Recorder*: Grabador de video casetera): graba, reproduce, retrocede el video, adelanta, pausa, etc (Cruz, 2013). Pero en oposición a estos, los DVR poseen con una variedad de servicios adicionales como:

- Detección de movimientos.
- Exploración de acontecimientos determinados del video
- Manejo de cámaras PTZ, etc.

El DVR consta de varias funciones que lo hacen muy útil cómo:

- **Quads**, comprime las capturas de 4 cámaras instaladas independientemente y de forma simultánea las representa en la pantalla del monitor.
- **Matrices**, es un método de administración que admite al usuario conmutar distintas señales de video del sistema a la pantalla que se desee visualizar.

Además el DVR trabaja con un códec de compresión estándar de video de H.264. El H.264 es la obtención de un trabajo contiguo de la asociación especializada en codificación de vídeo de ITU-T y la asociación de especialistas en imágenes animadas de ISO/IEC (MPEG). Este códec posee algunas características como (AXIS Communicatios, 2008):

- Sistemas que brinden una disminución de la frecuencia de bits al 50%, con el inicio de una calidad de vídeo estable y contrastado con diferentes estándares de vídeo.
- Resistencia a fallas, de manera que soporten caídas de transmisión por medio de diversas redes.
- Mantiene baja latencia y excelente eficacia para las mayores latencias.
- Sintaxis directa detallada que facilite las implementaciones.
- Tiene una coincidencia en decodificación exacta, que precisa puntualmente los cálculos que ejecuta un codificador y decodificador para frenar la acumulación de fallas.
- Ofrece la flexibilidad apta como para aceptar un vasto grado de transmisiones con distintos requerimientos de frecuencia de bits.

La forma en la que trabaja el códec se la describe de la siguiente manera: la compresión de vídeo consta en minimizar y excluir la redundancia de datos en el video para que el archivo digital logre exportarse y almacenarse eficientemente. En este paso se emplea un algoritmo al vídeo original que elabore un fichero comprimido y lo prepara para transferirlo o almacenarlo. Se emplea el algoritmo opuesto para reproducir en contenido grabado y se elabora un vídeo que domina usualmente el contenido equivalente al vídeo original. El lapso que se espera en comprimir, transportar, descomprimir y revelar un fichero se menciona latencia. En cuanto más se desarrolle el algoritmo de compresión, aumenta la latencia a equivalencia de la potencia de procesamiento (Cruz, 2013). El proceso se describe gráficamente en la figura 17.

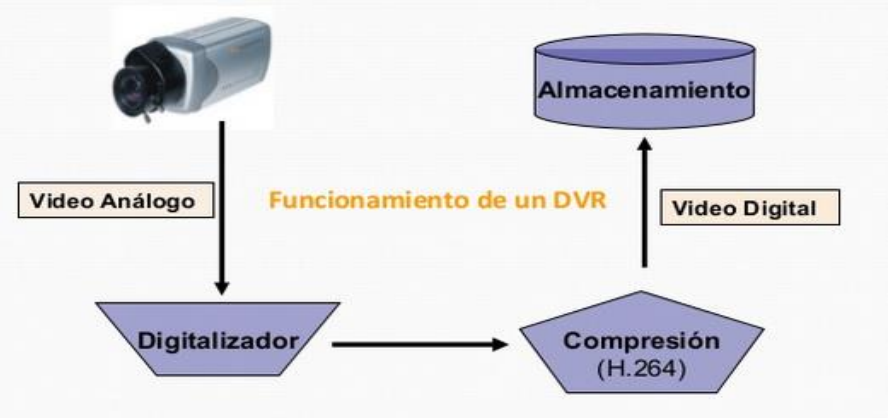


Figura 17. Esquema de funcionamiento de un DVR.
Fuente: (Cruz, 2013).

2.3. Sistema de Control de Acceso.

Son usados habitualmente para el control de puertas tanto interiores como exteriores en instalaciones. Su utilidad va desde comunidades hasta edificios de alta tecnología, por medio de la utilización de módulos de entrada (tales como lectores de proximidad, magnéticos, de códigos de barras o biométricos), el sistema reconoce al usuario y admite o deniega el ingreso a un recinto luego de validarlo en la base de datos que el sistema posea. Las credenciales más usuales en este sistema son el ingreso por contraseña, reconocimiento de voz, detector de huella dactilar, detector ocular (retina) y tarjeta magnética (tags), entre otros. Para la validación de identidades se utiliza varias plataformas de código abierto y una de ellas es la plataforma Arduino la cual proporciona un código y entorno favorable para el programador (Promatco Seguridad, 2005).

Al utilizar la plataforma Arduino para construir el control de acceso, se debe evaluar algunos aspectos importantes, como ¿qué necesita custodiar?, ¿qué tipo de credenciales son la adecuadas para la implementación? y ¿cuáles son los dispositivos que funcionarán en conjunto con el sistema (actuadores)?. En base a estas interrogantes se procede a considerar el tipo de placa Arduino a utilizar y sus características.

2.3.1. Arduino

Arduino es una plataforma de código abierto basado en su inicio al proyecto Procesing, el cual, se apoyaba en un lenguaje de programación llamado Java. Hernando Barragán, que en ese tiempo era un estudiante se basó en el Procesing para crear una placa que disponga de su propio lenguaje de programación y entorno de desarrollo nombrada Wiring. Luego de realizar varios estudios del uso de PIC's los señores Massimo Banzi, David Cuartielles y Gianluca Martino desarrollan una placa de menor tamaño y más económica que la placa Wiring, la cual la llamaron Arduino (García Gonzalez, Antony; Navarro, Kiara;PanamaHitek Creative Team, 2015).

Su funcionamiento se relaciona con la utilización de un microprocesador para grabar instrucciones. Estas instrucciones son elaboradas en base a un lenguaje de programación, que permite a la placa interactuar con varios dispositivos electrónicos. Esta placa posee varios elementos que permiten la comunicación con periféricos de entrada y salida que estén conectados a la misma. Para programar la placa se debe

realizar una comunicación de la misma con un computador por medio de un puerto serial (COM). La comunicación serial hacia el computador se lo hace mediante el puerto USB (García Gonzalez, Antony; Navarro, Kiara;PanamaHitek Creative Team, 2015).

2.3.1.1. Características de Arduino.

Por ser una placa muy versátil y con mucha demanda en el mercado, se presentan las características más relevantes:

- Costo, por tratarse de una plataforma de hardware y software libre, cualquier persona que cuente con la tecnología necesaria puede fabricar estas placas. Existen empresas como en EEUU que se dedica a fabricar sus propios prototipos llamados Arduino y las empresas Italianas llaman a sus prototipos Genuino. También fabrican sensores y placas de expansión no precisamente propias de Arduino, pero que poseen características que se acoplan a las placas, en precios notablemente económicos y que hacen sea de mayor demanda a nivel mundial.
- Disponibilidad, en todas las tiendas de productos electrónicos. Por ser un producto de mayor demanda, se lo puede conseguir en cualquier portal de ventas, incluso hay comercios que ofrecen de primera instancia productos Arduino como una solución para proyectos a elaborar.
- Flexibilidad, la mayoría de modelos de placas Arduino comparten uan característica muy peculiar, que es de menor tamaño y más compactas, con la misma capacidad para realizar desde el encendido automático de un LED hasta el de un motor trifásico, y porque no automatizar procesos industriales. Existen modelos con la capacidad de procesar tareas idéntico al de un computador del siglo 21, como el Arduino Yún, Intel Galileo o el Tre (García Gonzalez, Antony; Navarro, Kiara;PanamaHitek Creative Team, 2015).

Figura 18. Sello de la marca Arduino.
Fuente: (Arduino, 2015).

2.3.1.2. Arduino Leonardo.

La nueva versión apoyada en un microcontrolador ATmega32u4 con atractivas características. Arquitectura de un microcontrolador ubicado en la tarjeta que se conecta con el computador directamente por el puerto USB. Las librerías se agregan al Arduino IDE de modo que el Leonardo pueda operar como un dispositivo USB. Posee 12 entradas analógicas. Posee una característica que determina más conectividad.

El ATmega32u4 posee de un puerto USB originario que puede comunicar el ordenador al Arduino a la misma vez que se establece conexión con otro equipo. Conector micro-USB, 20 pines de Entrada/Salida, todas estas entradas se configurar como digitales; 7 de estas entradas son PWM y el resto son analógicas con un valor de 10 bits. Utiliza un terminal de alimentación tipo jack. Conector ICSP. Botón de reseteo. Funciona a 16MHz. También cuenta con el pin ARef, y para conexión I2C posee SDA y SCL (Ardutienda, 2015).

2.3.1.3. Arduino Yún.

El Arduino Yún es el primer miembro de una nueva serie de tarjetas Arduino que disponen la fuerza de Linux adyacente con la simplicidad característica de Arduino. Adopta el chip del modelo Leonardo (ATMega32U4) junto a un módulo SOC (System-On-a-Chip) dispone de una distribución de Linux cuyo nombre es Linino, establecida en OpenWRT. La característica más atractiva es que resiste red WIFI y red cableada Ethernet. El chip Arduino está conectado al módulo Linux, por lo que es muy fácil que se notifiquen entre ambos y encomendar métodos pesados al equipo Linux integrado en la placa. Contiene dos redes para conectar. Una Ethernet 10/100 Mbps y la otra WIFI (IEEE 802.11 b/g/n, 2,4GHz) que logra acoplarse como cliente o como punto de acceso (BricoGeek, 2014).

Para establecer conexión el pequeño ATMega32U4 con el módulo Linux, se usa la librería Bridge, que proporciona facilidad y es tolerada directamente por el equipo. El puerto en serie del AR9331 está acoplado al puerto en serie del 32U4 con los pines 0 y 1. El puerto serial del AR9331 es un medio para acceder a la consola CLI, lo que admite arrojar procesos y rescatar paquetes directamente desde la consola. Diversos mensajes de administración del sistema de archivos y gestión ya se encuentran instalados por defecto (inclusive el intérprete de Python) y la librería bridge

admite también colocar y arrojar aplicaciones adecuadas con ese mismo sistema (BricoGeek, 2014).

Existe una ventaja que es muy interesante, por la cual la placa (en la ubicación del 32U4) consigue ser programada por WIFI a modo del módulo Linux. Es una placa llena de posibilidades. También cabe destacar que dispone de una ranura para insertar la memoria MicroSD que admite recolectar datos en la misma como páginas web, datos de ingresos o cualquier otra cosa que se necesite y extiende aún más las posibilidades de la placa. No es compatible con el módulo PoE de Arduino. El Arduino Yún solo funciona con el IDE 1.5.4 o superior.

2.3.1.4. Arduino UNO Rev3.

El microcontrolador se puede programar con la utilización del lenguaje establecido en Wiring y el medio de proceso apoyado en Processing. Los prototipos logran ser independientes o pueden comunicarse con el software que actúa en un ordenador. Se basan en algunos microprocesadores y plataformas disponibles en computación física, que poseen un desordenado y complicado código. Estos instrumentos reúnen todas estas alteradas referencias de la programación del microcontrolador y la recluyen en un sistema cómodo para utilizar (Arduino, 2015).

Arduino también facilita la manipulación de microcontroladores y brinda diversas ventajas para los aficionados en el campo de la electrónica automatizada. Es multiplataforma porque trabaja en OS como Windows, GNU/Linux, OSX y Machintosh. Muchos de los microcontroladores se limitan a Windows.

El ambiente de programación tiene una fácil manipulación para la mayoría de personas y es suficientemente útil para las personas que tengan sólidos conocimientos en esta rama. El lenguaje logra ser prolongado mediante librerías C++, y si se desea apreciar las referencias sistemáticas, puede observar la codificación que se basa en el lenguaje AVR. De forma congruente, se puede añadir este código ACR-C directamente en los programas Arduino que se compilen (Arduino, 2015).

El Arduino se basa en microcontroladores ATMEGA8, ATMEGA168 y ATMEGA238 de Atemel. Las versiones están disponibles para su extensión y mejoramiento ya que los modelos están anunciados sobre licencias Creatives Commons.

En este proyecto se utilizará el Arduino Uno Rev3, la cual es una versión mejorada de su predecesor Duemilanove. La cual incluye funciones de autoreset, protección de sobrecargas (ya que se encuentra expuesto a voltajes alto debido a la inducción de las interfaces), conector USB para programarlo, conformado con componentes miniatura de montaje superficial SMD (salvo el microcontrolador, para cambiarlo cuando se lo requiera y un nuevo bootloader OptiBoot a 155Kbps (Arduino, 2015).

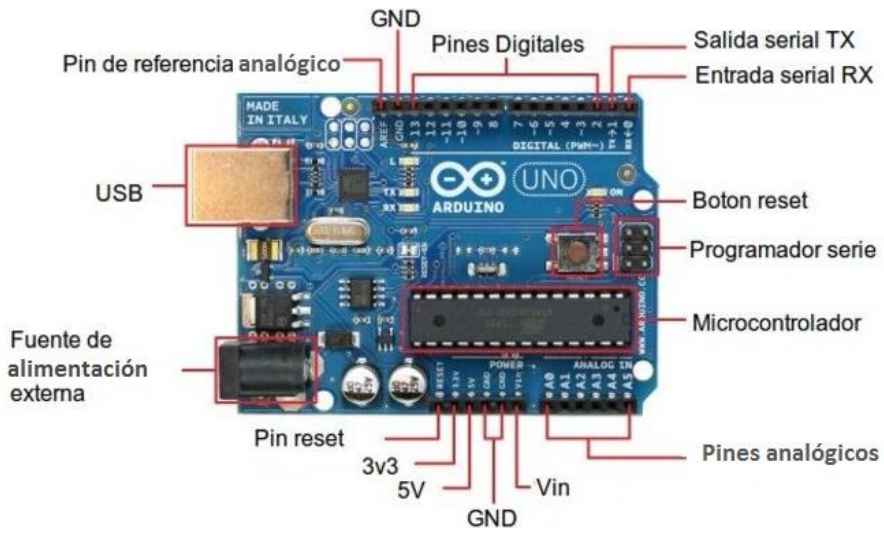


Figura 19. Arduino UNO Rev3 y sus partes.
Fuente: (Arduino, 2015).

2.3.1.5. Ventajas en la utilización de Arduino UNO Rev3.

La ventaja principal de Arduino es que posee un código abierto el cual, no necesita ninguna tarjeta para programar como sucede con algunos microcontroladores, por lo tanto, la misma tarjeta se conecta vía puerto serial al ordenador con la utilización de un cable USB y se logra ingresar a todas las funciones del circuito y algoritmos de las placas. Dispone de varios de los ficheros Eagle, esquemas y elementos. Posee un microcontrolador Atmel ATmega320 de 8 bits de 16 MHz que trabaja a 5v. Posee un mejoramiento en el procesamiento del código ingresado. El Arduino Uno Rev3 posee una memoria flash de 32KB (0,5KB reservados para el bootloader), 2KB de SRAM y EEPROM de 1Kb donde se guardan los códigos de programación (Isaac, 2014).

Otra de las ventajas importantes es que posee librerías para habitualmente cualquier módulo exterior que desee ensamblar y por lo tanto, hace prolijo ilustrarse

del datasheet perteneciente al mecanismo y crear el software preciso para obtener las medidas de los sensores. En la actualidad constan de librerías con funciones destinadas al uso óptimo de los periféricos (Isaac, 2014).

Se escogió esta tarjeta ya que posee muchas ventajas, una de ellas es que tiene los suficientes pines en comparación con el Arduino Leonardo que tiene muchas ranuras para conectar pero es innecesario para el proyecto a implementar. Al conectarse con el Arduino Ethernet Shield se puede conectar a internet, en comparación con el Arduino Yún que tiene más características a su favor pero que por motivo de costos elevados no se considera dentro del proyecto.

2.3.2. Arduino Ethernet Shield.

La Arduino Ethernet Shield es una placa que admite la conexión a internet. Resiste cuatro comunicaciones sincrónicas de socket. Se utiliza la librería de Ethernet que cifra esquemas que se transmiten a Internet por medio del escudo. Este escudo Ethernet se incluye en el Arduino con largas cabeceras wire-wrap que se desarrollan por medio del mismo. Conserva la habilidad inmune de los terminales y permite acumular otro escudo encima de la tarjeta (Enrique, 2014).

La Ethernet Shield posee una comunicación con conectores RJ-45 e incluyen un transformador de línea y powerover Ethernet habilitado. Conserva una ranura por si se desea colocar una memoria micro-SD, que se utiliza para recopilar archivos y así usarse en la red. Es relacionado con varias placas Arduino / Genuino. Posee LED's indicadores de las diferentes conexiones que utiliza el Ethernet Shield, como lo demuestra la figura 20, tales LED's se describen a continuación (Enrique, 2014):

- **PWR:** muestra el encendido de la placa y el escudo.
- **LINK:** indica que el enlace está conectado y parpadea en el momento que existen envío o recepción de los datos por medio del escudo.
- **FULLD**: muestra la conexión full duplex con la que trabaja la red.
- **100M:** muestra la conexión de red de 100 Mb / s (en oposición a 10 Mb/s).
- **RX:** parpadea al momento que el sistema recibe datos.
- **TX:** parpadea en el momento que el sistema envía datos.
- **COLL:** parpadea cuando existen colisiones en la red.

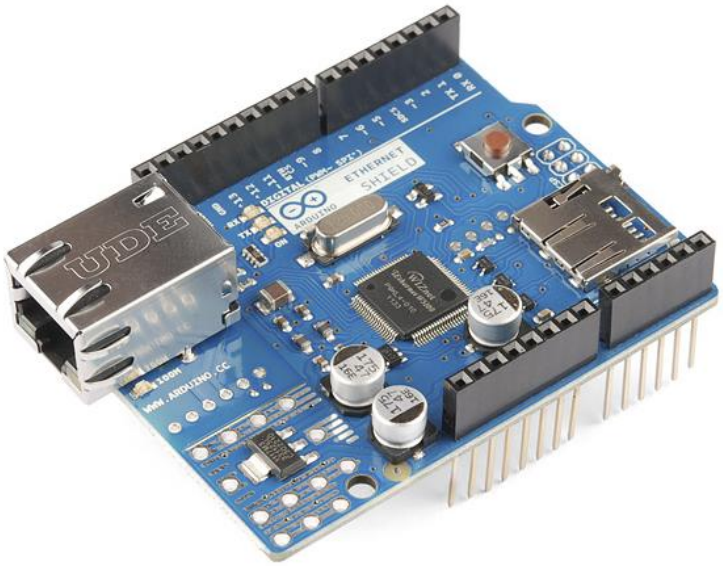


Figura 20. Vista de una Arduino Ethernet Shield.
Fuente: (Enrique, 2014).

2.3.3. Módulo de Interface I2C

El Módulo de interfaz serial I2C permite manejar de un modo suficientemente cómodo a la pantalla LCD. El controlador Arduino posee diversos recursos que son ciertamente definidos, por lo tanto, no admite la conexión de numerosos sensores o tarjetas SD como se muestra en la figura 21. Con este módulo de interfaz I2C, se podrá visualizar los datos por medio de dos terminales con los cuales, ahorra algunas salidas que pueden ser utilizadas por el Arduino. La primacía de manejar este mecanismo evita la conexión engorrosa de cables que algunas veces se dañan y provocan fallas al sistema (Prometec, 2015).

El módulo emplea la dirección (0x20 ~ 0x27), la original es 0x20, pero puede ser reformada. La tensión de alimentación solo se basa en 5V. Con la ayuda de un potenciómetro acoplado al módulo es permisible manejar el backlight y el contraste, por lo tanto se podrá modificar a la necesidad que se presente. Este módulo es absolutamente factible para las adaptaciones 1602 LCD y 2004 LCD. Las pantallas LCD 16×2 y 20×4 poseen ambas 16 pines en su estructura (Prometec, 2015).

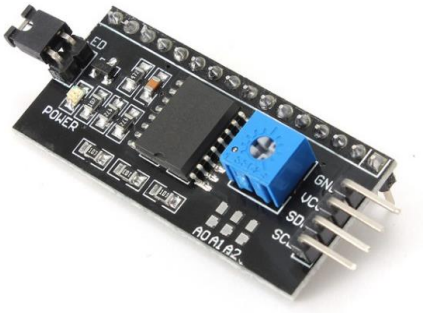


Figura 21. Módulo de Interfaz I2C.
Fuente: (Prometec, 2015).

2.3.4. LCD HD44780.

Un LCD (Liquid Crystal Display: Representación visual por cristal líquido) es un dispositivo de salida donde se dispone letras números y caracteres especiales que se quiera mostrar. Absolutamente espera en que se genere una información admitida. En ese instante la pantalla procesa la información o instrucciones, los muestra y retorna en modo espera, hasta poseer diferentes datos se envíen o reciban. De ningún modo se recogerá datos de la LCD mientras el pin R/W (L/E) se localice siempre bajo, esto indica que existe escritura por parte de la LCD. El pin RS estará bajo, al momento que se escriba caracteres, en vista que todo se considera instrucciones (Svenungson, 2004). Todo estos pines se muestra en la figura 22. Todas estas conexiones hacen que sea sencillo programar la pantalla.

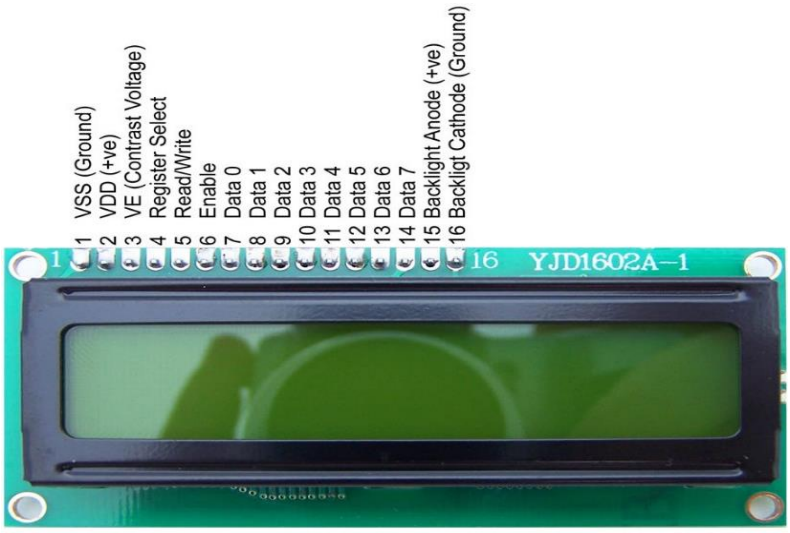


Figura 22. Display LCD HD44780 con su respectiva configuración de pines.
Fuente: (Protostack, 2014).

2.3.5. Teclado matricial 4 x 4.

La matriz de botones es un pequeño ajuste de pulsadores conectados en filas y columnas, de tal manera que se logran examinar algunos pulsadores con el pocos pines solicitados como se muestra en la figura 23. Esta matriz 4x4 utiliza solamente 4 pines para las filas y 4 para las comunas, con esto se pueden leer 16 teclas al usar 8 pines de un microcontrolador. Si se adjudica en alto (1 lógico) a las filas y columnas de la matriz, al presionar un botón el circuito correspondiente a la fila y columna de dicho botón cierran el circuito y manda esa información para la interpretación del microcontrolador de acuerdo a su programación (Murillo, 2012).

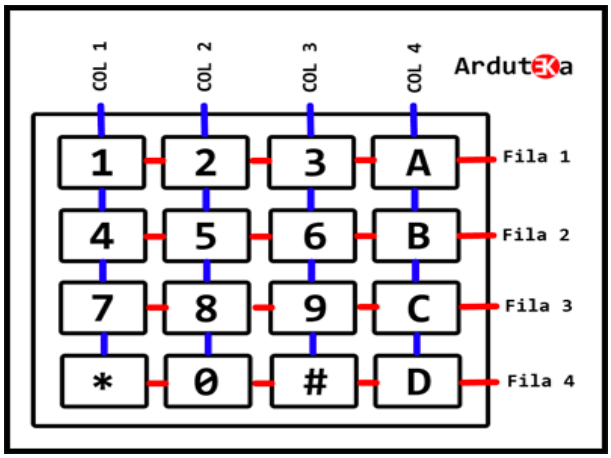


Figura 23. Teclado matricial 4 x 4 con su estructura interna.
Fuente: (Murillo, 2012).

2.3.6. Relé.

Un relé es un dispositivo electromecánico que posee una bobina en su interior que al ser energizada genera un campo magnético y sirve para activar el electroimán y atraer unas platinas que realizan la función de conmutado, puede ser de tipo NO (*Normally Open*: Normalmente abierto) y NC (*Normally Closed:* Normalmente cerrado*)*. Por lo general trabaja a voltajes desde 3.3v hasta 50v en VCA y VCD para inducir el electroimán. La alimentación que recibe para abastecer el actuador va desde 1 VCD/CA hasta los 240 VCA/VCD según las especificaciones del fabricante. En la actualidad existen relés de mayor capacidad para aplicar en interfaces de industrias automatizadas, estos relés, son llamados contactores. En la figura 24 se puede observar un relé con sus especificaciones de fábrica impresas (Electronica Unicrom, 2014).

Figura 24. Relé de 5V con sus respectivas especificaciones del fabricante.
Fuente: (Electronica Unicrom, 2014).

2.3.7. Buzzer (Zumbador)

Un zumbador es un mecanismo cuyo trabajo es transformar energía eléctrica en acústica. Contiene dos terminales una positiva donde se envía la señal eléctrica y otra negativa que va conectada a tierra. Generalmente se encuentra señaladas a través de colores: rojo (positivo) y negro (negativo).

Está formado por una lámina metálica y un electroimán como se observa en la figura 25. Su funcionamiento reside en originar un sonido a cierta frecuencia o diversas frecuencias que para el oído humano se percibe como tonos.

Para crear un sonido de un tono, o sea de una sola frecuencia, basta con emplear una onda cuadrada al positivo del zumbador para que éste convierta la onda cuadrada a un tono con su respectiva frecuencia. Remitir una onda cuadrada logra ser tan fácil si se cuenta con un microcontrolador (GlobeRed, 2011).

Figura 25. Vista de un modelo de buzzer.
Fuente: (GlobeRed, 2011).

2.3.8. Direccionamiento IP

Es un direccionamiento lógico que tienen una identificación única para cada host y que se comunica mediante protocolo TCP/IP. La dirección IP está conformada por 32 bits y se divide en 4 octetos (1 Byte u 8 bits en cada octeto). Esta dirección identifica la localización de un host en la red como lo hace la dirección de un domicilio en una ciudad. En el direccionamiento se elige la mejor ruta hacia el destino por medio del uso los protocolos de enrutamiento (Andreu Gómez, 2010).

2.3.8.1. Direccionamiento estático.

El Direccionamiento estático es un número asignado permanentemente a una computadora, o sea, su dirección IP no cambia. Cuando el cliente accede a la red automáticamente se conectará a ella con la misma IP sin necesidad que el router entre en negociación para asignar una IP al equipo (Andreu Gómez, 2010).

2.3.8.2. Direccionamiento dinámico.

La asignación de una dirección IP dinámica lo realiza un servidor DHCP al usuario. La duración máxima de la IP que se designa al usuario es limitada de acuerdo a la configuración de su servidor DHCP. Este servidor suministra a cada cliente que desee participar en la red, parámetros de configuración específicos. Las direcciones IP del cliente se incluyen en aquellos parámetros que ofrece el servidor (Andreu Gómez, 2010).

2.3.8.3. IP pública

La utilización de la IP pública es aplicada la mayoría de veces en servidores de internet. Para montar estos servidores se configura la IP estática y no dinámica porque puntualmente se necesita que la IP no cambie, sin embargo se puede configurar de manera dinámica (Andreu Gómez, 2010).

2.3.8.4. IP privada

Las IP privadas se utilizan para distribuir conectividad entre equipos internos sin que se pueda acceder directamente a Internet. Cuándo se crea una red de trabajo local (LAN, Local Area Network) donde se conectan varias computadoras se considera una red privada (Andreu Gómez, 2010).

2.3.9. Protocolo de Comunicaciones

Un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas, para transmitir información por medio de alguna clase de variación de una magnitud física (Tomasi, 2003).

Al pasar el tiempo la tecnología de las comunicaciones se optimizó Por aquello surgieron nuevos protocolos a los que se adecuan los productos de cada fabricante. El más usado en Internet es el TCP/IP (Tomasi, 2003).

2.3.9.1. Protocolo TCP/IP

El protocolo TCP/IP (Transmission Control Protocol / Internet Protocol) El TCP / IP es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, que incluye a la PC, minicomputadoras y computadoras centrales sobre redes de área local y área extensa. En sus inicios los nodos de las redes ARPANET, PRNET (packet radio) y SATNET (packet satellite) se interconectaban. Las redes antes nombradas ya no se hallan activas pero el protocolo aún les sobrevive. En la actualidad se usan para comunicar redes universitarias, comerciales, gubernamentales, entre otros (Tomasi, 2003).

2.3.9.2. Ethernet

Ethernet es un nombrado método de conexión LAN, que usa el CSMA/CD (Carrier Sense Múltiple Access with Collision Detection: Acceso múltiple con portadora y detección de colisiones) entre grupos de computadores con varias topologías de cables (Tomasi, 2003).

2.3.9.2.1. Características.

- Es pasivo, por lo tanto, no necesita de una fuente de alimentación independiente, y por consiguiente, falla solo cuando el cable se corte realmente, termine incorrectamente o que el puerto sufra algún desperfecto.
- Se enlaza al usar una topología de bus donde el cable culmina en los dos extremos.
- Usa varios protocolos de comunicación y logra enlazar medios informáticos complejos, al contener Netware, UNIX, Windows y Macintosh.

2.3.9.2.2. Método de acceso de la Ethernet.

Dicho método para acceder que usa Ethernet es el Acceso Múltiple con Portadora Y Detección de Colisiones. CSMA/CD es una serie de pautas que establece la forma de contestación de los mecanismos de red cuando dos de ellos pretenden remitir datos en la red paralelamente (Area de Ingeniería Telemática, 2012). La figura 26 describe el momento que se origina múltiples transmisiones entre equipos se provocan colisiones.

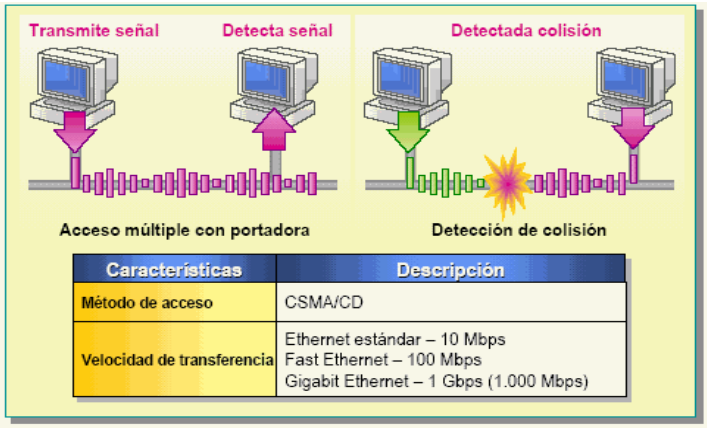


Figura 26. Modo de función del método de acceso CSMA/CD.
Fuente: (Area de Ingeniería Telemática, 2012).

Cada dispositivo que pertenezca a la red, inclusive los clientes y servidores, busca el cable en rastreo de tráfico en la red. Exclusivamente cuando un dispositivo descubre que en el medio de transmisión no hay circulación de energía y que no existe tráfico, proceda a transmitir los datos. Luego de que el dispositivo envíe los datos en el medio de transmisión, ningún otro dispositivo logra enviar datos hasta que los originales alcancen su destino y el medio retorne a estar libre. Después de descubrir una colisión, un mecanismo espera un tiempo aleatorio y a continuación intenta reenviar el mensaje. Si el equipo descubre de nuevo una colisión, antes de reenviar el mensaje espera la segunda colisión (Area de Ingeniería Telemática, 2012).

2.3.9.2.3. Importancia y velocidad de transferencia.

Ethernet es un protocolo muy conocido ya que logra características de muy buena atención en cuanto a velocidad, modo de instalación y costo. Estas muy buenas consideraciones, combinadas con la extensa aprobación en el mercado y la destreza de aguantar implícitamente todos los protocolos de red más conocidos hacen a Ethernet la tecnología excelente para la red de la totalidad de usuarios de la informática moderna. Ethernet Estándar, nombrada 10BaseT, tolera velocidades de transmisión de datos de 10 Mbps encima de una extensa diversidad de cableado. Además están favorables adaptaciones de Ethernet de alta velocidad. Fast Ethernet tolera velocidades de transmisión de datos de 100 Mbps y Gigabit Ethernet tolera velocidades de 1 Gigabyte por segundo (Gbps) (Area de Ingeniería Telemática, 2012).

Figura 27. Conexiones a puertos Ethernet del Switch.
Fuente: (Area de Ingeniería Telemática, 2012).

2.4. Descripción del proceso investigativo del sistema de seguridad automatizado de videovigilancia con Arduino.

2.4.1. Metodología de investigación.

Para el desarrollo de este sistema se aplicaron varios métodos de investigación que lograron avanzar cada etapa del proceso de implementación.

2.4.1.1. Método empírico de observación.

Se utilizará el método empírico de observación para realizar la inspección técnica donde se receptará los requerimientos necesarios con el fin de asignar los

dispositivos pertinentes de un sistema de seguridad automatizado de videovigilancia en el laboratorio computación que mejore la custodia de los recursos educativos.

2.4.1.2. Método analítico sintético.

Se utilizará el método analítico sintético para identificar las condiciones de inseguridad que necesita el laboratorio de computación y seccionar los sistemas con sus elementos respectivos que atenderán cada condición y así tener una correcta custodia de los equipos.

2.4.1.3. Método de medición.

Se utilizará el método de medición para ubicar estratégicamente las cámaras que cubrirán los puntos ciegos y el control de acceso que intervendrá en el sistema automatizado.

2.4.1.4. Método empírico sistemático.

Se utilizará el método empírico sistemático para organizar procesos que controlará el sistema de seguridad al momento de detectar las acciones ilícitas y realizar una acción frente a los resultados que se obtengan en las grabaciones o intentos de alterar el acceso al laboratorio.

2.4.1.5. Método empírico experimentado.

Se utilizará el sistema empírico experimentado para analizar la conducta del método automatizado en el campo de acción y evaluar los resultados obtenidos en el momento y aplicar las correcciones necesarias en conjunto con las personas experimentadas en el campo de la botánica.

2.5. Resultados que se esperan del proyecto.

Con la ejecución del sistema, se espera brindar de seguridad al laboratorio de computación de la Unidad Educativa Luxemburgo y por lo tanto, tener un mejor registro de ingreso a la misma y video en tiempo real que pueda enviar alertas que registren el método de localización de los sucesos en la institución educativa.

3. Presentación de los resultados.

Se detalla en la exposición de los resultados alcanzados en el proyecto, el diseño, implementación y montaje del hardware, software que componen los equipos utilizados en la seguridad del establecimiento educativo.

3.1. Estudio de los diferentes sistemas de seguridad de videovigilancia que se empleen en la Unidad Educativa Luxemburgo.

Para desarrollar el sistema de CCTV adecuado en la Unidad Educativa Luxemburgo, se realizó las correspondientes investigaciones de sistemas CCTV ubicados en la ciudad de Quito. Con el objetivo de tomar las observaciones respectivas y adecuadas para diseñar e implementar el sistema en la institución antes mencionada. Por lo tanto la investigación se realizó en diferentes lugares de Quito en instituciones educativas y empresas de comercio a fin. A continuación se describen tres diseños e implementaciones de sistemas de CCTV diferentes.

3.1.1. Sistema de seguridad con videovigilancia en la escuela Jorge Escudero Moscoso.

De acuerdo a la visita de la escuela Jorge Escudero Moscoso, cuenta con un sistema de videovigilancia de 2 cámaras analógicas tipo tubulares-exteriores y 2 cámaras tipo domo-interior. La marca de las cámaras es HIKVISION con una resolución de 720 líneas de televisión. También cuenta con un DVR de 4 canales marca ViperTek.

La distribución del sistema se caracteriza de la siguiente manera. Las dos cámaras tipo tubular se encuentran ubicadas al exterior de la sala de audiovisuales de la escuela. El primero apunta a un extremo de la sala donde se encuentra la escalera de ingreso a otras aulas. La otra cámara exterior captura los videos en el otro lado del laboratorio donde se ubica el jardín. Las dos cámaras domo se ubican el interior de la sala, la primera está en un extremo encima de la puerta y la otra se encuentra el otro extremo a lado de una estantería de libros. En la figura 28 y 29 se pueden observar las cámaras distribuidas por toda el área interior y exterior del aula de audiovisuales.

Figura 28. Cámara tipo domo ubicada en el extremo interior de la sala de audiovisuales de la escuela.
Fuente: Escuela Jorge Escudero Moscoso.

Figura 29. Cámaras tipo bala ubicadas en los exteriores de la sala de audiovisuales de la institución educativa.
Fuente: Escuela Jorge Escudero Moscoso.

La ubicación del DVR fue estratégica, ya que está en la oficina del rectorado académico. Con el fin de respaldar la información de las cámaras, al momento de que surja un inconveniente. A continuación en la figura 30, se observa el DVR que se utilizó y el modo de visualización de los videos en el monitor del sistema.

Figura 30. DVR ViperTeK que se utilizó en el sistema CCTV de la escuela y su modo de visualización.
Fuente: Escuela Jorge Escudero Moscoso.

A continuación se describen todas las características del sistema CCTV implementado en la escuela Jorge Escudero Moscoso:

- **Cámara exterior PICADIS DS-2CE15C2P(N)-IR:** Posee un lente tipo 1/3 PICADIS**.** Sensor de 1,3 MP: 1280 (H) x 960 (V) Píxeles Efectivos**.** Ofrece una resolución de 720 TVL Líneas de TV de Resolución Horizontal. Es una cámara con la funcionalidad Día / Noche. Su lente fija es de 3.6mm, 0.1 lux / F1.2**.** La distancia IR 20m**.** Smart IR, Alto Rango Dinámico**.** La salida de la imagen de video superior y ultra baja iluminación de luz**.** Amplia Gama de Temperaturas de Funcionamiento. IP66 Resistente a la Intemperie (HIKVISION, 2014).

- **Cámara interior PICADIS DS-2CE55C2P(N)-IR:** Posee un lente tipo 1/3" PICADIS. Sensor de 1,3 MP: 1280 (H) x 960 (V) Píxeles Efectivos. Ofrece una resolución de 720 TVL Líneas de TV de Resolución Horizontal. Funcionalidad Día / Noche. 2.8/3.6/6mm Lente Fijo, 0.1 lux /F1.2. Distancia IR 20m. Smart IR, high dynamic range. La salida de la imagen de video superior y ultra baja iluminación de luz. Amplio rango de temperatura (HIKVISION, 2014).

- **VIPERTEK – Videograbador Digital DVR de 4 canales – VIP-DV4:** Es un DVR de 4 canales Vipertek. Soporta hasta 4 cámaras a 1080p en tiempo real. Compresión H.264 dual-stream. Grabación en D1 (4CIF) en los 4 canales. Salidas simultaneas de HDMI / VGA / TV. Soporta 1 disco duro SATA de hasta 4 TB y 2 USB 2.0 (ViperTek, 2014).

En conclusión se realizó una inversión de 735 dólares, en la adquisición de las 4 cámaras interiores y exteriores, el DVR de 4 canales, un disco duro de 1TB, placas de conexión para comunicación inalámbrica a telefonía celular y el cableado estructurado pertinente.

3.1.2. Sistema de videovigilancia mediante cámara IP para la empresa Chasquis Compu Store.

De acuerdo a la visita en la empresa Chasquis Compu Store, se constató la instalación de un sistema de videovigilancia mediante cámaras IP respaldadas con un servidor de video. El esquema de conexión se basó en la implementación de los siguientes elementos: Un servidor de video, 2 cámaras IP ubicadas en sitios estratégicos del lugar, un router de acceso, y un Switch para la conexión interna de la red.

La distribución del sistema se caracteriza de la siguiente manera. La primera cámara e encuentra ubicada en el interior del establecimiento donde se encuentra las computadores que los usuarios utilizan para acceder al internet (consumo por cobrar). La otra cámara IP se encuentra instalada en el área de despacho y facturación (caja de cobranzas). En la figura 31 se observa la cámara IP que se utilizó en el establecimiento. A continuación se describe las características de las cámaras IP utilizadas en la instalación.

Figura 31. Cámara IP SONY VMD-900
Fuente: (SONY, 2004).

Para almacenar los videos se cosideró para la instalación un ordenador con las características que se muestra en la tabla 6:

Tabla 6. Características del servidor.

DETALLE	DESCRIPCIÓN
Sistema operativo	Windows XP, SP2
Monitor	LG 15”
Resolución de la pantalla	1024 x 768 Pixeles
Memoria	4GB
Mainboard	Intel DG3145
Procesador	Intel Pentium Dual Core 3,2 GHz
Disco Duro	500GB
Sistema de archivos	NTFS
Capacidad de espacio libre en disco	250GB

Fuente: (Gualotuña Suntasig, 2009).

Para la conexión remota del servidor y el acceso de un usuario autorizado fuera de la red se considera utilizar un router D’Link DIR 655. Soporta encriptación WEP64/128 bit, WPA, WPA2. Soporta DHCP server, DHCP client y Servidor Virtual. Soporta firewall de seguridad con filtrado de puertos, filtrado de IP, filtrado de MAC, Puerto de envío, puerto trigger y funciones de DMZ hosting. Procesador de alta velocidad, que ofrece en mejor rendimiento. Administración por Web Browser (Gualotuña Suntasig, 2009). A continuación en la figura 32, se observa el router utilizado en la instalación del sistema en el establecimiento.

Figura 32. Access Router D’Link DIR-655.

Fuente: (Gualotuña Suntasig, 2009).

En todo el sistema instalado en el establecimiento Chasquis Compu Store, se presupuestó un total de $ 855,36. Que incluye las 2 cámaras IP, servidor, router y varios elementos importantes dentro de la red.

3.1.3. Sistema CCTV implementado en el local comercial de TOTTO para monitoreo a través de internet.

Se realizó la visita técnica a el local de TOTTO en el CC El Recreo, donde se pudo constatar algunas instancias de la instalación, ya que el local guardar reservas, con respecto a su sistema de videovigilancia. En los cuales se logró investigar sobre la estructura del sistema implementado.

Para la implementación se usó una cámara PTZ tipo mini domo, con las siguientes características. Posee una resolución entre 300 TVL - 600 TVL. Se ajusta a un Zoom entre 10-20X. Tiene un rango de rotación de 0°-360°. Rango de rotación vertical de 90°. Visión nocturna con IR (HIKVISION, 2014). A continuación en la figura 33, se observa la cámara utilizada en el local comercial.

Figura 33. Cámara IP HIKVISION Mini Domo Wifi-exterior Ds-2cd2120.
Fuente: (HIKVISION, 2014).

Al implementar las cámaras era necesario ubicar un lugar estratégico para respaldar toda la información de video que provenía de todos los locales de TOTTO a nivel nacional. Se recibió información que el servidor se encuentra en la ciudad de Quito, por cuestiones de seguridad no se especificó el lugar. Sin embargo, se informó de las posibles características del DVR que se encuentra en cada local comercial. Las cuales se detallan a continuación. Visualización remota por red, internet* o teléfono

móvil**.Compresión de video H.264. Permite de forma simultánea: Reproducción, copia de seguridad, control y acceso remoto. Cuatro modos de grabación: Grabación manual, grabación por calendario (VTA, 2013).

Grabación por detección de movimiento. Grabación automática al encendido. Incluye disco duro de 500GB que permite la grabación continua durante varios días según configuración. Salida de video VGA compatible con la mayoría de monitores. Resolución de grabación D1, Half D1, CIF Sistema operativo LINUX. Sistema de televisión NTSC / PALM. Canales de video: 4 Canales de entrada de video. 1 canal de salida de video. 1 canal de salida de video VGA. Canales de audio: 1 Canal de audio de entrada. 1 Canal de audio de salida. Visualización: Resolución: NTSC: 720 x 480 / PAL: 720 x 576. Tasa de tramas: NTSC: 120fps / PAL: 100 fps (para las 4 cámaras). Grabación: Resolución: NTSC: CIF (352x240) / HD1 (704x240) / D1 (704x480). Tasa de tramas: PAL: CIF (352x288) / HD1 (704x288) / D1 (704x576). Almacenamiento: Un disco duro 320GB, conector SATA compatible con discos duros hasta de HDD 2 TB. Funciones puerto USB: Mouse, copia de seguridad, actualización. Control PTZ: Incluye interface RS485 para protocolo PELCO P & PELCO D. Conexión a red: RJ45, 10 M / 100M. Formato de compresión de audio ADPCM. Detección de movimiento con sensibilidad y área ajustable. Notificación de alarma remota a través de correo electrónico. Calidad de grabación ajustable. Alarma en caso de pérdida de señal de video. Control de acceso por contraseña. Puerto (RS485) de control para cámaras PTZ. Incluye control remoto, mouse USB y conector BNC RCA. Voltaje de funcionamiento: 110 V AC 12 V DC/500 mA (VTA, 2013).

En conclusión la inversión de la empresa TOTTO en el sistema de seguridad a nivel nacional es sumamente alto, cuando se toma en cuenta la cantidad de locales comerciales y también puesto consideración una cámara IP y un DVR en cada establecimiento. Para calcular un presupuesto estimado por cada local, se basó en los precios que tiene actualmente los elementos del sistema. Por lo tanto se calcula un estimado de $ 440 para la implementación.

3.2. Análisis del sistema recomendable para la automatización de la seguridad en el laboratorio de la Unidad Educativa Luxemburgo.

3.2.1. Etapas del proyecto.

Dentro del proyecto existen dos sistemas de seguridad: el sistema de videovigilancia y el control de acceso Arduino. Estos sistemas en conjunto realiza la

custodia del laboratorio de computación. Para la elaboración de estos sistemas se los dividió por etapas, con el fin de buscar las mejores alternativas para el funcionamiento correcto del sistema en general en el laboratorio de computación en la institución destinada.

3.2.1.1. Etapas del sistema de CCTV.

Para la elaboración del sistema CCTV se dividió por etapas. Dichas etapas ayudarán a desarrollar el funcionamiento correcto del sistema, con la ubicación del área de cobertura, las cámaras necesarias y la elección y ubicación del DVR que administra las grabaciones del sistema.

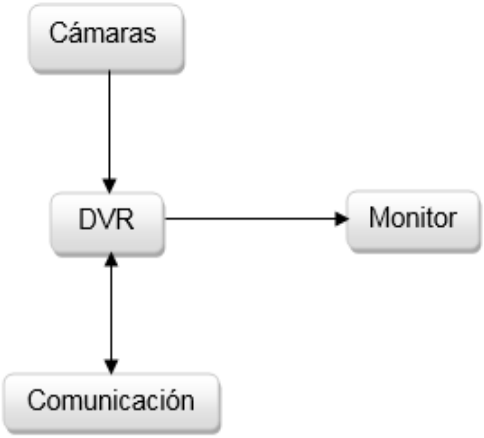


Figura 34. Etapas del sistema de CCTV.
Fuente: El Autor

3.2.1.1.1. Etapa de cámaras.

Para esta etapa se consideró las cuatro cámaras de la marca ISmart modelo C1030DP7 propias del sistema. Tienen una resolución de 700 TVL que permiten IR a prueba de agua, consta también de un sensor de imagen CMOS LED 36pcs IR para visión nocturna. Mínimo de iluminación: OLux (IR encendido). Posee un lente 3.6 /6mm, es resistente al agua: IP66 que sirve para uso interior y exterior.

Estas cámaras son analógicas, por lo tanto, solo envían señales al DVR, no las recibe como se representa en la figura 34, cuya conexión indica una flecha direccional, es decir, que solo enviará señales. Permiten cubrir un ángulo de visibilidad de 90°, por lo cual se eligió los lugares de ubicación de las cámaras, para enfocar el área de monitoreo.

El medio de transmisión utilizado por las cámaras es el cobre y que encuentra alojado en el cable coaxial. El tipo de cable coaxial es el RG58U que tiene una impedancia de 50 ohmios y utiliza también conectores BNC para ejecutar el vínculo de la cámara con los canales de video del DVR. La atenuación del enlace de cada cámara con cada canal del DVR es de 7,59 dB (tramo de 100 metros a 10MHz 4,59 dB y 1,5 dB cada conector BNC). La mayor medida de los tramos de conexión es de 60 metros, por lo tanto, se considera un enlace que cumple con las normas especificadas en el cableado estructurado de la ITU-T.

3.2.1.1.2. Etapa del DVR.

En esta etapa se considera usar el DVR ISmart D5004FH, que es un dispositivo propio del sistema. Posee cuatro canales de entrada de video (BNC) para la conexión de las cámaras. Consta de cuatro puertos de salida de video para conectar el monitor, ya sea con conexión BNC, VGA o HDMI. También contiene cuatro puertos de conexión RCA para la entrada de audio (cuando existan micrófonos conectados al dispositivo). Posee un puerto Ethernet para comunicarse con la red de Internet. También contiene dos puertos USB para conectar dispositivos de entrada que usualmente se utiliza en estos sistemas como lo es el mouse y el teclado. Y consta de un terminal hembra para conectar la alimentación DC que proporciona el adaptador de corriente.

El DVR ISmart soporta una conexión de disco duro de hasta 2GB de almacenamiento. Trabaja con un mecanismo de compresión de video H.264 doble flujo para utilizar una mayor capacidad de almacenamiento. Además trabaja con una interface gráfica muy usual en estos sistemas de CCTV. También posee un sistema de MD (Motion Detection: detección de movimiento). Al momento de la configuración de grabación puede cambiarse a modo MD. Con este cambio en la configuración se grabarán las porciones de video sólo cuando exista movimiento y el resto de tiempo se parará la grabación.

El software que usa el DVR tiene varias opciones y una de ellas es la administración del puerto Ethernet para la comunicación por IP estática o dinámica; La configuración de P2P para conectar los dispositivos smartphone con el sistema de CCTV ISmart. También existe una opción de alarmas, donde se puede configurar la sensibilidad de la cámara: a modo de “mayor” para que capture los movimientos más

diminutos, o a modo de “normal” para que capture los movimientos más representativos, y otras opciones propias del procesamiento de la imagen.

3.2.1.1.3. Incorporación del monitor.

En esta etapa se incorpora el monitor LCD HP 17”. La característica más importante de este monitor es que por su sistema LCD el consumo de energía es menor al de un CRT. Posee un conjunto de botones que regulan en brillo, la posición de la imagen en el interior del monitor, zoom, etc. Además para hacer más énfasis en el ahorro de energía, posee un sistema automático de hibernación. Por lo tanto, cuando el monitor no esté en uso entrará a modo de reposo, de acuerdo al periodo de tiempo que se configure en el mismo monitor.

3.2.1.1.4. Etapa de comunicación.

La función de esta etapa es la comunicación del DVR con la red de internet. Para esta comunicación se dispone a utilizar un cable UTP RJ-45 Cat. 6A, que se conecta al router de la inspección que provee el servicio de internet. El motivo por el cual no se puede conectar con un dispositivo smartphone es que el servicio de la institución es con IP privada. Por lo tanto, no se puede acceder remotamente desde otra red que no sea la de la institución.

3.2.1.2. Etapas del sistema de control de acceso.

Para la elaboración del control de acceso Arduino se lo dividió por etapas. Cada etapa tiene un papel muy importante en el sistema y se relacionan la una con la otra. A continuación en la figura 35 se describen las actividades y elementos de cada etapa:

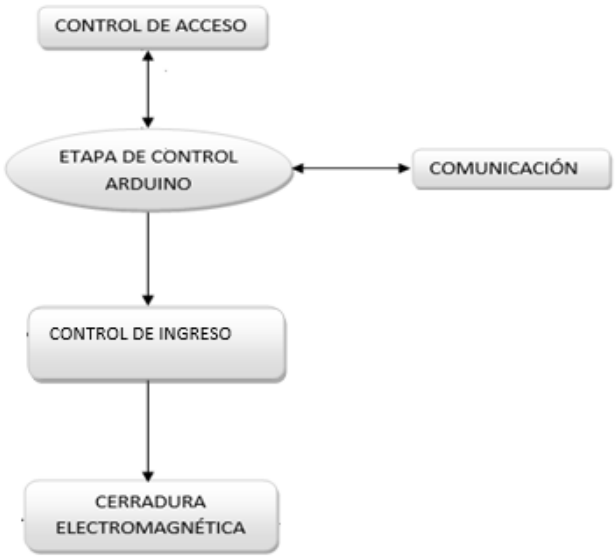


Figura 35. Esquema de las etapas del sistema de control de acceso Arduino.
Fuente: El Autor.

3.2.1.2.1. Etapa de control Arduino.

Esta etapa se compone de tres tarjetas Arduino: la tarjeta Arduino Uno, la Shield Ethernet y el módulo relés Arduino. La tarjeta Arduino Uno consta de un procesador ATMEGA328 de 8 bits a una velocidad de 16 MHz y funciona a 5 VCD. Esta tarjeta posee una flash de 32Kb, una SRAM de 2Kb y una memoria EEPROM de 1Kb. Como el código que se utilizó para programar el Arduino no ocupa mucha memoria se consideró utilizar esta tarjeta por motivo de costos y espacio.

Otra tarjeta considerada para controlar el ingreso es la Shield Ethernet de Arduino. Esta tarjeta tiene la facilidad para adaptarse al Arduino Uno por medio de las ranuras. Cuenta con un puerto Ethernet para conectarse a la red de internet. Posee varios LED's indicadores de transmisión y conexión de los puertos. Se la consideró también por su precio módico y en conjunto con el Arduino Uno se compatibilizan para incluir códigos HTML y crear una página web que contenga lo necesario para el acceso remoto de la cerradura electromagnética.

El módulo relé de Arduino también es una tarjeta muy importante en este control, ya que es la interface entre los pulsos (instrucciones) que genera el microcontrolador y el actuador (cerradura electromagnética). El módulo se alimenta de voltaje que provee el Arduino Uno, con esto se evita alimentarlo independientemente.

Aunque la alimentación independiente es muy recomendable para circuitos que requieran de más actuadores.

3.2.1.2.2. Etapa de control de ingreso.

Esta etapa consta de teclado 4x4 para ingreso de caracteres, la LCD para visualizar los caracteres ingresados por teclado, los LED's indicadores de activación y desactivación de la cerradura electromagnética y el buzzer. El teclado 4x4 se utiliza en esta etapa para ingresar los caracteres que se utilizarán para validar la contraseña almacenada. Se consideró configurar la tecla "#" para encender la LCD cuando está en modo de reposo; la tecla "*" servirá para borrar los caracteres mal ingresados. Este dispositivo se encuentra instalado en el centro de la caja.

La LCD que se utilizó es la HD44780 16x2. En esta pantalla se puede visualizar 16 caracteres en cada fila y existen 2 filas en total, se puede observar 32 caracteres. Como la LCD posee 16 pines y utilizar todos, ocuparán todas las ranuras del Arduino Uno, se decide colocar un módulo interface I2C para optimizar todos los pines y sólo utilizar 2 entradas analógicas para transmitir datos a la tarjeta Arduino. Este módulo utiliza la alimentación de 5v que provee la tarjeta Arduino Uno. Se encuentra instalada en el lado superior de la caja, con su respectiva etiqueta.

Los LED´s que se utilizan son de alta luminosidad. El LED rojo indica que la cerradura está desactivada y se encuentra instalado en la parte derecha de la caja (vista de frente) entre la LCD y teclado. El LED verde indica que la cerradura está desactivada y se ubica en el lado izquierdo. El buzzer utiliza el tono para identificar el carácter que se ingresó y también cuando la contraseña se ingresó correcta o incorrectamente. Se encuentra instalado por dentro de la caja.

Otro aspecto muy importante en este sistema es controlarlo remotamente. Para esto, se desarrolló un software en HTML para validar una contraseña de ingreso y así darle paso a la ventana de desactivación o activación de la cerradura electromagnética. Dicha ventana contiene dos botones para activar y desactivar, también un texto de estado que indica si la cerradura esta activada o desactivada. Este programa se comunica por medio del puerto de Ethernet del Arduino, siempre y cuando el computador que contenga el programa se encuentre dentro de la red.

3.2.1.2.3. Etapa de comunicación.

Esta etapa comprende la conexión del Arduino con la red privada de la institución. Para esta conexión se utilizó un cable UTP Cat. 6A con ponchado certificado de RJ45. Este cable conecta el router del laboratorio con el puerto Ethernet de la Shield. En la figura 35 se observa que la etapa de comunicación es bidireccional, esto se debe a que puede enviar y recibir datos.

3.3. Diseño del sistema de seguridad automatizado.

Para el diseño del sistema de seguridad automatizado de videovigilancia con Arduino, existen varios requerimientos que se toman en cuentan como:

- Las cámaras de vigilancia deben cubrir todas las áreas en el interior y exterior del laboratorio de computación del bloque uno de la institución educativa.
- Un software capaz de administrar el DVR, que configure la detección del movimiento, y un dispositivo capaz de almacenar los registros de las acciones capturadas.
- Un dispositivo y software que controle el acceso al laboratorio y valide las credenciales de ingreso por medio de contraseñas y remotamente.
- Un dispositivo capaz de establecer la conexión de las interfaces utilizadas a la red privada.
- Se requiere tener una red LAN para conectar los dispositivos y manejarlos de manera remota tanto las cámaras como el control de acceso.

La figura 37 demuestra un plano del bloque uno de la Unidad Educativa Luxemburgo, con la distribución estratégica de las cámaras alrededor del laboratorio, donde se observan que están colocadas de una forma que no existan puntos sin cobertura de videograbación. Y por supuesto la ubicación del control de acceso en la puerta de ingreso al laboratorio. También se observa en la figura 38 las diferentes coberturas que poseen las cámaras en cada ambiente vigilado.

3.3.1. Cálculo de la distancia de objeto al lente de acuerdo al modelo de las cámaras analógicas del sistema CCTV implementado.

La tecnología de cámaras analógicas se encuentra instalada en el laboratorio de computación del bloque 1 de la Unidad Educativa Luxemburgo. Consta de 4

cámaras analógicas cuyo modelo es C1030DP7 con un CMOS de 1/3".con las siguientes características

- Salida de video de 700 TVL
- 24 LED infrarrojos de alta intensidad, permite hasta 60 pies de visión nocturna.
- Una compresión de video: H.264 con doble flujo.
- Grabación de 4CIF a 30fps.
- Tipo de lente sensor de imagen CMOS LED 36pcs IR para visión nocturna.
- Posee un lente 3.6 /6mm, es resistente al agua: IP66:
- Relación señal/ruido: 50 dB.
- Alimentación: 12 VDC (Universidad de Zaragoza, 2006).

En la figura 36, se observa un diseño de la cámara con su distancia focal, anchura de la cobertura de visualización y distancia del objeto a la lente. Para calcular la ubicación de la cámara en relación a la distancia de la entrada al laboratorio, se utiliza la fórmula a continuación (Universidad de Zaragoza, 2006).

$$f = h\,x\,D/H$$

f= longitud focal

h= anchura CMOS

H= anchura del objeto a visualizar

D= distancia a la lente.

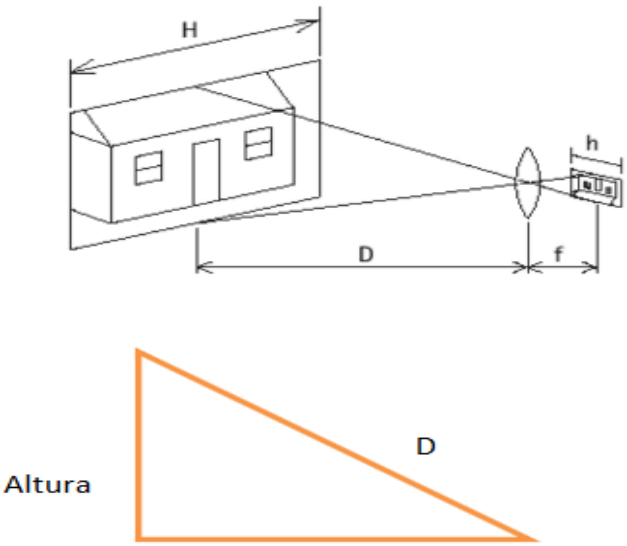


Figura 36. Diseño de visualización de las diferentes instancias de la cámara.

Fuente: El Autor.

Al seguir dicha fórmula, se utilizan los datos descritos en la misma, donde se toman consideración que el sensor de la cámara es 1/3" cuya anchura es de 3.6/6 mm y a continuación se describe el proceso: Cámara analógica, distancia focal, f= 6 mm, h (1/3") = 3.6 mm. Mientras que la anchura a cubrir es de aproximadamente 9 metros (H= 9 m) qué es lo que más o menos mide la puerta de ingreso al laboratorio, se puede calcular la mínima distancia a la que se debe colocar:

$$D = \frac{6\,mm}{3.6\,mm}\ x\ 9000\ mm = 1{,}6667\ x\ 9000\ mm = 15000\,mm = 15\ m$$

Por lo tanto, se debe colocar la cámara una distancia de 15 m con relación al objeto de vigilancia.

3.3.2. Esquema de conexión.

3.3.2.1. Sistema CCTV.

En la figura 39 se puede observar el esquema de conexión del sistema CCTV. El sistema es ISmart y cuentan con el DVR que posee su respectivo adaptador de alimentación y éste a su vez ostenta un cable con derivación para alimentar las cámaras. Las cuatros cámaras analógicas se conectan a los cuatro canales analógicos del DVR por medio del cable RG58 y los conectores BNC. En el interior del DVR se realiza la conversión analógica-digital, la compresión de los archivos y el almacenamiento. El DVR se comunica por medio del puerto Ethernet a la red privada. Para la salida de video al monitor se utiliza el cable VGA.

3.3.2.2. Sistema de control de acceso Arduino.

La figura 40 describe la distribución de los componentes que se conectan al control de acceso. En el interior del tablero de control se encuentran las tarjetas Arduino Uno, Shield y módulo relé, también está la fuente del sistema. El Arduino uno se alimentará con su adaptador de 9v, la Shield al montarse en la tarjeta de Arduino Uno no necesita tener alimentación independiente ya que el Uno le proveerá este voltaje. La alimentación del módulo relé le provee el Arduino Uno por medio de la ranura de 5V. Las alimentaciones para la caja exterior del control donde se ubica la LCD, teclado, buzzer y diodos los provee también el Uno. La fuente de poder provee de energía a la cerradura electromagnética y al ventilador del tablero. También sirve como circuito de conmutación para activar o desactivar la cerradura, ya sea por medio del pulsador manual o el circuito Arduino.

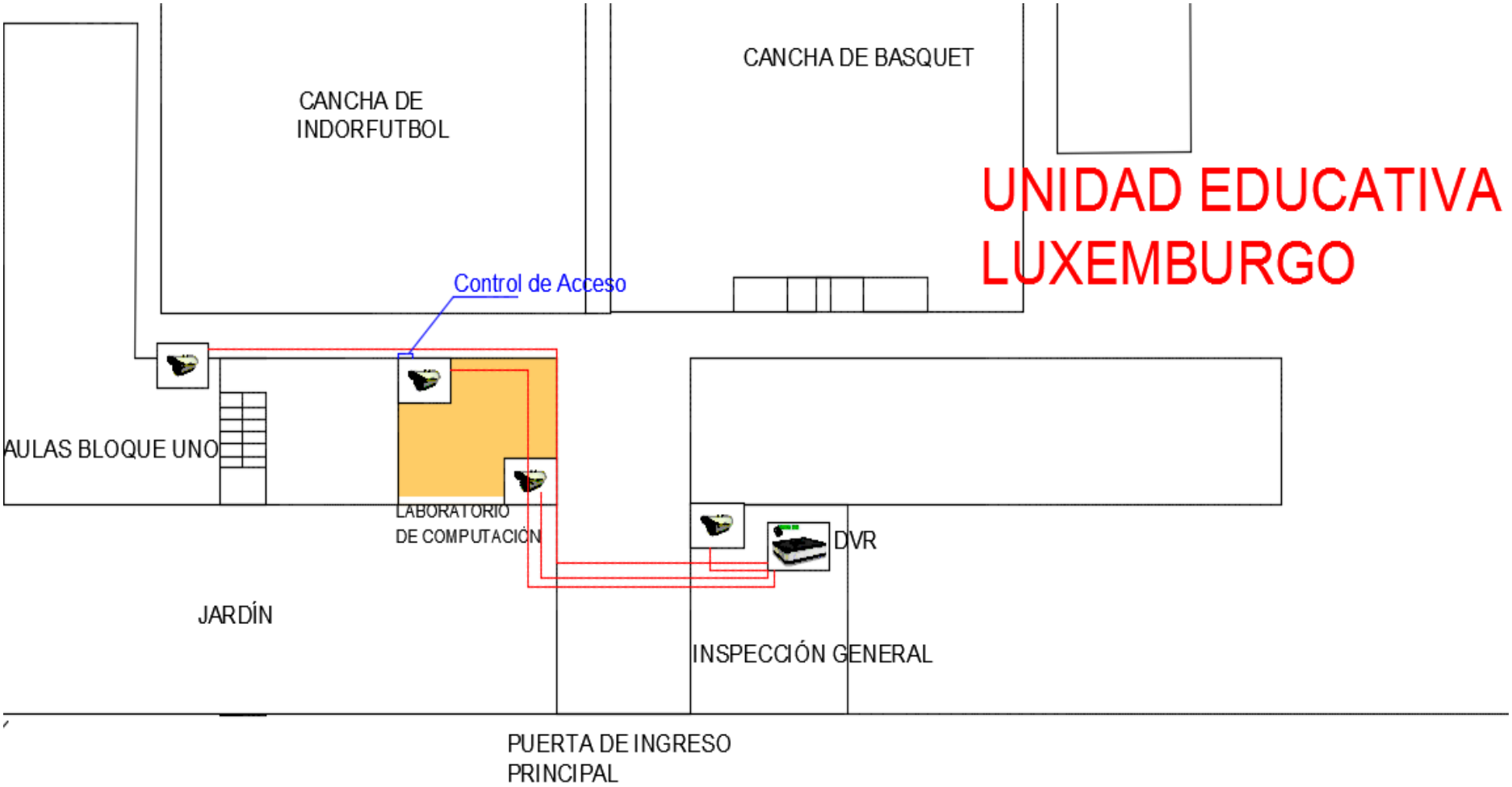


Figura 37. Esquema de distribución de las cámaras y control de acceso.

Fuente: El Autor.

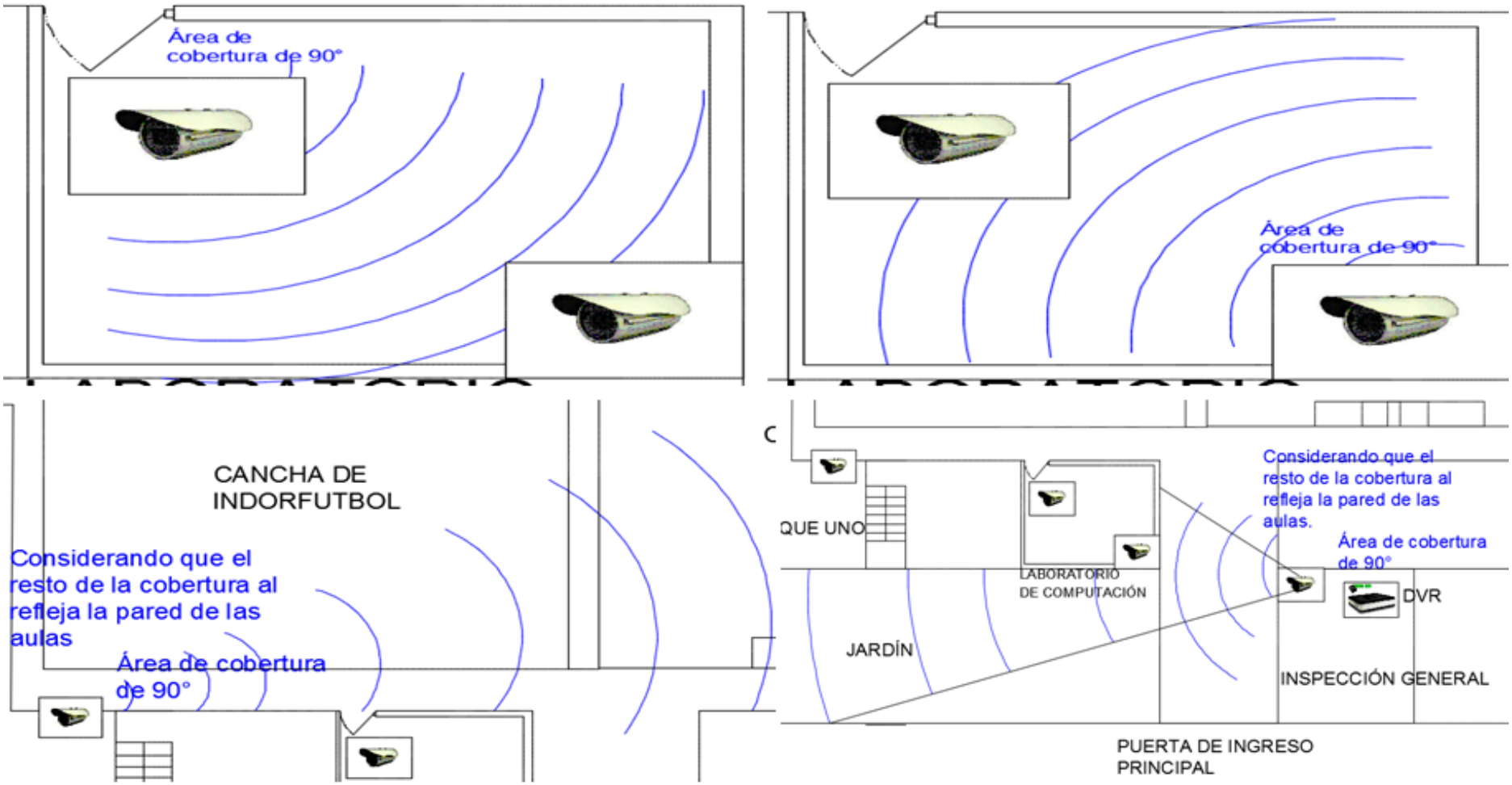


Figura 38. Área de cobertura de las cámaras de videovigilancia instaladas en la Unidad Educativa Luxemburgo.

Fuente: El Autor.

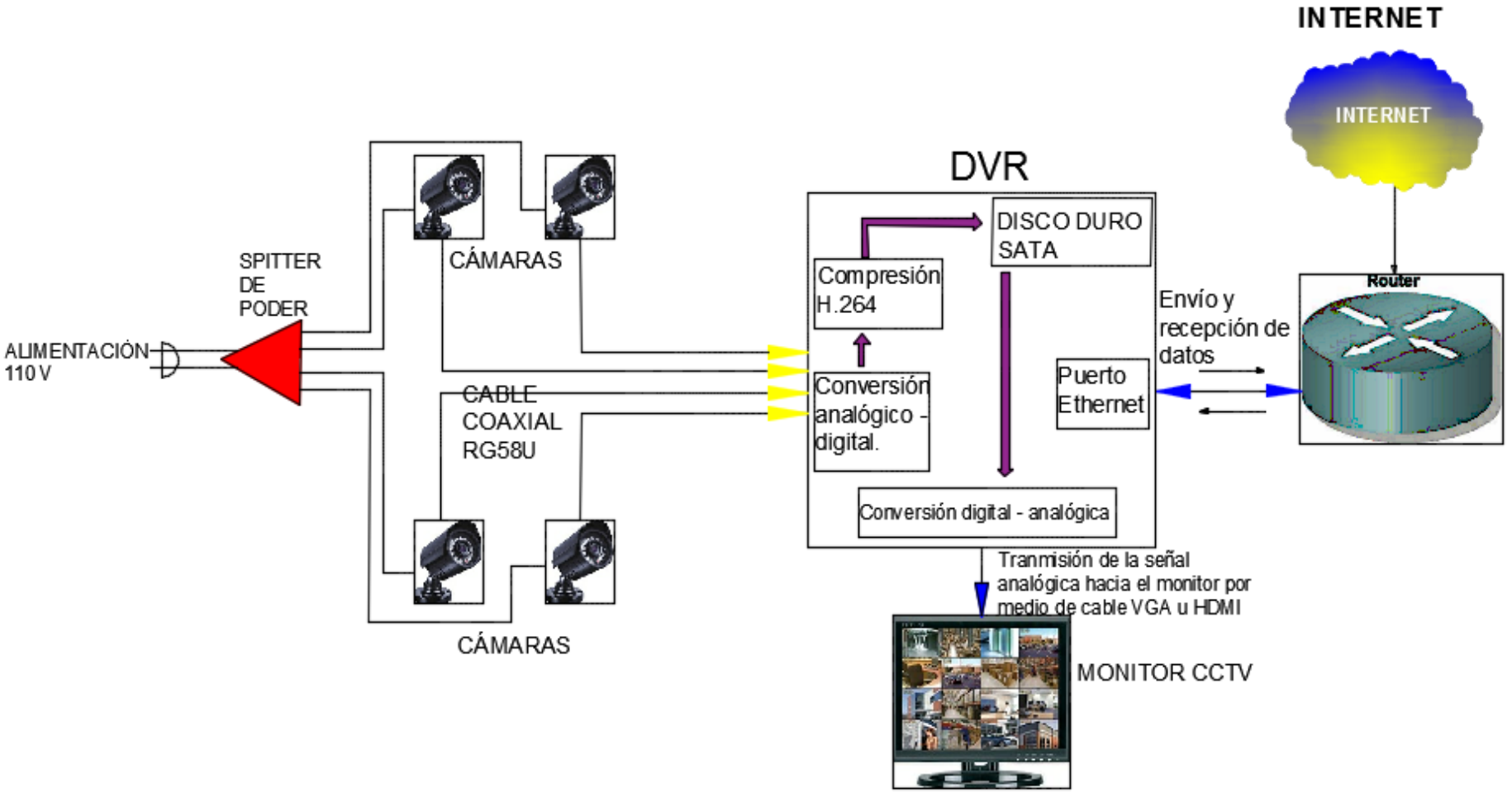


Figura 39. Diagrama de conexión del sistema CCTV con sus respectivos elementos.

Fuente: El Autor.

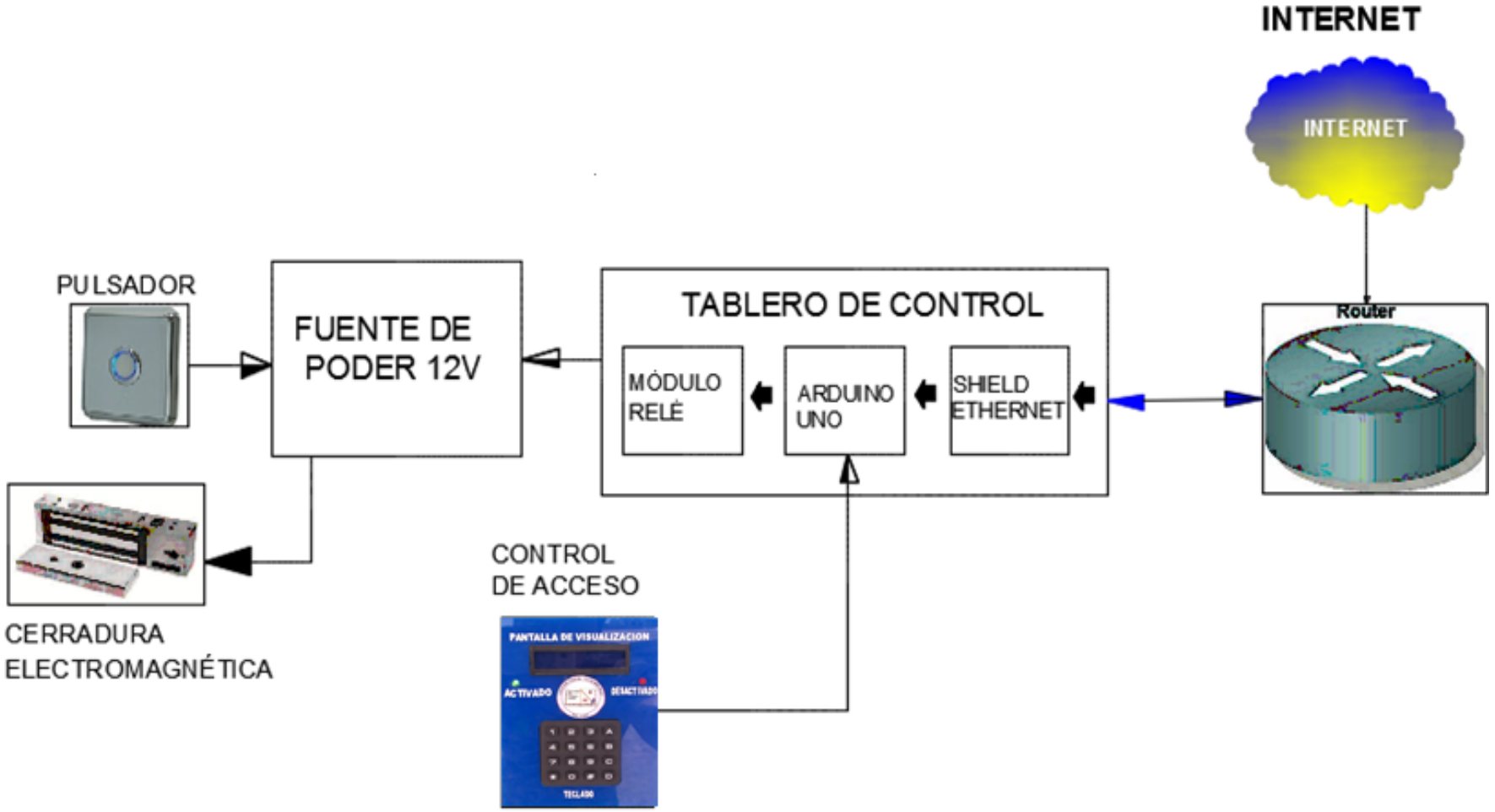


Figura 40. Esquema de conexión del control de acceso con cada uno de sus dispositivos.

Fuente: El Autor.

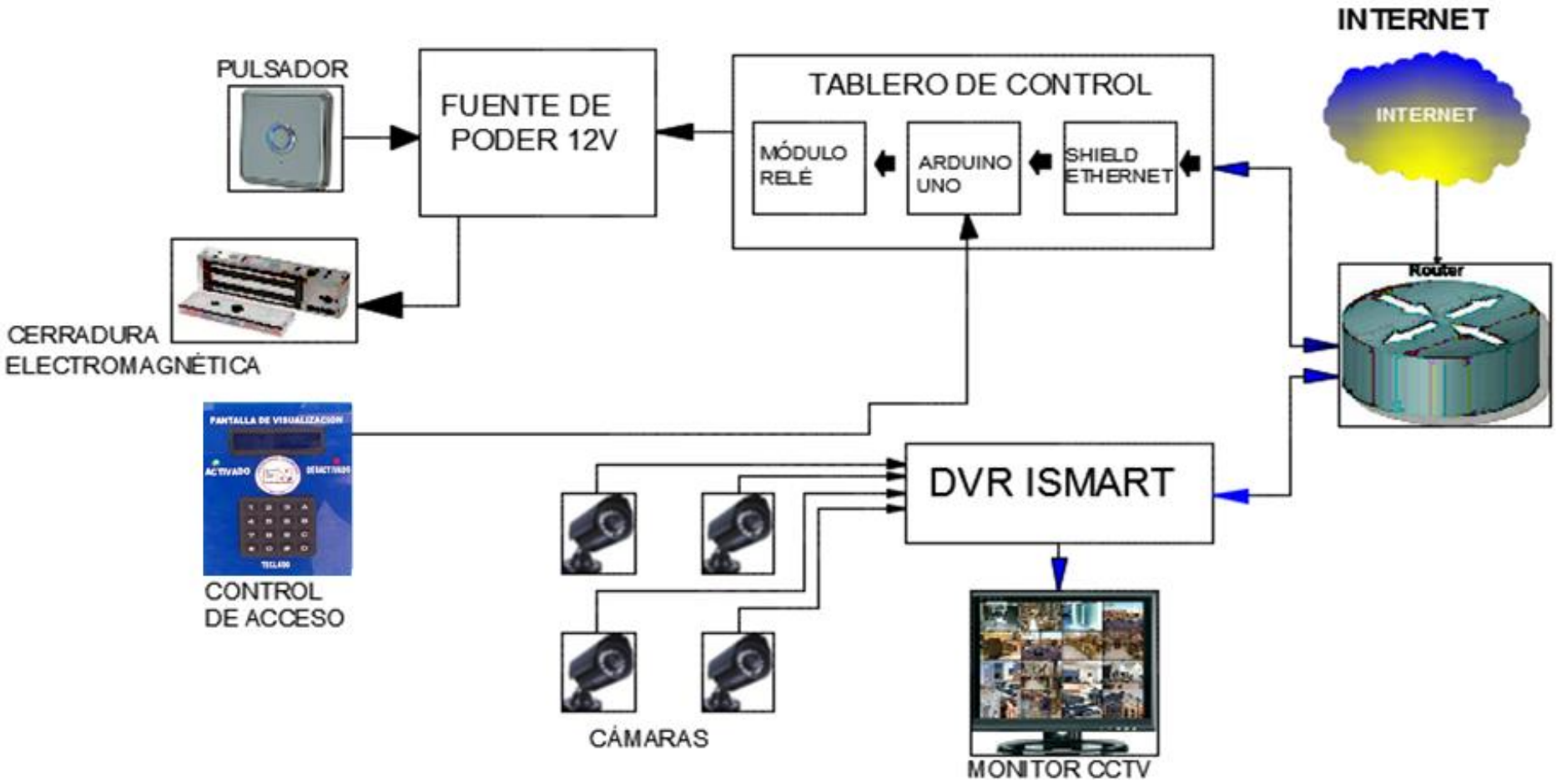


Figura 41. Esquema de conexión general del sistema de seguridad automatizado con cada uno de sus dispositivos.

Fuente: El Autor.

3.4. Implementación del sistema de seguridad automatizado de videovigilancia con Arduino.

3.4.1. Montaje del hardware.

Para el ensamblaje del sistema de seguridad interior se realizó el montaje de dos cámaras con sus respectivos cables de poder y video, mediante las investigaciones del área se pudo establecer los lugares donde irán las cámaras, con el objetivo de cubrir todos los puntos ciegos en el exterior del laboratorio de computación del bloque uno; Como lo es el acceso 1 y cancha de indor fútbol y jardín. Las cámaras instaladas se pueden observar en la figuras 42 y 43.

Figura 42. Cámara 1, pasillos del bloque 1 y escalera.
Fuente: Unidad Educativa Luxemburgo.

Figura 43. Cámara 2, ubicada sobre la inspección general.
Fuente: Unidad Educativa Luxemburgo.

Para la instalación en la parte interior del laboratorio de computación del bloque uno de la misma manera se instalaron dos cámaras con sus respectivos cables BNC y alimentación de energía para percibir todo el interior del laboratorio y custodiar los equipos como se contempla en la figura 44 y 45.

Figura 44. Cámara 3 ubicada en el interior del laboratorio con vista al rack de equipos.
Fuente: Unidad Educativa Luxemburgo.

Figura 45. Cámara 4 ubicada en el interior del laboratorio con vista a la puerta de acceso al mismo.
Fuente: Unidad Educativa Luxemburgo.

El proceso siguiente fue instalar el DVR que es el dispositivo que administra todas las señales que reciben de las cámaras, en el cual se colocó un disco duro de 320GB con un tiempo de respaldo de 1 semana para guardar todo la información de

los videos grabados y alarmas activadas. En la figura 46a y 46b y 47 se muestra la instalación.

a)

b)

Figura 46. a) Monitor y DVR instalado en el departamento de Inspección General. b) Cables de alimentación, de video (BNC), VGA, USB (mouse) y de red (puerto Ethernet).

Fuente: Unidad Educativa Luxemburgo.

Figura 47. Instalación del Disco Duro en el interior del DVR.
Fuente: Unidad Educativa Luxemburgo.

Para la instalación del DVR se colocó el cable el adaptador de corriente con un cable terminal con derivación de cuatro de pines de alimentación para las cámaras y un pin para alimentar al DVR. Así mismo se procede a colocar los cables de BNC (video) en los canales del DVR. Se observa en la figura 46b las conexiones respectivas del cableado tanto video y poder como el de la red desde el DVR hacia el router del proveedor de internet para su acceso a la misma. También se realizaron las conexiones del mouse y del monitor donde se visualizarán las Quads como se muestra en la figura 48.

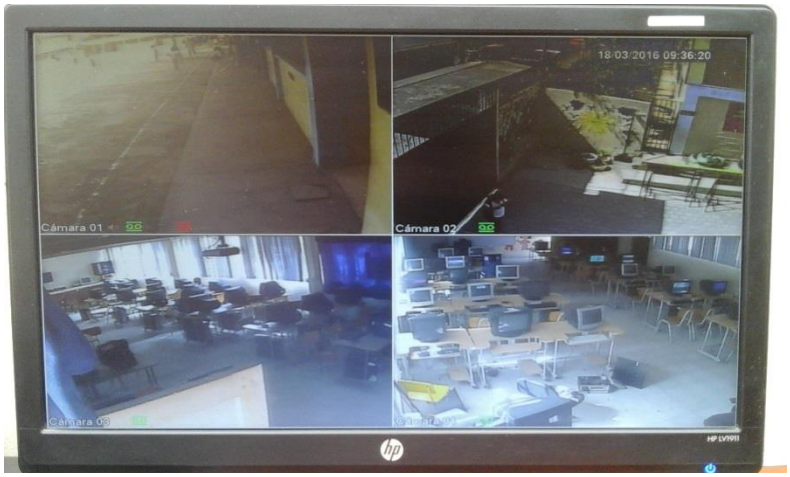


Figura 48. Activación del sistema Quads en el DVR.
Fuente: Unidad Educativa Luxemburgo.

Las conexiones realizadas entre las cámaras analógicas, el DVR y el Router en la elaboración del proyecto se presentan a continuación. El cable de alimentación con derivación de varios cables (plug macho) que proporciona energía a las cámaras y al

DVR mediante un adaptador a 110 VCA. El patchcord UTP cat.6 se lo utiliza para conectar el DVR a la red del router en cualquier de los puertos LAN libres y acceder remotamente a las cámaras desde cualquier dispositivo que esté conectado al internet.

Los cables coaxiales (conector BNC) se conectan de forma analógica y permiten transmitir la señal del video desde la cámara hacia los puertos de los cuatro canales del DVR y este a su vez lo transmite en tiempo real al internet. El cable VGA tiene la función de enviar la señal de video al monitor donde se muestra la interfaz gráfica del DVR y realizar la administración respectiva. Existen puertos USB donde se conectan los periféricos de entrada del DVR (teclado y mouse), los mismos que se utilizan para interactuar de una manera más sencilla el aspecto gráfico.

Para el montaje del control de acceso se procede a identificar en la tarjeta Arduino Uno cada uno de los pines de E/S digitales, entradas analógicas y alimentación. La tarjeta Arduino posee 13 pines de E/S digitales, 6 pines de entradas analógicas, pines de alimentación al circuito de 5v, 3.3v, GND y RESET. Posee un puerto serial que sirve de comunicación directa con la computadora y un puerto de plug hembra donde se puede alimentarlo, sin necesidad de estar conectado mediante el puerto serial a la computadora. En la figura 49 se muestra la conexión de la cerradura con el sistema del Arduino.

Posee un microprocesador ATmega328P que procesa las instrucciones que se agregan a la línea de comandos. Se construyó un array donde se guardarán los caracteres los cuales sirven para validar la contraseña de acceso.

Para visualizar los datos que se ingresan y a su vez algún mensaje de bienvenida, se procede a instalar la LCD HD44780. La misma que viene en su Shield configurado sus pines de salida y entrada. El pin 1 es el VSS y debe ir conectado a tierra para protección de la LCD. El pin 2 es el de alimentación del circuito de la LCD, el pin 3 es el pin de contraste y debe conectarse al pin 2 de un potenciómetro (preferentemente de 10KΩ), el cual debe ir configurado con un pin a la alimentación y el otro pin a tierra, para regular el contraste al gusto del ensamblador.

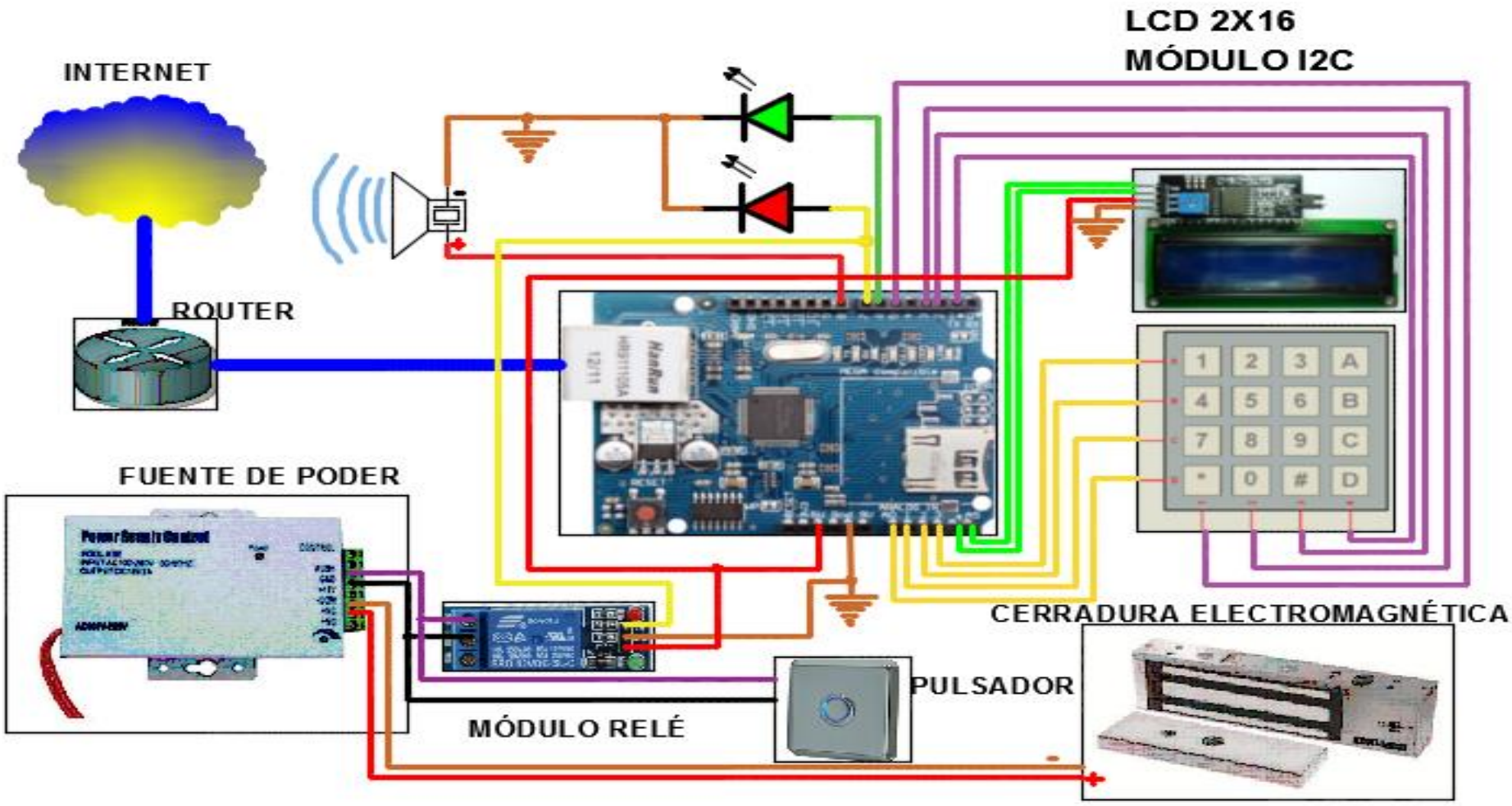


Figura 49. Diagrama de conexión del sistema de control de acceso Arduino con sus respectivos dispositivos.

Fuente: El Autor.

Del pin 4 (RS) depende si la pantalla está dispuesta a recoger instrucciones o información. El pin 5 (R/W) es el que controla la lectura y escritura cuando la pantalla envía o recibe datos. El pin 6 (E) es el de activación para poner a funcionar los pines del 4 al 5 y del 7 al 14. Los pines del 7 al 14 son la línea del bus de datos conocidas como DB0-DB7, este bus envía los bits de datos al LCD, controla la ubicación de los dígitos y los que en la pantalla se escriben. Para la retroiluminación se utilizan los pines 15 y 16, donde el 15 se debe colocarlo con una resistencia de 3.8Ω hasta 10Ω para protección (sin embargo, estas conexiones no son necesarias, en vista de que se utiliza el módulo de interface I2C) y el 16 conectado al GND.

Para tratar de ocupar menos pines del Arduino, los que serán muy útiles para las salidas de los actuadores, se utilizará un módulo de interface I2C, cuya función principal es la de conectar lógicamente todos los pines de la LCD con los del Arduino a través de las salidas SDA (línea de datos) y SCL (línea de reloj). Por medio de estas conexiones la LCD trabaja casi automáticamente con el envío y recepción de datos.

La LCD proporcionará la visualización de los mensajes de bienvenida, al igual que los caracteres que se ingresará por teclado. El Arduino Uno ya posee una librería de la LCD para agregarlo en sus instrucciones y permitirá una administración optimizada de sus pines.

El teclado 4 X 4 es un dispositivo electrónico de entrada que proporciona un ingreso de un dato específico en el Arduino, el mismo que lo procesará y lo mostrará mediante la LCD. Posee un conjunto de 16 teclas (8 pines) que van configuradas en un estilo de 4x4 (4 filas y 4 columnas). En la figura 50 se observa la configuración de las teclas de acuerdo al uso en este proyecto. Los 4 primeros pines son los que controla las filas y los 4 siguientes las columnas. Se puede poner un ejemplo, al presionar la tecla “1” se cerrará el circuito de la fila 1 con la columna 2 y mediante el Arduino y su librería Keypad se procesará que esa conexión pertenece a la tecla 1 y se visualizará el 1 en la pantalla. Su forma plana y pistas conectadas a un grupo de cables tipo buses, optimiza el espacio de la caja dónde se ubicará el circuito de entrada y salida que interactúe con el usuario.

Al utilizar el módulo de interface I2C, los pines PWD y el resto de entradas analógicas quedan libres para utilizarlas. Por lo tanto, se puede utilizar las cuatro entradas analógicas para las filas del teclado y 4 pines digitales como entradas para

las columnas del teclado. Así puede tener libre 3 pines que son necesarios para activar el LED indicador de activación, el LED indicador de desactivación de la cerradura electromagnética y por último el buzzer que genera sonidos (pitidos) como indicador que se digita una tecla.

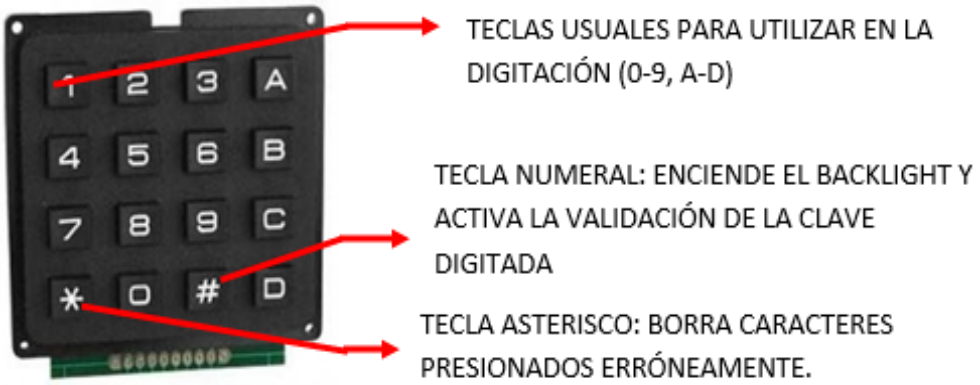


Figura 50. Teclado 4x4 con la respectiva función de las teclas.
Fuente: (Tecno Store, 2014).

Al momento de que el circuito se encuentre implementado y se proceda con el arranque del mismo, estará encendido un LED verde (pin salida digital 8), que indicará que la cerradura electromagnética está activada y la pantalla LCD estará apagada. Luego se teclea el botón de "#" para encender la LCD (este paso es necesario para entrar en modo de ahorro de energía al momento de mantener encendida la LCD sin utilizarla). Una vez que aparezca el mensaje de inicio "U. E. LUXEMBURGO", "DEPT COMPUTACION" y por último "INGRESE CLAVE", se ingresará por teclado la contraseña (guardada por defecto internamente y constará de 6 dígitos entre números y letras). Mediante el Arduino Uno se validará caracter por caracter con los que tengan almacenados en el array tipo char (caracter) y así se constatará que la cadena de caracteres sea la correcta y mediante un pulso en la salida digital 9 se activará un relé, el cual a su vez desmagnetizará una cerradura electromagnética de 480 libras fuerza, y permitirá que la puerta se abra sin prejuicio alguno. Durante el proceso de ingreso de carácter por carácter se emitirá un tono que indicará que se digitó una tecla.

Como se mencionó anteriormente el circuito de activación con el relé realiza el trabajo de conmutación, por motivos de dimensionamiento se decidió incluir un módulo relé de Arduino para realizar éste trabajo.

El módulo de relé que se utilizará contiene dos entradas para activar dos relés, pero se puede encontrar módulos con más relés, lo que se necesite para los diferentes

proyectos. El esquema de conexión realizado en el programa de diseño electrónico Electronics Workbench v5.12 que se representa en la figura 51. Donde se necesita una fuente de alimentación de 5v (suficiente con la que genera el Arduino) fuente que en conjunto con el pulso de la salida digital 9 del Arduino activa al optoacoplador, que de forma óptica utiliza un diodo LED envía un pulso de luz, dicho pulso al pasar por un fototransistor en modo de saturación, se traduce en una pequeña corriente, la misma que ingresa a la base de transistor y que puede cambiar de su estado de corte al de saturación, y puedan conectar dos circuitos a manera de interfaz. De esta modo quedan unidos ópticamente, por motivos de protección del circuito se implementa una resistencia de un valor elevado (se habla de MΩ).

Una vez que esto ocurre el electroimán induce a una platina para que cambie de posición (proceso de conmutación) y así conectar el elemento que funcione a través de este sistema. Para realizar toda esta conexión se necesita realizar un cálculo para aplicar una resistencia a la corriente de base.

Para saber que resistencia de base se necesita, se debe verificar que ganancia de corriente (hFE) tiene el transistor (ver datasheet) que se va a utilizar, en este caso el módulo relé cuenta con un transistor NPN J3Y con una hFE = 120 (para este caso se utilizó el valor mínimo). A parte de éste valor se necesita el voltaje del microcontrolador (Arduino) y la corriente que consume el circuito a encender o apagar y el valor de voltaje de diodo (silicio). Entonces se aplica la fórmula siguiente:

$$R_B = \frac{Voltaje_{micro} - 0{,}7}{\frac{Corriente}{hFE}}$$

$$R_B = \frac{5\,V - 0{,}7\,V}{\frac{500\,mA}{120}} = \frac{4{,}3\,V}{0{,}00417\,A} = 1031{,}175\,\Omega = 1\,K\Omega$$

$$= 102\ (en\ caso\ de\ montaje\ superficial)$$

Con éste cálculo se puede colocar una resistencia entre la salida del optoacoplador y la base del transistor, con la finalidad de reducir la corriente de base que circula por el circuito, porque la corriente de base debe ser 100 veces menor a la corriente de colector. Adicional se debe colocar un diodo rectificador en paralelo con el electroimán del relé, de forma que sirva como protección de cortocircuitos.

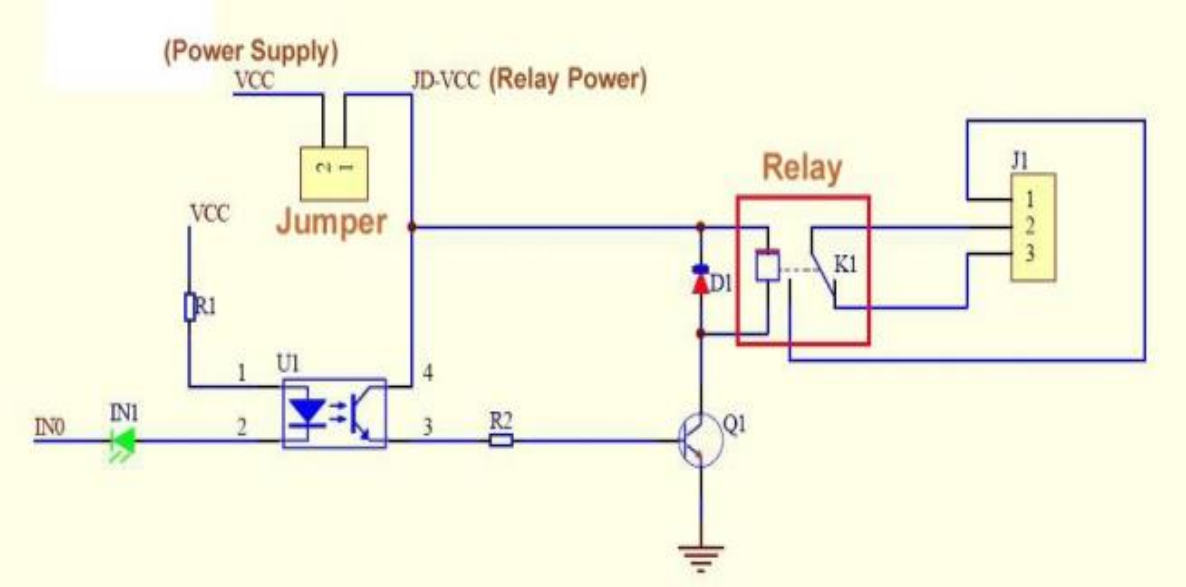


Figura 51. Diagrama esquemático de un módulo relé.
Fuente: (Álvarez, 2014).

En la figura 52, se puede observar un módulo relé de 2 entradas, se puede apreciar los elementos de 4 pines de forma rectangular que son los optoacopladores, los transistores NPN, condensadores y las resistencias de base (todos de montaje superficial), que en conjunto realizan el trabajo de conmutación del módulo.

Figura 52. Módulo Relé Arduino de 2 entradas.
Fuente: (Álvarez, 2014).

La cerradura electromagnética se constituye de dos elementos: una lámina metálica y un electroimán. En la figura 53 se observa la cerradura con sus partes principales. El electroimán (que se encuentra asegurado en el marco de la puerta) es de tipo “Fail Safe” el cuál al momento de recibir una alimentación de la fuente, éste se magnetiza y atrae a la lámina de metal que está afianzada en la puerta. Mientras tanto, si no tiene alimentación alguna, se desmagnetizará. Este dispositivo además posee un

pulsador tipo timbre que ayudará a desmagnetizar a la cerradura manualmente desde el interior para abrir la puerta sin necesidad que la acción se la ejecute desde afuera, como la figura 54 representa.

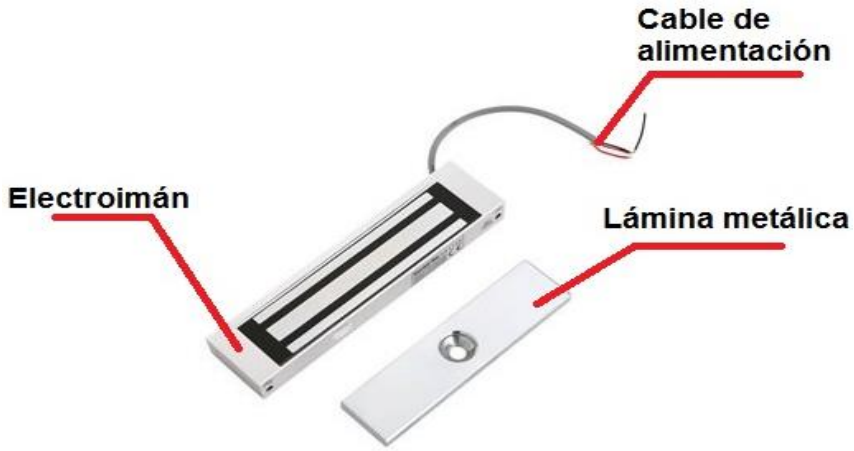


Figura 53. Cerradura electromagnética y sus partes.
Fuente: El Autor.

Figura 54. Cerradura electromagnética instalada en la puerta de acceso del laboratorio con el pulsador de apertura.
Fuente: Unidad Educativa Luxemburgo.

Al momento que se realicen las pruebas respectivas con el Arduino Uno, se proviene a montar el Arduino Ethernet Shield. Para afirmar que el módulo Ethernet W5100 se restituya cabalmente en el encendido, se incluye en el escudo y

administrador de reajuste. Este dispositivo pertenece a la plataforma Arduino y permite acceder a la red mediante su puerto RJ45. El escudo también incluye un controlador de reajuste, para asegurar que el módulo Ethernet W5100 se restablece correctamente en el encendido. Se diseña un modelo de suministro a través de Ethernet (PoE), que el escudo incluye, para obtener energía de un cable Ethernet de par trenzado:

- IEEE802 .3af compatible
- Ondulación baja producción y el ruido (100mVpp)
- El nivel de voltaje de entrada es de 36V a 57V
- Sobrecarga y protección contra cortocircuitos.
- 9V de salida
- Convertidor de alta eficacia DC / DC: typ 75% @ 50% de carga
- Puede tener un aislamiento de la entrada a la salida a un voltaje de 1500 v.

Al momento de montar la Shield en el Arduino Uno, existen componentes muy útiles que posee, son los pines de conexión del bus ICSP (*In Circuital Serial Programming:* En el circuito serial programable). Para la comunicación del W5100 y una tarjeta microSD, Arduino usa el bus SPI (por medio de su cabecera) con los pines digitales 10, 11, 12, y 13 El pin 10 se usa para distinguir el W5100 y para la tarjeta microSD se utiliza el 14, por lo tanto, si no se usa la ranura para la tarjeta microSD, se debe declarar en el código como salida, para así no tener complicaciones en el trabajo del sistema por el motivo que se necesita esa salida para el buzzer. Los pines digitales 0 y 1 son para transmisión y recepción (TX y RX), así que, se evitará utilizar esos pines para no tener problemas con la comunicación de la PC con el Arduino.

Para el reinicio se oprime el pulsador en el escudo para restituir la placa Arduino y el W5100. Una ventaja de la Shield de Ethernet Arduino es que de hecho se debe montar en el Arduino Uno y los pines coinciden exactamente en todas las ranuras, se describe en la figura 55 el montaje de la Shield de Ethernet Arduino con el Arduino Uno. De manera que la configuración del Arduino Uno no sufra ningún cambio en sus salidas digitales, simplemente la ubicación de las conexiones estarán en la Shield Ethernet Arduino tanto de la LCD, el teclado 4x4 y la salida de interface con la cerradura electromagnética.

Figura 55. Montaje del Arduino Ethernet Shield en el Arduino Uno.
Fuente: El Autor.

En la figura 56 se muestra la Shield del Arduino Ethernet en comunicación con la red de internet. Se considera que el router establece una conexión importante con la red, porque al configurar la placa Arduino Ethernet se tiene la elección de un IP fija y no trabaja por DHCP. Como la red privada de la institución posee un sistema de asignación de IP estática, se configura una al Arduino. De modo que si existe algún cambio de energía o reinicio del dispositivo, se conectará con la misma IP a la red.

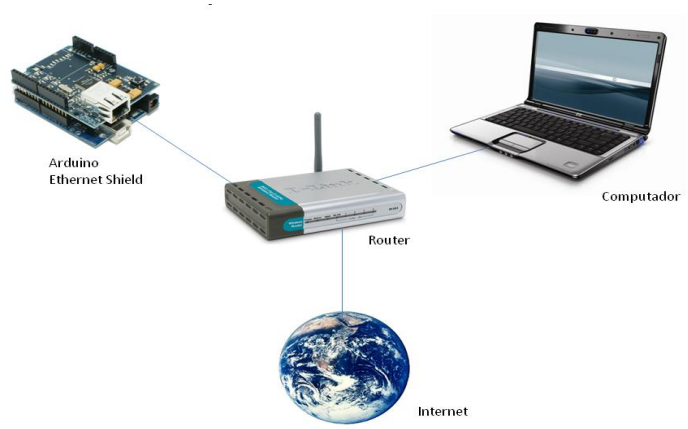


Figura 56. Esquema de conexión del Arduino Ethernet Shield con la red de internet.
Fuente: (Duarte, 2013).

Los pines de la tarjeta Arduino Ethernet-UNO que se utilizaron para la conexión entre la LCD, el teclado y el router y el DVR, en la elaboración del proyecto con su respectiva configuración se presentan a continuación:

- Los pines analógicos (A0-A3) y los pines digitales (3,5 - 7), están configurados para las entradas por teclado (4x4) como lo representa a figura 30.

- Los pines A4 y A5 (SDA y SCL respectivamente), se conectan al módulo de interface I2C y éste a su vez con los 16 pines de la LCD, con el fin de ahorrar pines para utilizarlos con los actuadores.
- El módulo I2C viene incorporado con un potenciómetro ajustable “trim” que sirve de mucha ayuda para ajustar el contraste de la pantalla.
- Pin 9, a éste pin se conecta el LED rojo indicador de desactivación y el módulo relé que recibe el pulso de la salida del Arduino. Al momento que la salida de éste pin esté en alto, energice el relé y desactive el electroimán de la cerradura electromagnética y retire las seguridades de la puerta.
- Pin 8, a éste pin se conectará el LED verde indicador que la cerradura está activada, por lo tanto sólo cuando el pin de salida 9 de módulo Arduino esté en alto este cambiará su estado a bajo (LOW).
- Pin 5v, alimenta al módulo relé, la LCD, el buzzer y los diodos indicadores, en sí a todo el circuito conformado por el Arduino, sin considerar a la cerradura que tiene su propia fuente de alimentación.
- Pin GND, proporciona el chasis para la protección de los diferentes dispositivos acoplados al Arduino, por lo tanto se conecta a éste pin todos los negativos de los circuitos, tanto los ánodos de los diodos como el GND del módulo relé y el de la LCD.

En la figura 49 se muestra el esquema de conexión del Arduino con el periférico de entrada (teclado 4x4), de salida (LCD) y el router. Se observa que el Arduino Ethernet Shield ya se encuentra ensamblado sobre el Arduino Uno.

Al momento que se realizó las pruebas correspondientes se procedió a implementar el sistema en el interior del laboratorio. Para ello, se colocó una caja metálica donde se alojarán todos los dispositivos que intervienen en el control (Placa Arduino Uno, Shield Ethernet, fuentes de poder, módulo relé y tomas de alimentación de 110v. Dicha caja se encuentra adecuada para fijar a cada dispositivo. Adicionalmente se coloca un ventilador de 12v para conservar la temperatura adecuada en el interior y así evitar que los dispositivos se calienten y pueda existir algún deterioro. Demuestra la figura 57, la caja de control implementada con los diferentes dispositivos en su interior.

Figura 57. Tablero de control de la puerta de acceso implementada en el interior del laboratorio.
Fuente: Unidad Educativa Luxemburgo.

3.4.2. Montaje de software.

3.4.2.1. Configuración software CCTV.

Al momento que se encuentra el hardware del sistema CCTV instalado, se debe configurar el DVR para su conexión a internet, grabación y generación de alarmas. El primer paso, se ingresa al menú principal con un clic derecho al mouse del sistema. Para ingresar a la configuración del sistema se debe ingresar en modo administrador y la contraseña respectiva.

También se realiza las configuraciones respectivas para lograr el trabajo de las cámaras en conjunto con las aplicaciones Android (válido sólo cuando se posea en la red de internet una IP pública) y el programa de acceso remoto para administrar desde el internet con la validación de un usuario. Para acceder a la red mediante DHCP o con IP estática, se estableció algunos parámetros importantes como se representa en la figura 60, configuraciones de almacenamiento, alarmas, duración de las grabaciones en la figura 59 se demuestra, administración de cuentas de usuario, etc. Como se muestra en la figura 58, la configuración del P2P para que la aplicación IMSeye tenga conexión con el DVR y observar la captura de las cámaras incluso

configurar en la misma aplicación, las alarmas correspondientes conforme a la sensibilidad del movimiento.

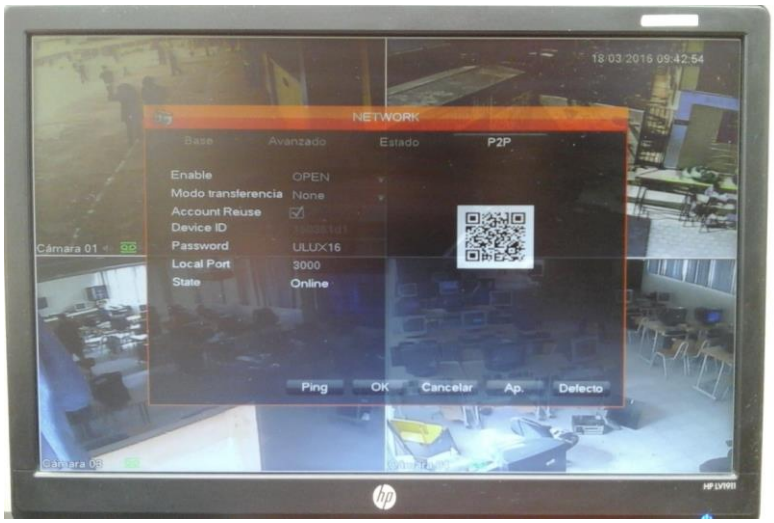


Figura 58. Configuración P2P en el DVR.

Fuente: Unidad Educativa Luxemburgo.

Figura 59. Configuración en el DVR para el acceso al internet.

Fuente: Unidad Educativa Luxemburgo.

Figura 60. Configuración para la grabación de las cámaras.
Fuente: Unidad Educativa Luxemburgo.

3.4.2.2. Configuración del Software HTML para la cerradura electromagnética.

En la Shield Ethernet Arduino se puede colocar código HTML (página web) y se agrega automáticamente en la web y mediante la IP asignada a la Shield se puede acceder a dicha página. En el proyecto se creó una página en la cual manejará la desactivación y activación remota de la cerradura electromagnética desde cualquier dispositivo que se encuentre conectado la red (puede ser privada o pública), en la figura 62 se puede observar la página que se creó para manejar la cerradura remotamente. Los botones del código HTML están configurados para dar una instrucción al Arduino Ethernet respecto a la señal que recibió enviará mediante el Arduino Uno una acción que activará la cerradura electromagnética.

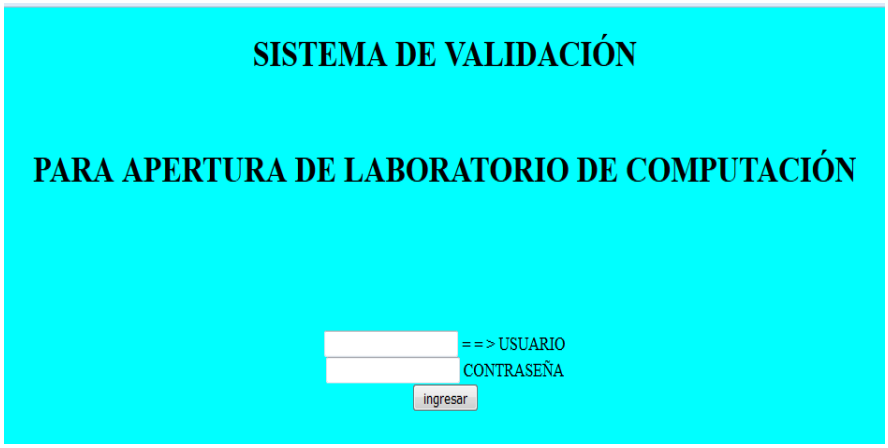


Figura 61. Formulario para validar el acceso a la página de control del acceso al laboratorio de computación.
Fuente:El Autor.

Como el acceso al laboratorio es restringido para personas particulares y cierto personal ajeno al área de computación, se crea un programa para que valide un usuario y contraseña para acceder al control de apertura y cierre de la puerta. En la figura 61 se observa la creación de un método que valide un usuario y la contraseña que está cifrada, con este fin que al momento de su digitación no se podrá observar que caracteres se ingresaron. Todo estas instrucciones fueron creadas en formularios JavaScript. Una vez que la validación sea la correcta le redireccionará a una página donde se administrar la apertura y cierre de la puerta del laboratorio de computación como en la figura 52 se observa.

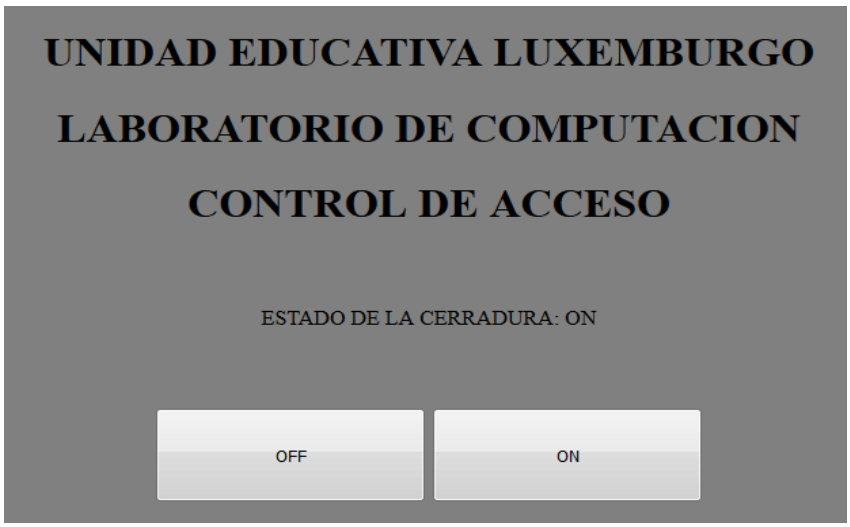


Figura 62. Página creada para la administración remota del control de acceso Arduino. Fuente: El Autor.

Se observa que en la página HTML existen dos botones “OFF” y “ON”, cuya función es activar y desactivar la cerradura electromagnética. Así mismo un cuadro de texto que indica el estado de la cerradura, con el fin de conocer si la cerradura está activada o desactivada. Y un cuadro de texto de información que identifica que sistema es, a qué lugar e institución pertenece.

Esta acción aprueba que el usuario posea una administración más ordenada del acceso al laboratorio. No solo con la contraseña, si no también remotamente mediante el manejo de las cámaras y el código HTML en la red de internet. Si el administrador del control de acceso reconoce al usuario que pretende ingresar mediante la cámara ubicada lo más cerca a la puerta de ingreso al laboratorio puede autorizarle el ingreso remotamente, con la pulsación del botón de encendido de la cerradura electromagnética.

3.4.3. Pruebas de funcionamiento.

3.4.3.1. Prueba 1. Generación de alarmas por detección de movimiento.

Para la prueba 1 se configura la detección de movimiento en el DVR con la finalidad de generar notificaciones automáticas, para esta prueba se establece el nivel de sensibilidad en “mayor”.

Al instante que se guardan los cambios, los mensajes de alarma en el software ISmart llegan con éxito, pero llegan demasiadas notificaciones de alarma, sin existir una verdadera localización de movimiento como en la figura 63 se demuestra.

Figura 63. Detección de movimiento en sensibilidad ajustada a nivel de “mayor”.
Fuente: Unidad Educativa Luxemburgo.

Para la segunda parte de la prueba se baja el nivel de sensibilidad en nivel medio y los mensajes dejan de llegar de forma reiterada como en la figura 64 se observa y estos solo llegan cuando verdaderamente existe movimiento en las zonas monitoreadas. En la tabla 7, se observa la cantidad de alarmas generadas en el modo de alarma mayor y medio.

Figura 64. Detección de movimiento en sensibilidad ajustada a nivel “media”.
Fuente: Unidad Educativa Luxemburgo.

Tabla 7. Evaluación de las alarmas de acuerdo a la sensibilidad configurada en el DVR.

N°	NIVEL DE SENSIBILIDAD	ALARMAS IMSeye 200	Alarma	Periodo de tiempo
1	Mayor	8	Falsa	09:00 a 11:00
2	Media	1	Verdadera	11:00 a 13:00

Fuente: Unidad Educativa Luxemburgo.

3.4.3.1.1. Análisis de resultados.

La primera prueba consistió en habilitar la detección de movimiento en las cámaras para que se generen alarmas automáticas en el sistema y puedan llegar a la aplicación móvil o de escritorio. Sin embargo al configurar el nivel de sensibilidad con un valor de referencia “mayor” el sistema genera alarmas falsas, para corregir el inconveniente se cambia el nivel de sensibilidad al valor referencia “media”, y el sistema responde manera correcta con la generación de alarmas verdaderas, solo si existe la presencia de movimiento en las zonas monitoreadas.

En la activación manual y automática el sistema reconoció las alarmas sin inconvenientes. Sin embargo para el ajuste automático fue necesario regular el nivel de sensibilidad en la localización de movimiento de las cámaras, para que no se generan en el sistema falsas alarmas.

3.4.3.2. Prueba 2. Grabación de video en base a la configuración DM (Detection Motion: detección de movimiento).

Antes de configurar el modo de grabación se configura el canal de video a una resolución óptima, en la cual la calidad de video y la compresión se mantenga como se muestra en la figura 65. Esta prueba consiste en configurar los parámetros de grabación en modo detector de movimiento. Es decir, cada momento que se produce un movimiento y la cámara lo percibe el sistema del DVR detecta ese movimiento y automáticamente por medio de algoritmos se produce el almacenamiento de ese instante en el disco duro. Cuantas veces haya movimiento en el lugar monitoreo, esas veces el DVR grabará el video captado. En la figura 66 se muestra la opción de configuración de grabación en interior del canal 1.

Figura 65. Configuración de la calidad del video en cada canal.
Fuente: Unidad Educativa Luxemburgo.

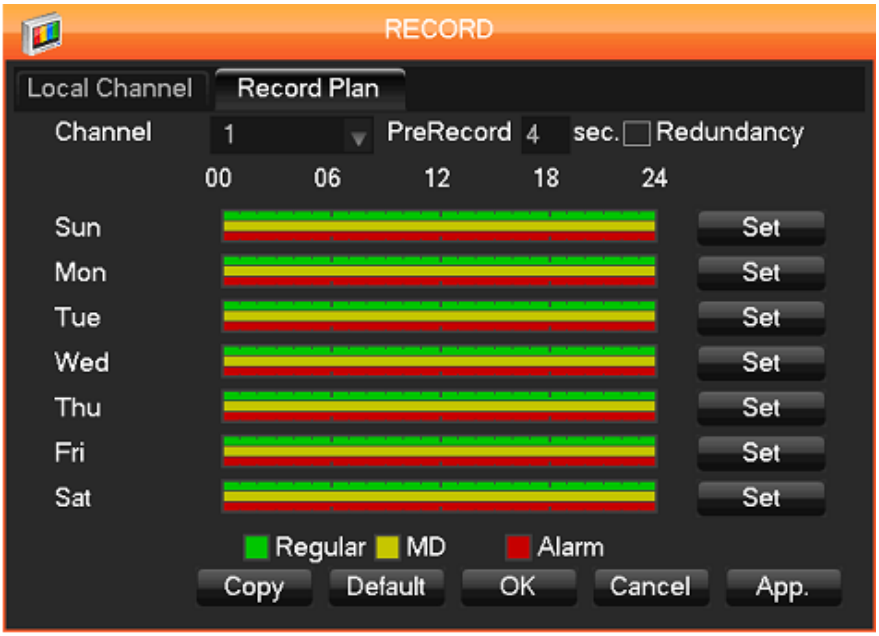


Figura 66. Visualización del control de grabación por medio de configuración Regular y DM.

Fuente: Unidad Educativa Luxemburgo.

3.4.3.2.1. Análisis de los resultados.

Al realizar la configuración de modo Detección de Movimiento se logró comprobar la cantidad de almacenamiento que se ahorra un DVR en comparación con la grabación Regular que almacena el video en el disco duro en todo momento. En la tabla 8 y 9, se muestra las pruebas realizadas en modo regular en comparación con las realizadas en modo DM.

Tabla 8. Medición del consumo de espacio de almacenamiento en el disco duro con la utilización del modo de grabación regular.

Fecha	Cantidad de espacio utilizado	Canales utilizados	Modo de configuración	Horario de grabación	Tiempo grabación
06/09/2016	3,67 GB	Canal 1	Regular	12:00 a 16:00	4 horas
	14,67 GB	4 canales simultáneos		16:00 a 20:00	4 horas

Fuente: Unidad Educativa Luxemburgo.

Tabla 9. Medición del consumo de espacio de almacenamiento en el disco duro con la utilización del modo de grabación DM (Detection Motion).

Fecha	Cantidad de espacio utilizado	Canales utilizados	Modo de configuración	Horario de grabación	Tiempo grabación
07/09/2016	2,48 GB	Canal 1	DM (Detection Motion)	08:00 a 12:00	4 horas
	9,92 GB	4 canales simultáneos		12:00 a 16:00	4 horas
	0,05 GB	Canal 1		17:00 a 21:00	4 horas
08/09/2016	0,20 GB	4 canales simultáneos		17:00 a 21:00	4 horas

Fuente: Unidad Educativa Luxemburgo.

Como se observa en las tablas 8 y 9, el consumo de MB por los videos almacenados en el disco cuando se configura el modo DM es menor en consideración al modo regular donde las cámaras graban todo el tiempo. Se realizó unas pruebas en el horario donde no existe movimiento y prácticamente se ahorra 14,47MB (un aproximado del 98% del almacenamiento en ese horario). Con estos resultados se concluye que el tiempo de almacenaje en el disco duro con el modo DM se duplica. Si la duración del disco duro de 320 GB instalado en el DVR de la Unidad Educativa Luxemburgo es de aproximadamente 14 días, configurado el DVR en DM el disco duro se saturaría en 28 días.

3.4.3.3. Prueba 3. Consumo de energía del UPS en caso de ausencia de la energía de la red eléctrica de la Unidad Educativa Luxemburgo.

El centro de control del sistema CCTV se encuentra ubicado en la oficina de Inspección General de la Unidad Educativa Luxemburgo. Por lo tanto, toda la suministración de energía la realiza la red eléctrica del lugar. Sin embargo, existe un UPS backup cuando ocurran cortes de energía inesperados. El UPS suministra energía a un ordenador, 2 monitores (CCTV y computador) y el suministro personal de energía (cargador) del DVR y las 4 cámaras analógicas. A continuación en la tabla 10 se muestra las especificaciones técnicas del UPS.

Tabla 10. Especificaciones técnicas del UPS APC instalado en la Unidad Educativa Luxemburgo.

Especificaciones No-Breaks y UPS	
Tipo de conexión de entrada UPS	NEMA 5-15P
Capacidad de salida voltios amperios (VA)	550 VA
Capacidad de salida Watts	330 Watts
Salida Nominal de Voltaje	120 V
Cantidad / Tipo de Salidas	- 4 x NEMA 5-15R (Respaldo de batería) - 4 x NEMA 5-15R (Protección contra sobretensiones)
Tipo de Batería	Batería sellada de plomo sin necesidad de mantención con electrolito suspendido: a prueba de filtración
Tiempo de Recarga de Batería	24 horas
Cartucho de Repuesto (Batería)	APCRBC110
Protección de Línea de Datos	Línea de teléfono analógica para teléfono/fax/módem/DSL
Filtrado	Filtrado completo de ruidos multipolares
Alarma	Alarma de batería encendida: alarma distintiva de carga de batería baja: alarma de sobrecarga de tono continuo
Panel de Control (LED o Pantalla)	Visualizador de estatus LED en línea
Puerto de Interfaz	USB
Normas Ambientales	RoHS
Características Físicas	
Dimensiones	84 x 305 x 178 mm
Peso	5.91

Fuente: (PCEL, 2013)

La batería que contiene el UPS es una seca de 12V a 3Ah (Amperios-hora). Esta información es muy importante para saber el tiempo que dura el suministro de

energía a todas las cargas conectadas al UPS. Por lo tanto, se realiza el estudio de cargas del UPS. Lo cual se muestra a continuación en la tabla 11.

Tabla 11. Estudio de cargas de los dispositivos conectados al UPS.

Cantidad	Nombre del dispositivo	Consumo de corriente (Amp)		Voltaje de trabajo (V)	Potencia (W)	
		unidad	total		unidad	total
1	PC de escritorio	1,6 máximo	1,6	120	150	150
2	Monitor HP 20”	0,5 máximo	1	120	25	50
1	Cargador sistema CCTV ISmart (DVR y 4 cámaras analógicas)	1 máximo	1	120	85	85
Total consumo (W):						285

Fuente: Unidad Educativa Luxemburgo.

3.4.3.3.1. Análisis de los resultados.

Para calcular el consumo de corriente total de las cargas se aplica la Ley de Ohm. No se considera la corriente descrita en la tabla porque es un valor nominal.

$$CT = \frac{Pt}{E} = \frac{285\ w}{120\ v} = 2{,}375\ Ah$$

Donde:

CT: Corriente total de las cargas del UPS.

Pt: potencia total de consumo.

E: Voltaje de suministro del UPS.

Para que se prolongue el tiempo de duración de la batería (no utilizar a la máxima capacidad de la batería) se debe obtener un porcentaje de eficiencia. Para conocer la eficiencia de la batería perteneciente al UPS de estudio se debe calcular lo siguiente:

$$C_{sal} = \frac{P_{sal}}{E_{sal}} = \frac{330\ w}{120\ v} = 2{,}75\ Ah$$

$$Eff = \frac{C_{sal}}{C_{nom}} = \frac{2{,}75\ A}{3\ A} = 0{,}92$$

$$Eff = 0{,}92 = 92\ \%$$

Donde:

Csal: Corriente de salida del UPS.

Psal: Potencia de salida del UPS.

Esal: Voltaje de salida del UPS.

Eff: eficiencia de carga de la batería del UPS.

Conm: Corriente nominal de la batería.

Calculo del tiempo de suministro de energía para las cargas:

$$C_{\Delta} = \ C_{Batt} - C_{consumo} = 2{,}75\ Ah - 2{,}375\ Ah = 0{,}375\ Ah$$

Donde:

CΔ: Diferencia que existen entre el consumo de las cargas del UPS y la corriente de la batería que puede suministrar el UPS.

Cbatt= Corriente eficiente de la batería.

Cconsumo: Corriente de consumo de las cargas del UPS.

Está entendido que el consumo de corriente de las cargas durante 1 hora es de 2,38 A. Sin embargo el consumo total que provee la batería es de 2,75. Por lo tanto, se realiza la conversión del resta para reflejar cuantos minutos y segundo equivaldría.

$$\%_{CBrest} = \ \frac{C_{\Delta} * 100}{C_{Batt}} = \frac{0{,}365\ Ah * 100}{2{,}75\ Ah} = \frac{36{,}5}{2{,}75} = 13{,}27\ \%$$

$$T_{min} = \ \frac{60\ min * \ \%_{CBrest}}{100\ \%} = \frac{60\ min * 13{,}27\ \%}{100\ \%} = \frac{796{,}2}{100} = 7{,}962\ min$$

$$T_{seg} = \ 0{,}962\ min * \frac{60\ seg}{1\ min} = 57{,}72\ seg$$

En conclusión, el tiempo que el UPS suministra energía para las cargas durante la ausencia de voltaje de la red eléctrica de la oficina es de 1 hora, 7 minutos y 57 segundos aproximadamente. Por lo tanto, si el corte de energía sobrepasa ese tiempo no se podrá realizar el monitoreo hasta que retorne el flujo de energía en ese sector. Para evitar estos inconvenientes, realizar un estudio del flujo constante de

energía en el sector y adquirir un UPS con las características para suministrar el voltaje a los dispositivos durante el tiempo que dura el corte.

3.4.3.4. Prueba 4. Validación de acceso por contraseña.

Para la prueba 4 se programó la placa Arduino para que al momento de presionar la tecla “#” se encienda el backlight de la LCD y genere un mensaje de presentación “U. E. LUXEMBURGO” Y “DEPT. COMPUTACIÓN” como en la figura 67 se describe. Luego del anterior mensaje se muestra otro, el cual muestra el ingreso de una clave como en la figura 68 se observa. Siempre permanecerá encendido el LED de color verde que indica la activación de la cerradura electromagnética. Si la clave es la correcta se encenderá el diodo de color rojo y mostrará un mensaje de acceso correcto como en la figura 69 se observa, se desactivará la cerradura electromagnética durante 7 segundos y luego volverá a su etapa inicial.

Figura 67. Inicio de la validación de contraseña con la presentación del mensaje de inicio.

Fuente: Unidad Educativa Luxemburgo.

Figura 68. Mensaje que indica el inicio de la digitación de clave.
Fuente: Unidad Educativa Luxemburgo.

Cuando solicita el ingreso de la clave y ésta sobrepasa los 6 dígitos el sistema borrará todos los datos ingresados y volverá a pedir la clave hasta que sea ingresada correctamente, o a su vez existen la tecla "*" que ayuda a borrar los caracteres ingresados.

3.4.3.4.1. Análisis de resultados.

La primera prueba con el Arduino consistió en ingresar la clave incorrectamente. Como el sistema no la valida que sea la correcta borrará todos los datos de la LCD y volverá a pedir la clave. En esta prueba también se considera presionar la tecla "*" para borrar los caracteres mal ingresados.

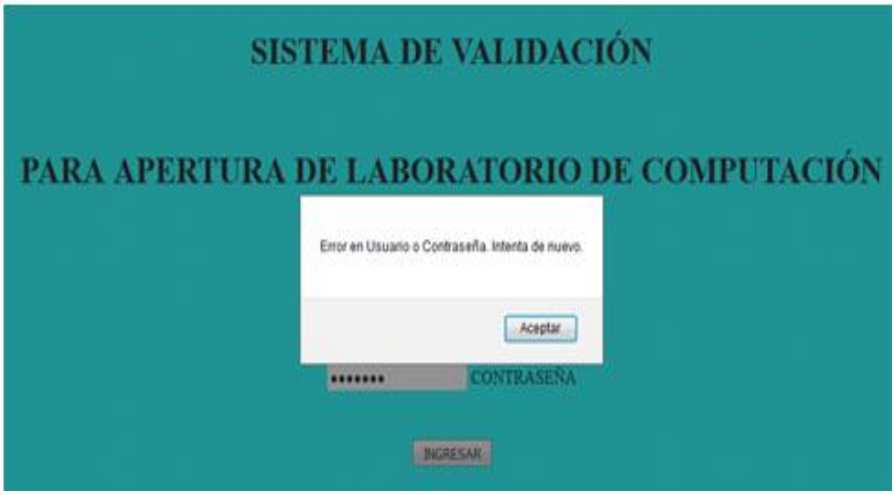
En la segunda prueba se valida la clave ingresada por teclado con la clave guardada en el array, como la clave es correcta se mostrará un mensaje que indicará "ACCESO CORRECTO" simultáneamente encenderá el diodo y desactivará la cerradura electromagnética durante 7 segundos (como en la figura 69 se representa) y luego volverá a su estado original, donde la LCD se pone en reposo (el back light se apaga) y espera hasta que se presione "#" de nuevo.

Figura 69. Mensaje que se presenta rápidamente de la digitación correcta de la contraseña.
Fuente: Unidad Educativa Luxemburgo.

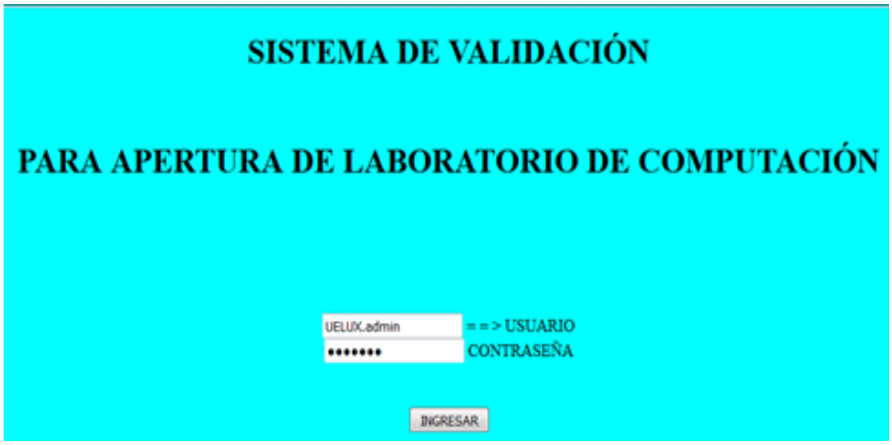
3.4.3.5. Prueba 5. Apertura de la cerradura electromagnética a través de la red.

Esta prueba consiste en una conexión remota con el sistema Arduino mediante la Ethernet Shield. Primeramente se tiene que abrir un programa HTML que aceptada un usuario y contraseña digitados correctamente para ingresar a la página que se ubica el control de la cerradura electromagnética.

Si el usuario o contraseña no son los correctos expresará un mensaje que diga que en ingreso fue incorrecto y vuelva a solicitar los datos (contraseña y usuario), como en la figura 70 se representa el acceso correcto e incorrecto.



a)



b)

Figura 70. a) Validación incorrecta de la clave de ingreso al sistema. b) Validación correcta de la clave de ingreso.
Fuente: El Autor.

La segunda prueba que se realiza es la validación del usuario y contraseña de forma correcta. Al momento que esto ocurra le redireccionará a una página donde se encuentra el control de la cerradura electromagnética. En esa ventana se ubica dos botones el uno es para desactivar la cerradura y el otro es para activarla. También se localiza un texto que indica el estado de la cerradura electromagnética (activada o desactivada), como en la figura 62 se observa.

3.5. Proceso de elaboración del proyecto.

Para empezar el proyecto se procedió a conversar con la representante de la institución y realizar los trámites respectivos para implementarlo sin que exista algún motivo que impida realizarlo. Luego se realizó la inspección del lugar en donde

necesita un monitoreo de cámaras y un control del ingreso a personal ajeno a la institución. Se logró ubicar los posibles puntos ciegos y cubrirlos con la cobertura de visualización de las cámaras. Localizar un área segura donde se coloque el DVR y realizar todo el control sin que ésta sea un lugar vulnerable para cualquier acto vandálico. Se investigó sobre los posibles sistemas de videovigilancia que se puedan utilizar en el proyecto. Se encontró tres sistemas CCTV diferentes y el ISmart fue seleccionado como el más recomendable por su resolución, precio y se ajusta a las condiciones ambientales previstas en el lugar de monitoreo.

Se realizó también la investigación sobre la utilización del método de control de acceso y la cerradura considerada para la protección de la puerta. La plataforma que se consideró en este proyecto para el control fue Arduino, ya que, ésta posee las características necesarias y un código muy sutil que hace que Arduino sea una plataforma manejable y muy interesante. Se realizó las investigaciones respectivas sobre el hardware que se utilizará, y se llega a la conclusión que al combinar Arduino Uno y la Shield Ethernet se puede adquirir un código muy versátil y una comunicación remota de la aplicación con el control de acceso.

Luego se implementó los dos sistemas en días planificados con personal asignado para la supervisión del proyecto por parte de la institución beneficiaria. Se realizó las pruebas respectivas de los elementos del sistema, para comprobar la correcta funcionalidad y si no cumple con los cargos respectivos, sustituir el dispositivo. Se realizó las pruebas respectivas de los dos sistemas implementados para cumplir con los objetivos planteados desde un principio con la institución y se verificó la correcta funcionalidad del mismo en presencia de personal asignado por la institución.

Se realizó la capacitación de las personas involucradas en el manejo del sistema CCTV y control de acceso para la correcta utilización y conservación del sistema. En última instancia se entregó el sistema implementado, y se dio paso a la inauguración del proyecto de beneficio para la institución educativa, con todos los objetivos planteados, cumplidos y el agradecimiento de todo personal que conforma la Unidad Educativa Luxemburgo.

3.6. Análisis de Costos.

Para el análisis presupuestal se consideró varios factores de consumo de efectivo los cuales se describen en la tabla 12. Se realizó la adquisición del sistema de CCTV esto incluyen las 4 cámaras interior/exterior, el DVR, Disco Duro, cables de conexión video, alimentación, cable de red, monitor y mouse.

También se realizó la adquisición del sistema de control de acceso que consta de las tarjetas de control y comunicación, la cerradura electromagnética, módulos, tablero de control, tablero exterior, teclado, pantalla, componentes electrónicos y demás dispositivos anexados al sistema.

Para las conexiones de los sistemas se utilizaron consumibles tales como cinta aislante, cable UTP, cable RG58, conectores RJ45, conectores BNC, tornillos, soportes, canaletas, adhesivos, etiquetas, etc. Adicional se incluyeron gastos de alimentación de los días de trabajo en la institución y los gastos de transporte que se consideraron para trasladarse al lugar de trabajo.

Para la videovigilancia se consideró utilizar el sistema CCTV ISmart, porque poseen las cuatro cámaras interior y exterior cuya resolución de 700TVL es óptima para la implementación en la institución educativa. Además, que cuenta con acceso a la red de internet y se puede acceder al DVR remotamente, por medio de un smartphone (es válido cuando la red cuente con una IP pública). Su costo es económico en comparación con otros sistemas en HD de elevado costo y otros de menor valor con una resolución no recomendable para este tipo de monitoreo. Para el ingreso al laboratorio se utilizó dos tarjetas: Arduino Uno y Shield Ethernet. El costo de estas tarjetas es menor en comparación con tarjetas de usos más complejos.

El retorno de la inversión se ve reflejado en el mejor control de los asistentes. Permite visualizar alguna situación de interés institucional como los hurtos, robos o cualquier acto delincuencial que afecte el prestigio de la institución educativa. La institución tiene pérdidas de equipos electrónicos y demás herramientas de las TIC’s de un valor considerable, con este sistema implementado, se considera minimizar esa pérdida.

A continuación en la tabla 12 se visualiza la cantidad (en dólares) invertida en cada rubro y el porcentaje que éste es considerado en el valor total de proyecto.

Tabla 12. Presupuesto del sistema de seguridad automatizado.

Presupuesto desglosado por rubros		
Rubro	**Cantidad $ UDS**	**Porcentaje %**
Sistema CCTV	$ 380	27,44
Sistema de control de acceso	$ 300	21,66
Movilización	$ 80	5,78
Alimentación	$ 130	9,39
Materiales consumibles	$ 280,73	20,27
Mano de obra	$ 214	15,45
Totales	**$ 1.384,73**	100,00

Fuente: El Autor

CONCLUSIONES

- Se realizó el estudio sobre los diferentes sistemas de seguridad automatizados por modelos y también los implementados en instituciones educativas y de comercio, donde se concluye que tanto los sistemas analógicos como IP son recomendables para la instalación. Sin embargo por el ajuste presupuestal que se dispone se considera el sistema analógico con el uso de un DVR de red.
- De acuerdo al análisis presupuestal y estudios de ambientes, para implementar el sistema de seguridad automatizado de videovigilancia con Arduino, se consideró utilizar el sistema CCTV ISmart con 4 cámaras analógicas de 720 TVL y un DVR de red, acompañados de un control de acceso Arduino con las características de ingreso por clave y remoto.
- Al diseñar el sistema de seguridad automatizado de videovigilancia con Arduino, se tomó en cuenta de acuerdo a las áreas de cobertura ubicar las cámaras en sectores estratégicos para cubrir los puntos ciegos de área a vigilar. Así también, la ubicación más segura para el DVR, ya que permite tener los respaldos de videos en caso de alguna situación eventual. Mientras en el control de acceso se utilizó la plataforma Arduino para programar el código que permitirá la automatización del ingreso al laboratorio, acompañado del código HTML y JavaScript para credenciales de ingreso al acceso remoto.
- Para la implementación adecuada del sistema de seguridad automatizado de videovigilancia se consideró realizar cálculos para determinar el lugar donde se sujetará cada cámara. También se tomó en cuenta, los medios de transmisión adecuados de acuerdo al SNR (50 dB) de las cámaras con el fin de no distorsionar la señal que transmiten. Mientras, que el control de acceso se utilizó cable UTP Cat. 5e para trasmisión de datos desde la caja de control que se encuentra en el interior de laboratorio y la caja de control de ingreso donde se alojan la pantalla, teclado y LED indicadores y se respalda el suministro de energía del sistema CCTV con un UPS propiedad de la institución, en caso de que exista corte de energía en el lugar con una duración del suministro de 1 hora, 7 minutos y 57 segundos aproximadamente.

RECOMENDACIONES.

- En caso de ampliar el sistema videovigilancia en varios sectores de la Unidad Educativa Luxemburgo, considere implementar sistemas CCTV independientes con un DVR de red, o conexión LAN con cámaras IP si el presupuesto lo permite, conectados a un servidor de video, con el fin de respaldar todos los videos, utilizar menos cableado para evitar pérdidas y así administrar de mejor manera toda la institución.
- De acuerdo al UPS que se utiliza, los respaldos de potencia sólo cubrirá 1 hora de corte. En el caso que el sector presente cortes de energía mayores a 1 hora, realizar un diseño de suministro eléctrico de respaldo para el sistema CCTV, en el cual incluya una generación de potencia mayor a la actualmente instalada.
- Para obtener un registro con fecha y hora de los usuarios que ingresan al laboratorio se recomienda diseñar una base de datos en algún ordenador ubicado en inspección general, donde se almacenará toda la información pertinente con respecto a la administración de acceso al aula.
- Para una validación más sofisticada del control de acceso al laboratorio, considere implementar un detector de huella dactilar que funcione en conjunto con la contraseña, con el fin de controlar de una mejor manera la validación de usuarios, ya que la contraseña puede saberse pero con la huella dactilar evitará que cualquier intruso ingrese al aula de computación.

Bibliografía

Álvarez, D. (3 de Junio de 2014). *Cap 9. Control de voz entre Arduino – EasyVR*. Obtenido de Taller Arduino: https://tallerarduino.com/

Andreu Gómez, J. (2010). Servicios en red. En J. Andreu Gómez, *Servicios en red* (págs. 8-18). Editex.

Arduino. (2015). *Products: Arduino UNO & Genuino UNO*. Obtenido de Arduino Web Site: https://www.arduino.cc/en/Main/ArduinoBoardUno

Ardutienda. (2015). *Arduino: Arduino Leonardo*. Obtenido de Ardutienda: http://www.ardumania.es/ardutienda/es/

Area de Ingeniería Telemática. (2012). Acceso al medio (3). Navarra, España.

AXIS Communicatios. (2008). Estándar de compresión de video H.264. Suecia.

Axis Comunications. (2015). *Poductos y Soluciones: Cámaras PTZ de Axis*. Obtenido de AXIS Comunications Sitio Web: http://www.axis.com/ec/es/products/ptz-cameras

BricoGeek. (2014). *Modelos Arduino: Arduino Yún*. Obtenido de BricoGeek Sitio Web: http://tienda.bricogeek.com/modelos-arduino/570-arduino-yun.html

Cevallos M., G. F. (19 de Agosto de 2011). *Definiciones: Seguridad*. Obtenido de Seguridad Electrónica Sitio Web: https://sites.google.com/site/seguridadelectronicagcm/capitulo-1/1-1-definiciones

Cruz, G. (7 de Noviembre de 2013). *Conceptos básicos de CCTV: Slide Share.* Obtenido de SlideShare Sitio Web: http://es.slideshare.net/german_cruz/conceptos-basicos-cctv

Cumbajín Alférez, M. E. (Abril de 2012). Red Inalámbrica de Datos y Video Vigilancia con CCTV para mejorar el servicio de comunicación y seguridad en la instalaciones del Hotel Wendy's. Ambato, Tungurahua, Ecuador.

Duarte, A. (10 de Julio de 2013). *Arduino Ethernet*. Obtenido de Art Interactivo Sitio Web: http://www.artinteractivo.com/arduino-ethernet

Electronica Unicrom. (2014). *Tutoriales: Relé – Relay – Relevador (interruptor operado magnéticamente)*. Obtenido de Electrónica Unicrom Sitio Web: http://unicrom.com/rele-relay-relevador-interruptor-operado-magneticamente/

Enrique. (16 de Noviembre de 2014). *Arduino Ethernet Shield – Controla Tu Casa Por Internet*. Obtenido de EducaChip: http://www.educachip.com/arduino-ethernet-shield/

Forouzan, B. A. (2007). Transmisión de Datos y Redes de Comunicaciones. En B. A. Forouzan, *Transmisión de Datos y Redes de Comunicaciones* (págs. 187-188-190-192). New York: McGraw-Hill.

García Gonzalez, Antony; Navarro, Kiara;PanamaHitek Creative Team. (20 de Mayo de 2015). *Arduino: ¿Qué es Arduino y para qué se utiliza?* Obtenido de Panama Hitek Sitio Web: http://panamahitek.com/que-es-arduino-y-para-que-se-utiliza/

García Mata, F. J. (2011). Videovigilancia: CCTV usando videos IP. En F. J. García Mata, *Videovigilancia: CCTV usando videos IP* (pág. 11). Málaga: PUBLICACIONES VÉRTICE S.L.

GlobeRed. (24 de Agosto de 2011). *Electrónica digital: Buzzer*. Obtenido de GlobeRed Sitio Web: http://instrumentacion-electronica.globered.com/

Gualotuña Suntasig, D. A. (Diciembre de 2009). Implementación de un Sistema de Video Vigilancia mediante Cámara IP para la empresa “Chasquis Compu Store”. Quito, Pichincha, Ecuador.

Higuera Angarita. (2015). *Comparación de lentes para cámaras CCTV.* Obtenido de HigueraAngarita.com Sitio Web: http://www.higueraangarita.com/dvr/lentes.html

HIKVISION. (2014). *Prdouctos: Cámaras de CCTV*. Obtenido de HIKVISION Sitio Web: http://www.hikvisionecuador.com/

Home: Hangzhou Yingbang Cable Co., Ltd. (1 de Julio de 2013). Obtenido de Hangzhou Yingbang Cable Co., Ltd Sitio Web: http://yingbang.en.made-in-china.com/

Impomax. (2015). *Productos/Catálogo: Videovigilancia.* Obtenido de iM iMPOMAX Sitio Web: http://impomax.myshopify.com/collections/video-vigilancia

International Telecomunications Union. (Enero de 2010). *Standardization: Commited to connecting the world.* Obtenido de Commited to connecting the world: http://www.itu.int/en/ITU-T/info/Pages/resources.aspx

International Telecomunications Union. (Enero de 2010). *Stardardization: Committed to connecting the world.* Obtenido de Committed to connecting the world: http://www.itu.int/en/ITU-T/info/Pages/resources.aspx

Isaac, P. E. (29 de Julio de 2014). *Análisis comparativo de las placas Arduino (oficiales y compatibles)*. Obtenido de Comohacer.eu ¿Inventamos juntos?: http://comohacer.eu/analisis-comparativo-placas-arduino-oficiales-compatibles/

Macroquil. (21 de Noviembre de 2015). *Productos: 12 consideraciones para elegir la cámara IP adecuada.* Obtenido de Macroquil S.A. Sitio Web: http://macroquil.com/12-consideraciones-para-elegir-la-camara-ip-adecuada/

Murillo, P. (3 de Octubre de 2012). *Comparativa - Pulsadores para proyectos*. Obtenido de TR3SDLAND Sitio Web: https://www.tr3sdland.com/2012/10/comparativa-pulsadores-para-proyectos/

Notiseg. S.A. de C.V. (Enero de 2015). *Productos: Cámara tipo bala HD.* Obtenido de Notiseg.com Sitio Web: http://notiseg.com/images/cctv/Bulletdatasheet.pdf

Novicompu. (2014). *Tecnología; Redes; Cámaras de seguridad: Kit CCTV 1 DVR 4 CH + 4 cámaras 720 TVL + accesorios.* Obtenido de Novicompu lo mismo pero más baratos Sitio Web: https://www.novicompu.com/camaras-de-seguridad/2037/kit-cctv-1-dvr-4-canales-4-camaras-720tvl-accesorios.html

PC Componentes. (2015). *Seguridad y Vigilancia Conceptronic: PC COMPONENTES Y MULTIMEDIA SLU*. Obtenido de PC Componentes Sitio Web : https://www.pccomponentes.com/seguridad-y-vigilancia/conceptronic

PCEL. (2013). *PCEL, Electronica: Batería de Respaldo APC Back-UPS, 550VA (330WATTS) con 8 contactos NEMA 5-15R, USB.* Obtenido de PCEL: https://pcel.com/APC-BE550G-LM-81125

Promatco Seguridad. (2005). *Nuestros servicios: Sistemas de control de acceso*. Obtenido de Sistemas de control de acceso: http://www.promatco.com.ec/acc.html

Prometec. (17 de Agosto de 2015). *Home: El Arduino y el Bus I2C*. Obtenido de Prometec Sitio Web: http://www.prometec.net/bus-i2c/

Protostack. (2014). *LED/LCD: 16 x 2 character LCD module with blue backlight and white text*. Obtenido de Protostack: http://www.protostack.com/led-lcd/lcd-modules/16-x-2-character-lcd-module-with-blue-backlight-and-white-text

Rengel Rivera, M. S., & Jimbo Jérez, M. A. (Enero de 2015). Diseño, construcción e implementación de un dispositivo de seguridad que permite la intercomunicación con audio y video entre dos puntos y la activación remota de elementos de seguridad. Cuenca, Azuay, Ecuador.

skynetgroup2005. (2014). *Cable de fibra óptica: Galeon.com hispavista*. Obtenido de Galeon.com hispavista: http://modul.galeon.com/aficiones1366320.html

SONY. (2004). *Cámaras de seguridad IP en red, inalámbricas y digitales*. Obtenido de SONY Sitio Web: https://www.sony.es/pro/products/video-security-ip-cameras

Sunshine State Security, Inc. (Marzo de 2015). *Products: Surveillance Gold Packages*. Obtenido de Surveillance Gold Packages: http://www.sunshinestatesecurity.com/page.asp?page=5538

Superinventos. (2000). *Videovigilancia y seguridad electrónica: Cámara ojo de pez.* Obtenido de Superinventos.com Videvigilancia y seguridad electrónica Sitio Web: http://www.superinventos.com/s120400.htm

Svenungson, J. (4 de Febrero de 2004). *Comprendiendo las pantallas compatibles con LCD HD44780*. Obtenido de LinuxFocus.org: http://www.linuxfocus.org/Castellano/September2002/article258.shtml

TechResources. (2015). *Sistemas de seguridad: Kit cámaras de seguridad*. Obtenido de TechResources Cia. Ltda. Sitio Web: http://recursos-tecnologicos.com/57-kit-camaras-de-seguridad

Tecno Store. (2014). *Componentes electrónicos, CCTV, audio, computación.* Obtenido de Tecno Store C.A.: http://www.tiendaelectronica.com.ve/

Telefonía Total. (29 de Marzo de 2014). *Cámaras CCTV: ¿Que son las TVL?* Obtenido de Telefonía Total una extensión más para su empresa: http://telefoniatotal.com/que-son-las-tvl/

Tomasi, W. (2003). Sistemas de comunicaciones electrónicas. En W. Tomasi, *Sistemas de comunicaciones electrónicas* (págs. 605-612). Mexico: Prentice Hall.

TVC. (24 de Julio de 2014). *Configuración de grabación por detección de movimiento*. Obtenido de Configuración de grabación por detección de movimiento: http://ingenieria.tvc.mx/kb/a561/configuracion-de-grabacion-por-deteccion-de-movimiento-desde-la-interfaz-web.aspx

Ubierna Yuvero, O. (7 de Mayo de 2013). *Conceptos básicos de WiFi: Tecnología Wireless*. Obtenido de Tecnología Wireless : http://www.comunicacionesinalambricashoy.com/wireless/conceptos-basicos-de-wifi/

Unidad de Planificación del Ministerio Coordinador de Seguridad. (Febrero de 2015). *Plan Estratégico Institucional del Ministerio Coordinador de Seguridad 2015 - 2017.* Obtenido de Ministerio Coordinador de Seguridad Sitio Web: http://www.seguridad.gob.ec/wp-content/uploads/downloads/2015/02/pestrategico_2015_2017.pdf

Universidad de Zaragoza. (2006). *Estudio de CCTV del Edificio Betancourt.* Obtenido de CCTVCAD Software Sito Web: http://www.cctvcad.com/Files/TAZ-PFC-2011-581.pdf

Videovigilancia.com. (2006). *Catálogo: Cámaras de Vigilancia y Seguridad*. Obtenido de Videovigilancia.com Expertos en su seguridad Sitio Web: http://www.videovigilancia.com/camaras.htm

Villegas, J. (16 de Junio de 2012). *Análisis CCTV: Comparando las cámaras con iluminadores infrarrojos frente a las Día/Noche.* Obtenido de TECNOSeguro.com Magazine Digital - Online Media Sitio Web: https://www.tecnoseguro.com/analisis/cctv/comparando-las-camaras-con-iluminadores-infrarrojos-frente-a-las-dia-noche.html

ViperTek. (2014). *productos: CCTV*. Obtenido de Vipertek Sitio Web: http://viperteksecurity.com/product-category/cctv/

VTA. (2013). *Soporte: Centro de descargas*. Obtenido de VTA Sitio Web: http://vtacompany.com.co/index.php?r=site/descargas

ANEXOS

Anexo 1. MANUAL PARA EL USUARIO.

Señor usuario siga las instrucciones descritas en este manual para evitar una mala manipulación de los dispositivos que componente este sistema.

Precauciones Generales

No colocar encima del sistema de videovigilancia automatizado (tablero de control de acceso y DVR) objetos que causen daños en sus componentes.

No desarmar las piezas tanto mecánicas como electrónicas salvo el caso de daño en algún elemento, pero siempre con una persona especializada en Electrónica.

No manipular las piezas internas cuando este se encuentre en funcionamiento ya que puede provocar daños en las mismas y puede ser peligroso para el usuario.

Ubicar el DVR y sus demás componentes en una base firme, de lo contrario puede provocar daños en todos sus componentes electrónicos y mecánicos.

No realizar cualquier tipo de corte de energía al sistema de videovigilancia automatizado, puede provocar fallos en su funcionamiento.

Descripción y partes del dispositivo.

Figura 1. Partes y accesorios del tablero para el control de acceso.

Figura 2: Dispositivos conectados al DVR.

1. LCD (Visualizador de datos)
2. LED de activación
3. LED de desactivación
4. Teclado
5. Tecla para borrar caracteres.
6. Tecla de validación.
7. Pines de alimentación de las cámaras.
8. Pines de alimentación del DVR.
9. Cable UTP Cat.6 certificado.
10. Cable USB del teclado.
11. Entradas para dispositivos de audio.
12. Cable VGA.
13. Canales de video.

Visualización de datos.

La LCD es el dispositivo de salida que muestra los datos que recogen de cada pulsación que se realiza en el teclado. Al encender el dispositivo también indica el mensaje de bienvenida.

LED de activación.

Este LED es un dispositivo electrónico que se ilumina de color verde, cuando la cerradura electromagnética está activada.

LED de desactivación.

Este dispositivo se ilumina de color rojo, cuando la cerradura electromagnética se desactive, ya sea remotamente o por el ingreso de contraseña válido.

Teclado.

Este dispositivo de entrada, por medio de sus teclas, ayuda a ingresar los caracteres correctos para la validación de la contraseña. Además de contener los caracteres, para prender la pantalla posee la tecla de "#" y la tecla "*" para borrar caracteres mal ingresados.

Pines de alimentación.

Son los terminales en los que se vincula la energía con un adaptador de AC, que pone en marcha el funcionamiento del sistema de seguridad automatizado. Los conectores son representados de color rojo para la alimentación de las cámaras.

Puerto Ethernet.

En este puerto se conecta el cable UTP Cat.6 certificado que realiza el transporte de datos desde el DVR hacia el internet para comunicarse mediante un smartphone o viceversa. En cable es representado de color azul.

Puerto USB.

Es el terminal donde se conecta los dispositivos de entrada para controlar el software como los son el teclado y el mouse.

Entradas de audio.

Estos pines de entrada se usan para conectar dispositivos de audio, como lo son los micrófonos.

Cable VGA.

Se usa para conectar el cable de comunicación del DVR con la impresora y mostrar por medio de la interfaz gráfica el video en tiempo real y almacenado. El conector está representado de color azul.

Canales de video.

En el DVR existen 4 canales de video y sirven para que las cámaras se comuniquen con el DVR y así transmitir las imágenes capturadas, para que sean procesadas por el dispositivo antes mencionado. Los conectores están representados de color amarillo.

Sistema de seguridad automatizado.

Dentro del sistema se ubican dos partes: el circuito cerrado de televisión (CCTV) y el control de ingreso al laboratorio.

El CCTV, es un circuito de video vigilancia que ayuda a monitorear áreas específicas en tiempo real y que se pueden almacenar el disco duro, para mantener archivados los sucesos capturados por las cámaras.

El control de acceso Arduino, es un mecanismo que consta de varias partes técnicas en ellas: el tablero de control ubicado al interior del laboratorio, donde se realizan todas las instrucciones de funcionamiento del sistema. El tablero de control de acceso exterior en el cual están alojados la pantalla de visualización, el teclado y los LED indicadores de activación y desactivación. La cerradura electromagnética que es el dispositivo actuador que bloquea la puerta de ingreso al laboratorio, por medio de un campo magnético.

Anexo 2. GUÍA DE USO.

Manejo del sistema CCTV.

Para empezar a utilizar el sistema CCTV, en primer lugar se debe verificar que todos los cables de alimentación estén conectados al adaptador de voltaje de la red eléctrica del lugar.

Menú de Visualización.

Al momento de iniciar el sistema, aparecerá en la pantalla las capturas en cuadrícula (Quads) en tiempo real de las cuatro cámaras instaladas en el sitio, como en la figura 3 se observa.

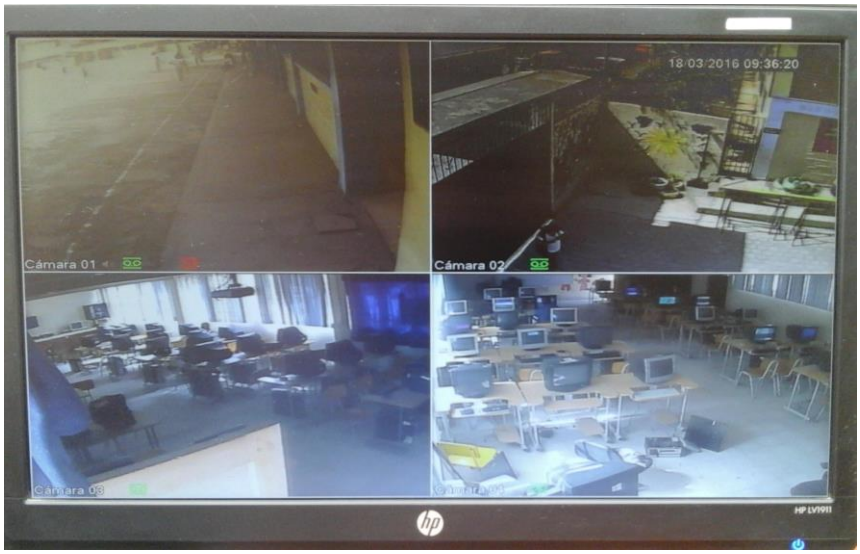


Figura 3. Vista en cuadrícula (Quads) de la percepción de las cuatro cámaras alrededor y al interior del laboratorio de computación.

Al dar clic derecho, se solicitará ingresar una clave y usuario del sistema para modificar la configuración y visualizar los videos almacenados en el disco duro, como en la figura 4 se observa.

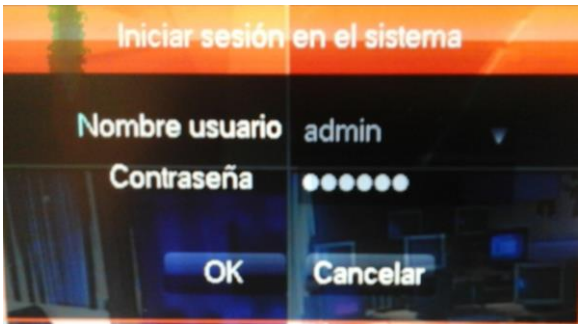


Figura 4. Validación del sistema para ingresar al modo de configuración.

Luego de autorizar el ingreso, se elige la pestaña buscar en el menú desplegable, al hacer nuevamente clic derecho en el escritorio. Y aparecerá una ventana como en la figura 5 se demuestra.

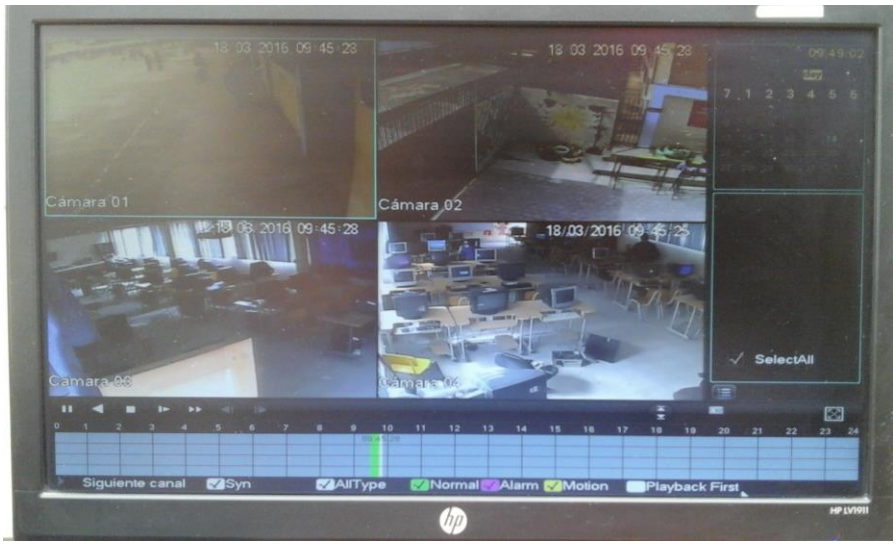


Figura 5. Ingreso al modo buscar, para revisar los videos grabados en el disco duro.

En la ventana mencionada anteriormente se visualizan los videos grabados en el disco duro en la ventana superior derecha de la figura 5, se demuestra el calendario de grabación donde consta el día, el mes y el año donde se aloja en video grabado en tal fecha determinada.

En la parte inferior de la pantalla se puede observar un cuadro cronológico de horas desde las 00:00 hasta las 23:59 del día determinado por el calendario. En el cuadro se puede observar también una franja verde que indica el espacio de tiempo que está ocupado por un video grabado.

Si se necesita ver el video en una hora determinada, basta con ubicarse con el puntero del mouse hacia el espacio de la hora requerida y darle clic izquierdo en el lugar, para acceder al video de las cuatro cámaras.

Para salir de la ventana de buscar, se necesita dar clic derecho hasta legar al escritorio.

Si se requiere ver la imagen completa de una de las cámaras, se realiza doble clic en la representación de la cámara y automáticamente se pondrá en pantalla completa, como en la figura 6 se observa.

Figura 6. Visualización a pantalla completa de la cámara del pasillo con video tiempo real.

Manejo del control de acceso Arduino.

Validación de usuario.

El control de acceso se ubica la parte centro este del portón de ingreso al laboratorio de computación. Es un tablero acrílico de forma rectangular color azul, como en la figura 1 se representa.

El tablero posee la pantalla de visualización, el teclado y los LED´s indicadores de activación y desactivación. En el interior del tablero se encuentra un zumbador que produce sonidos cada vez que se presiona una tecla.

El primer paso a realizar, es presionar la tecla "#" para encender la pantalla que está en modo de reposo, en la figura 7 se describe U. E. LUXEMBURGO, DEPT COMPUTACION.

Figura 7. Visualización de la presentación principal de la pantalla.

Luego de 2 segundos se mostrará en la pantalla un mensaje de INGRESE LA CLAVE, y a continuación el campo para ingresar los caracteres, como en la figura 8 se demuestra.

Figura 8. Pantalla donde si visualiza el espacio donde se ingresa la clave.

Luego de digitar la clave correcta, el LED rojo se enciende y la cerradura electrónica se desactiva, como en la figura 9 se observa.

Figura 9. Visualización del mensaje de acceso correcto.

Sin embargo, si no se accede correctamente seguirá encendido el LED de color verde que indica activación de la cerradura electromagnética.

Recomendaciones.

- Para que los videos sean almacenados por un largo periodo se puede considerar instalar un disco duro de al menos 1 Tb, y por supuesto realizar respaldos cada cierto periodo.
- Otra alternativa para evitar que se llene rápidamente el disco duro con el almacenamiento de grabaciones, es configurar al DVR en modo Detection

Motion (Detección de Movimiento). Este modo permite que el DVR grabe la señal que emite la cámara cuando ésta detecte movimiento en el lugar.

- Al acceder al sistema CCTV por medio de aplicación Android, se debe comprobar que el enlace de internet sea con IP pública, es decir, que se pueda acceder de forma remota desde otra red, a la red LAN de la institución. Sin embargo se puede acceder por medio de otro dispositivo con puerto Ethernet y con el programa respectivo conectado a la red privada de la institución.
- Para evitar el consumo excesivo de energía eléctrica, se recomienda apagar el monitor al momento de estar sin uso.
- Al momento de instalar la cerradura electromagnética, se puede considerar colocarla en una posición frontal con respecto al marco de la puerta, con la dependencia del material con el que está fabricada la puerta.
- Antes de cualquier utilización de los dispositivos, se debe tener una capacitación del mismo, para el correcto funcionamiento y buena utilización de los elementos de sistema de seguridad automatizado.

Anexo 3. TABLA DE FALLOS.

SISTEMA	PROBLEMA	SOLUCIÓN
CCTV ISmart	No enciende	• Revisar que el adaptador de CA esté conectado a la red eléctrica de la institución. • Revisar que el cable de derivación del adaptador hacia los pines de alimentación de las cámaras y DVR estén bien conectados.
	No visualiza el video mostrado por las cámaras	• Revisar que la conexión del cable coaxial estén bien asegurados en los canales del DVR. • Revisar que el cable coaxial esté bien conectado en el terminal de video de las cámaras. • Revisar los pines de alimentación de cada una de las cámaras tanto en el DVR como en la cámara.
	No accede a los videos grabados en el disco duro.	• Realizar un ingreso de usuario y contraseña proporcionado por el equipo, para ingresar al modo de configuración. • Entrar en modo de grabación y seleccionar activar grabación.
	Se congela la imagen de capturadas por la cámara.	• Realizar el reinicio del sistema, ubicándose en el escritorio y hacer clic derecho en el mismo. • Se selecciona la opción configuración. • Se da clic en el icono de SISTEMA y se selecciona la opción REINICIAR EL DISPOSITIVO. Automáticamente se reiniciará el sistema.

Control de acceso Arduino	No enciende	• Revisar si la distribución de energía eléctrica en el laboratorio esta interrumpida. • Si el LED verde se encuentra encendido y la pantalla de visualización activada, se necesita presionar la tecla “#” para usar el mecanismo.
	No permite ingresar los caracteres por teclado.	• Es posible que es sistema esté inhibido. • Abrir el seguro de la caja de control exterior. • Presionar el botón de reinicio ubicado en el interior de la caja. • Se reiniciará el sistema.
	No valida la contraseña ingresada.	• Digitar bien la clave de ingreso. • Es posible que el sistema esté inhibido, reiniciar el sistema.
	Los LED´s indicadores no encienden.	• Reiniciar el sistema. • Si el sistema activa y desactiva correctamente, es posible que los LED´s no funcionen. Llamar a un técnico para que realice el cambio respectivo de los LED´s.

E-MAIL Y TELÉFONO DE SOPORTE TÉCNICO

Luis Flores Rogel

Celular: 0992810375

E-mail: flores_rogel_luis@hotmail.com

Anexo 4. CÓDIGO FUENTE ARDUINO.

```
#include <Keypad.h>
#include <FastIO.h>
#include <I2CIO.h>
#include <LCD.h>
#include <LiquidCrystal.h>
#include <LiquidCrystal_I2C.h>
#include <LiquidCrystal_SR.h>
#include <LiquidCrystal_SR2W.h>
#include <LiquidCrystal_SR3W.h>
#include <LiquidCrystal_I2C.h>
#include <Wire.h>

////================/////////==============/////////=========////
  #include <SPI.h>
  #include <Ethernet.h> //Declaración de la direcciones MAC e IP. También del puerto
80
  byte mac[]={0xDE,0xAD,0xBE,0xEF,0xFE,0xED}; //MAC
  IPAddress ip(10, 187, 60, 139); //IP
  EthernetServer servidor(80);
  String readString=String(30); //lee los caracteres de una secuencia en una cadena.
  //Los strings se representan como arrays de caracteres (tipo char)
  String state=String(3);
  ////============//////////==========/////////========/////
  /* Funcion de configuracion
    de pines del modulo LCD/I2C (Direccion,en,rw,rs,d4,d5,d6,d7,backlight,polaridad)*/
  LiquidCrystal_I2C lcd(0x27, 2, 1, 0, 4, 5, 6, 7, 3, POSITIVE);


const byte Filas = 4;     //Cuatro filas
const byte Cols = 4;    //Cuatro columnas

byte Pins_Filas[] = {A3,A2,A1,A0};   //Pines Arduino a los que contar las filas.
byte Pins_Cols[] = {7,6,5,3};   // Pines Arduino a los que contar las columnas.
//no utilizar los pines 1 y 0 para no interferir en Rx y Tx

char Teclas [ Filas ][ Cols ] =
{
  {'1','2','3','A'},
  {'4','5','6','B'},
  {'7','8','9','C'},
  {'*','0','#','D'}
};

char codigoSecreto[6] = {'A','2','B','3','C','5'}; // Aqui va el codigo secreto
// Para cambiar el tamaño de la clave, solo hay que cambiar el tamaño del array

int posicion=0; // necesaria para la clave
int cursor=4; // posicion inicial de la clave en el LCD
int clave=0; // para el LCD
int luz=0;  // para el LCD
```

```
int tiempo=0;  // para el LCD
char pulsacion;
int abierto = 9;
int cerrado = 8;
int buzzer=2;  // pin altavoz
int reset;

Keypad Teclado1 = Keypad(makeKeymap(Teclas), Pins_Filas, Pins_Cols, Filas, Cols);

void setup(){
Serial.begin(9600) ;
lcd.begin(16,2); //se inicializa el LCD.
lcd.noBacklight(); //se apaga LCD
Ethernet.begin(mac, ip); //Inicializa con las direcciones asignadas
servidor.begin();
pinMode (abierto,OUTPUT);
pinMode (cerrado, OUTPUT);
 digitalWrite(cerrado,HIGH);  //se enciende el LED rojo
 digitalWrite(abierto, LOW);  //se apaga el verde
state="ON";
}


void loop(){
 login();
     //EthernetClient Crea un cliente que se puede conectar a
    //una dirección específica de Internet IP
    EthernetClient cliente= servidor.available();
   if(cliente) {
   boolean lineaenblanco=true;
   while(cliente.connected()) {
   if(cliente.available()) {
   char c=cliente.read();
   if(readString.length()<30) {
   readString.concat(c);
   //Cliente conectado
   //se lee petición HTTP caracter a caracter
   //Almacenar los caracteres en la variable readString
   }
   if(c=='\n' && lineaenblanco) //Si la petición HTTP ha finalizado
   {
   int LED = readString.indexOf("LED=");
   if(readString.substring(LED,LED+5)=="LED=T") {
    digitalWrite(abierto,HIGH);
    digitalWrite(cerrado,LOW);
    state="OFF"; }
    else if (readString.substring(LED,LED+5)=="LED=F") {
    digitalWrite(abierto,LOW);
    digitalWrite(cerrado,HIGH);
    state="ON";
    }
    //Cabecera HTTP estándar
   cliente.println("HTTP/1.1 200 OK");
   cliente.println("Content-Type: text/html");
```

```
   cliente.println(); //Página Web en HTML
   cliente.println("<head>");
   cliente.println("<title>CONTROL DE ACCESO</title>");
   cliente.println("</head>");
   cliente.println("<body bgcolor=""gray"" width=100% height=100% >");
   cliente.println("<center>");
   cliente.println("<h1>UNIDAD EDUCATIVA LUXEMBURGO</h1>");
   cliente.println("<h1>LABORATORIO DE COMPUTACION</h1>");
   cliente.println("<h1>CONTROL DE ACCESO</h1>");
   cliente.print("<br><br>");
   cliente.print("ESTADO DE LA CERRADURA: ");
   cliente.print(state);
   cliente.print("<br><br><br><br>");
   cliente.println("<input type=submit value=OFF style=width:200px;height:75px
onClick=location.href='./?LED=T\'>");
   cliente.println("<input type=submit value=ON style=width:200px;height:75px
onClick=location.href='./?LED=F\'>");
   cliente.println("</center>");
   cliente.println("</body>");
   cliente.println("</html>");
   cliente.stop();
   //Cierro conexión con el cliente
   readString="";
          }
        }
      }
    }
 }
void login(){
   pulsacion = Teclado1.getKey() ;  // lee pulsación

if (pulsacion != 0){  // Si el valor es 0 es que no se ha pulsado ninguna tecla

if (pulsacion != '#' && pulsacion != '*' && clave==0){  // descarta numeral y asterisco

    lcd.print("*");  // imprime pulsación
    cursor++;  // incrementa el cursor
     tone(buzzer,350);  // tono de pulsación
    delay(200);
    noTone(buzzer);

//--- Condicionales para comprobar la clave introducida ----------

if (pulsacion == codigoSecreto[posicion]){ // compara entrada con cada uno de los
digitos, uno a uno
      posicion ++;  // aumenta en uno el contador de posición si es correcto el digito

      }

if (posicion == 6){ // comprueba que se han introducido los 4 correctamente

      lcd.setCursor(0,0); // sitúa el cursor en la posición 0 de la linea 0.
      lcd.print("ACCESO  CORRECTO"); // escribe en LCD
      delay(200); // tono de clave correcta
```

```
      lcd.setCursor(5,1); // cursor en la posicion 5, linea 1
      clave=1;  // indica que se ha introducido la clave
      tone(buzzer,500);
      delay(100);
      noTone(buzzer);
      tone(buzzer,600);
      delay(100);
      noTone(buzzer);
      tone(buzzer,800);
      delay(100);
      noTone(buzzer);
      digitalWrite(cerrado,LOW);  // apaga el LED verde
      digitalWrite(abierto, HIGH);  // enciende el rojo
      delay(7000);
      digitalWrite(cerrado,HIGH);  // enciende el LED rojo
      digitalWrite(abierto, LOW);  // apaga el verde
      delay(1000);
      software_Reset() ;
      }
//--- En el caso de que este incompleta o no haya acertado ----------
    if(cursor>9){  // comprueba que no pase de la sexta posicion
      cursor=4;  // lo vuelve a colocar al inicio
      posicion=0; // borra clave introducida
      lcd.setCursor(4,1);
      lcd.print("               ");  // borra la clave de la pantalla
      lcd.setCursor(4,1);
      }
      if(clave==0){          // comprueba que se acertó
      tone(buzzer,70,500);  // para generar
      delay(250);          // tono de error
      noTone(buzzer);
      }
    }
  }

if (pulsacion != 0){
if (pulsacion == '#' && luz==0){ // comprueba tecla y enciende si está apagado
    lcd.backlight();  // enciende
    luz=1;  // indica que está encendida
    pulsacion =0; // borra el valor para leer el siguiente condicional
   lcd.setCursor(0, 0);
    lcd.print("U. E. LUXEMBURGO");
    lcd.setCursor(0, 1);
    lcd.print("DEPT COMPUTACION");
    delay(3000);
    lcd.clear();
lcd.setCursor(0,0); // situa el cursor en la posición 2 de la linea 0.
lcd.print(" INGRESE  CLAVE "); // escribe en LCD
lcd.setCursor(cursor,1); // cursor en la posicion de la variable, linea 1
  }

if (pulsacion == '#' && luz==1){  //  comprueba tecla y estado
    lcd.noBacklight();  // apaga
    luz=0;  // indica que esta apagada
```

```
      }

}
//---------------------------------------------------------------

//--- Condicionales para resetear clave introducida ----------

if (pulsacion == '*'){ // asterisco para resetear el contador
      posicion = 0;
      cursor = 4;
      clave=0;
      posicion=0;
      lcd.setCursor(0,0); // situa el cursor en la posición 2 de la linea 0.
      lcd.print(" INGRESE  CLAVE "); // se escribe en LCD

      lcd.setCursor(4,1);
      lcd.print("               "); // borra de la pantalla los numeros
      lcd.setCursor(4,1);


      digitalWrite(cerrado,HIGH);  // enciende el LED verde
      digitalWrite(abierto, LOW);  // apaga el rijo

}
    ////////=========/////////==========////////=======///////=

}
void software_Reset() // Restarts program from beginning but does not reset the
peripherals and registers
{
asm volatile (" jmp 0");
}
```

Anexo 5. CÓDIGO FUENTE HTML Y JAVASCRIPT PARA VALIDACIÓN DEL CONTROL DE ACCESO.

```
<html>
<head><title> ACTIVACIÓN CERRADURA LABORATORIO DE COMPUTACIÓN
</title>
</head>
<body bgcolor="cyan">
<script>

function usrpas(){

if (document.form1.txt.value=="UELUX.admin" &&
document.form1.num.value=="LUX2016"){window.location="http://10.187.60.139/?LED
=F"}

else {alert("Error en Usuario o Contraseña. Intenta de nuevo.")}
```

```
}

document.oncontextmenu=new Function("return false");

</script>
</body>

<form name="form1">

<center><h1> SISTEMA DE VALIDACIÓN</h1> <br></center>

<center><h1> PARA APERTURA DE LABORATORIO DE COMPUTACIÓN </h1>
<br></center>
<br> </br>
<br> </br>

<center><input type="text" name="txt"> = = > USUARIO<br></center>

<center><input type="password" name="num"> CONTRASEÑA <br></center>

<center><input type="button" value="ingresar" onclick="usrpas()"></center>

</form>
```

Anexo 6. HOJAS TÉCNICAS.

Tarjeta Arduino Uno Rev3

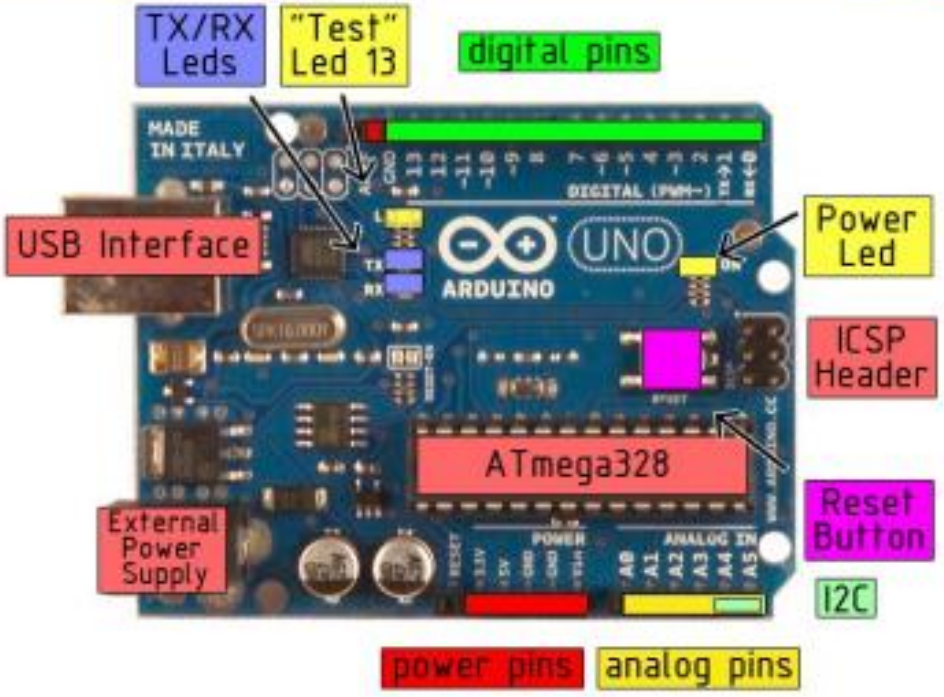
Technical Specification

EAGLE files: arduino-duemilanove-uno-design.zip Schematic: arduino-uno-schematic.pdf

Summary

Microcontroller	ATmega328
Operating Voltage	5V
Input Voltage (recommended)	7-12V
Input Voltage (limits)	6-20V
Digital I/O Pins	14 (of which 6 provide PWM output)
Analog Input Pins	6
DC Current per I/O Pin	40 mA
DC Current for 3.3V Pin	50 mA
Flash Memory	32 KB of which 0.5 KB used by bootloader
SRAM	2 KB
EEPROM	1 KB
Clock Speed	16 MHz

the board



Power

The Arduino Uno can be powered via the USB connection or with an external power supply. The power source is selected automatically.

External (non-USB) power can come either from an AC-to-DC adapter (wall-wart) or battery. The adapter can be connected by plugging a 2.1mm center-positive plug into the board's power jack. Leads from a battery can be inserted in the Gnd and Vin pin headers of the POWER connector.

The board can operate on an external supply of 6 to 20 volts. If supplied with less than 7V, however, the 5V pin may supply less than five volts and the board may be unstable. If using more than 12V, the voltage regulator may overheat and damage the board. The recommended range is 7 to 12 volts.

The power pins are as follows:

- **VIN.** The input voltage to the Arduino board when it's using an external power source (as opposed to 5 volts from the USB connection or other regulated power source). You can supply voltage through this pin, or, if supplying voltage via the power jack, access it through this pin.
- **5V.** The regulated power supply used to power the microcontroller and other components on the board. This can come either from VIN via an on-board regulator, or be supplied by USB or another regulated 5V supply.
- **3V3.** A 3.3 volt supply generated by the on-board regulator. Maximum current draw is 50 mA.
- **GND.** Ground pins.

Memory

The Atmega328 has 32 KB of flash memory for storing code (of which 0,5 KB is used for the bootloader); It has also 2 KB of SRAM and 1 KB of EEPROM (which can be read and written with the EEPROM library).

Input and Output

Each of the 14 digital pins on the Uno can be used as an input or output, using pinMode(), digitalWrite(), and digitalRead() functions. They operate at 5 volts. Each pin can provide or receive a maximum of 40 mA and has an internal pull-up resistor (disconnected by default) of 20-50 kOhms. In addition, some pins have specialized functions:

- **Serial: 0 (RX) and 1 (TX).** Used to receive (RX) and transmit (TX) TTL serial data. TThese pins are connected to the corresponding pins of the ATmega8U2 USB-to-TTL Serial chip .
- **External Interrupts: 2 and 3.** These pins can be configured to trigger an interrupt on a low value, a rising or falling edge, or a change in value. See the attachInterrupt() function for details.
- **PWM: 3, 5, 6, 9, 10, and 11.** Provide 8-bit PWM output with the analogWrite() function.
- **SPI: 10 (SS), 11 (MOSI), 12 (MISO), 13 (SCK).** These pins support SPI communication, which, although provided by the underlying hardware, is not currently included in the Arduino language.

- **LED: 13.** There is a built-in LED connected to digital pin 13. When the pin is HIGH value, the LED is on, when the pin is LOW, it's off.

The Uno has 6 analog inputs, each of which provide 10 bits of resolution (i.e. 1024 different values). By default they measure from ground to 5 volts, though is it possible to change the upper end of their range using the AREF pin and the analogReference() function. Additionally, some pins have specialized functionality:

- **I²C: 4 (SDA) and 5 (SCL).** Support I²C (TWI) communication using the Wire library.

There are a couple of other pins on the board:

- **AREF.** Reference voltage for the analog inputs. Used with analogReference().
- **Reset.** Bring this line LOW to reset the microcontroller. Typically used to add a reset button to shields which block the one on the board.

See also the mapping between Arduino pins and Atmega328 ports.

Communication

The Arduino Uno has a number of facilities for communicating with a computer, another Arduino, or other microcontrollers. The ATmega328 provides UART TTL (5V) serial communication, which is available on digital pins 0 (RX) and 1 (TX). An ATmega8U2 on the board channels this serial communication over USB and appears as a virtual com port to software on the computer. The '8U2 firmware uses the standard USB COM drivers, and no external driver is needed. However, on Windows, an *.inf file is required..

The Arduino software includes a serial monitor which allows simple textual data to be sent to and from the Arduino board. The RX and TX LEDs on the board will flash when data is being transmitted via the USB-to-serial chip and USB connection to the computer (but not for serial communication on pins 0 and 1).

A SoftwareSerial library allows for serial communication on any of the Uno's digital pins.

The ATmega328 also support I2C (TWI) and SPI communication. The Arduino software includes a Wire library to simplify use of the I2C bus; see the documentation for details. To use the SPI communication, please see the ATmega328 datasheet.

Programming

The Arduino Uno can be programmed with the Arduino software (download). Select "Arduino Uno w/ ATmega328" from the **Tools > Board** menu (according to the microcontroller on your board). For details, see the reference and tutorials.

The ATmega328 on the Arduino Uno comes preburned with a bootloader that allows you to upload new code to it without the use of an external hardware programmer. It communicates using the original STK500 protocol (reference, C header files).

You can also bypass the bootloader and program the microcontroller through the ICSP (In-Circuit Serial Programming) header; see these instructions for details.

The ATmega8U2 firmware source code is available . The ATmega8U2 is loaded with a DFU bootloader, which can be activated by connecting the solder jumper on the back of the board (near the map of Italy) and then resetting the 8U2. You can then use Atmel's FLIP software (Windows) or the DFU programmer (Mac OS X and Linux) to load a new firmware. Or you can use the ISP header with an external programmer (overwriting the DFU bootloader).

Shield Ethernet Arduino.

Arduino Ethernet Shield

Download: arduino-ethernet-shield-05-schematic.pdf, arduino-ethernet-shield-05-reference-design.zip

Download: arduino-ethernet-shield-schematic.pdf, arduino-ethernet-shield-reference-design.zip

The Arduino Ethernet Shield allows an Arduino board to connect to the internet. It is based on the Wiznet W5100 ethernet chip (datasheet). The Wiznet W5100 provides a network (IP) stack capable of both TCP and UDP. It supports up to four simultaneous socket connections. Use the Ethernet library to write sketches which connect to the internet using the shield. The ethernet shield connects to an Arduino board using long wire-wrap headers which extend through the shield. This keeps the pin layout intact and allows another shield to be stacked on top.

The latest revision of the shield adds a micro-SD card slot, which can be used to store files for serving over the network. It is compatible with the Arduino Duemilanove and Mega (using the Ethernet library coming in Arduino 0019). An SD card library is not yet included in the standard Arduino distribution, but the sdfatlib by Bill Greiman works well. See this tutorial from Adafruit Industries for instructions (thanks Limor!).

The latest revision of the shield also includes a reset controller, to ensure that the W5100 Ethernet module is properly reset on power-up. Previous revisions of the shield were not compatible with the Mega and need to be manually reset after power-up. The original revision of the shield contained a full-size SD card slot; this is not supported.

Arduino communicates with both the W5100 and SD card using the SPI bus (through the ICSP header). This is on digital pins 11, 12, and 13 on the Duemilanove and pins 50, 51, and 52 on the Mega. On both boards, pin 10 is used to select the W5100 and pin 4 for the SD card. These pins cannot be used for general i/o. On the Mega, the hardware SS pin, 53, is not used to select either the W5100 or the SD card, but it must be kept as an output or the SPI interface won't work.

Note that because the W5100 and SD card share the SPI bus, only one can be active at a time. If you are using both peripherals in your program, this should be taken care of by the corresponding libraries. If you're not using one of the peripherals in your program, however, you'll need to explicitly deselect it. To do this with the SD card, set pin 4 as an output and write a high to it. For the W5100, set digital pin 10 as a high output.

The shield provides a standard RJ45 ethernet jack.

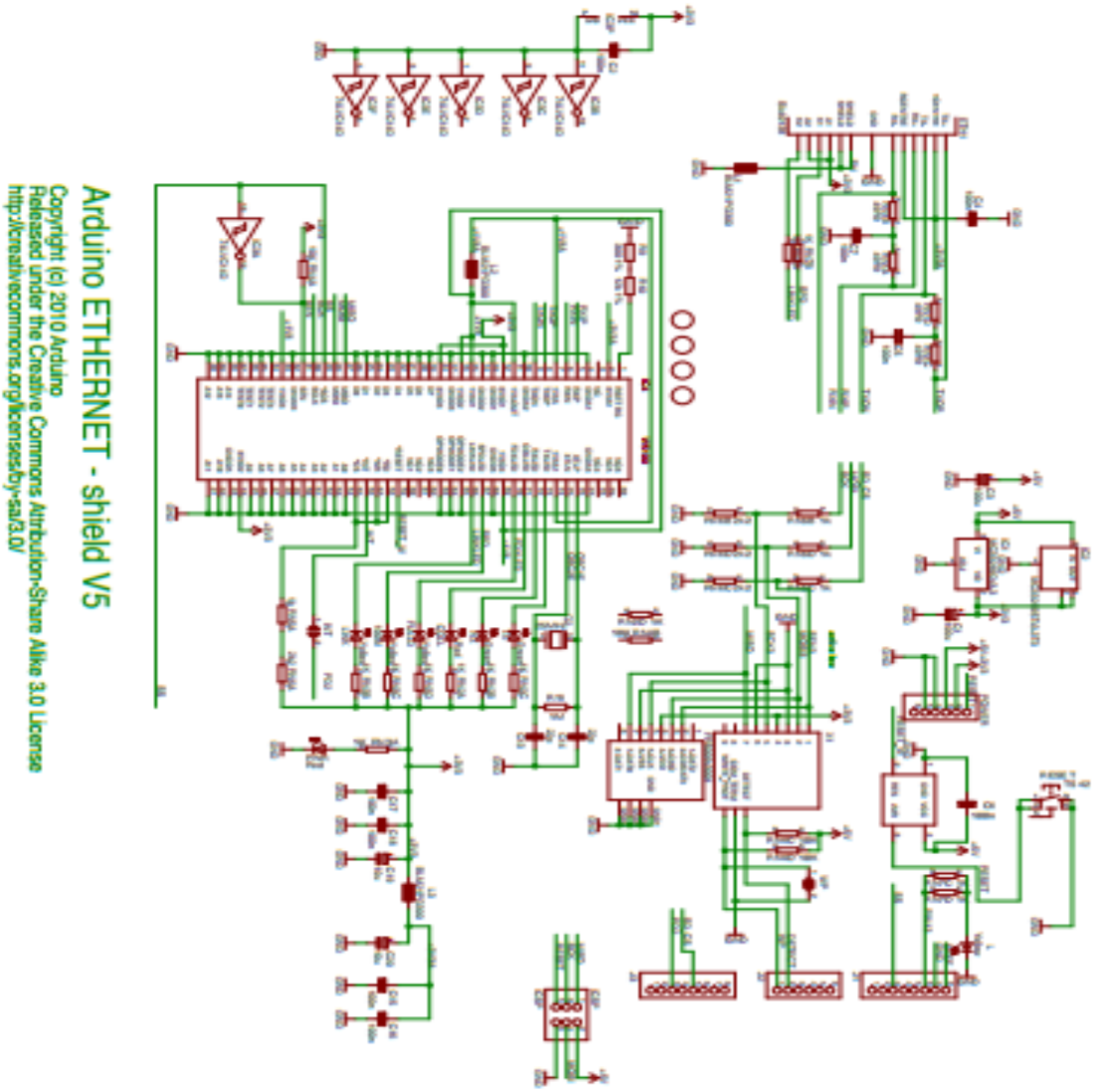
The reset button on the shield resets both the W5100 and the Arduino board.

The shield contains a number of informational LEDs:

- PWR: indicates that the board and shield are powered
- LINK: indicates the presence of a network link and flashes when the shield transmits or receives data
- FULLD: indicates that the network connection is full duplex
- 100M: indicates the presence of a 100 Mb/s network connection (as opposed to 10 Mb/s)
- RX: flashes when the shield receives data
- TX: flashes when the shield sends data
- COLL: flashes when network collisions are detected

The solder jumper marked "INT" can be connected to allow the Arduino board to receive interrupt-driven notification of events from the W5100, but this is not supported by the Ethernet library. The jumper connects the INT pin of the W5100 to digital pin 2 of the Arduino.

See also: getting started with the ethernet shield and Ethernet library reference



Anexo 7. INSTALACIÓN DEL SISTEMA DE SEGURIDAD AUTOMATIZADO.

Caja de alojamiento del sistema de control de acceso.

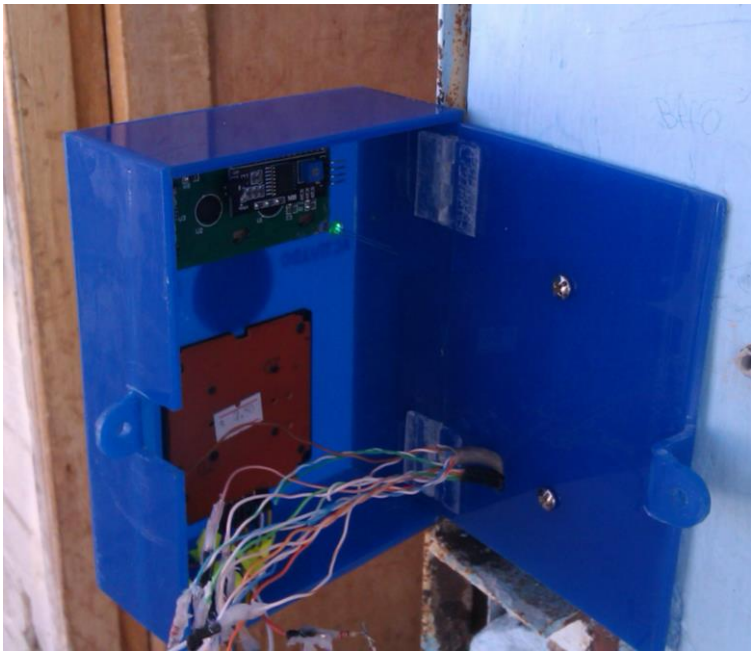
Vista lateral del tablero de control Arduino.

Tablero de control etiquetado.

Colocación de la cerradura electromagnética.

Colocación del pulsador manual para la cerradura electromagnética.

Sistema de desactivación manual terminada.



Armado de la caja de validación de contraseña que incluye la LCD, teclado, LED´s y buzzer.

Rack ubicado en el laboratorio de computación donde están alojados los dispositivos que interconectan la red LAN privada.