DISEÑO DE UN PROTOTIPO DE SEGURIDAD PARA EL RESGUARDO DE LA INFORMACIÓN FÍSICA Y DIGITAL DEL SALÓN ESPECIALIZADO DE LA CET COLSUBSIDIO (INFRAESTRUCTURA TECNOLÓGICA Y SEGURIDAD EN REDES)

HELBER LEANDRO BAEZ RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, COLOMBIA
2020

DISEÑO DE UN PROTOTIPO DE SEGURIDAD PARA EL RESGUARDO DE LA INFORMACIÓN FÍSICA Y DIGITAL DEL SALÓN ESPECIALIZADO DE LA CET COLSUBSIDIO (INFRAESTRUCTURA TECNOLÓGICA Y SEGURIDAD EN REDES)

HELBER LEANDRO BÁEZ RODRÍGUEZ

Proyecto Aplicado a la Seguridad Física de la Información en el Salón Especializado de la CET

Director:
Yolima Esther Mercado Palencia
Ingeniera de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, COLOMBIA
2020

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, 26 de mayo de 2020

AGRADECIMIENTOS

El proyecto aplicado es un gran reto que permite integrar y conocer varios aspectos relevantes para su consecución, es así como en el camino se encuentran personas e instituciones que permiten que las metas que se plantean se puedan ir cumpliendo hasta conseguir el objetivo propuesto. Resalto el apoyo del Ingeniero Electrónico Libardo Gómez, quien con su conocimiento en electrónica permitió que se fueran dando las posibilidades con el fin de lograr la funcionabilidad del prototipo, a la Líder de Investigación de la Corporación de Educación Tecnológica Colsubsidio – Airbus Group Leidy Torres por su aporte a nivel de estructura, redacción y conocimiento en las normas de presentación, a la Directora de Proyecto Yolima Mercado por sus aportes y exigencias a nivel técnico.

Por último, quiero dar mis más sinceros agradecimientos a la Corporación de Educación Tecnológica Colsubsidio - Airbus Group, quienes facilitaron el acceso a sus instalaciones (Salón1201) para realizar las diferentes pruebas con el prototipo, también por el patrocinio para la presentación de la ponencia derivada de este proyecto en el Congreso Internacional “Cientecg” realizado en Medellín, obteniendo como logro significativo, la publicación del artículo en la Revista Modum del Sena.

CONTENIDO

pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

Seguridad Informática: métodos y procedimientos que permiten asegurar los diferentes recursos físicos y de sistemas de información, para evitar ataques de ciberdelincuentes o cracker a las Compañías.

Arduino: placa usada como medio para la ejecución de diferentes proyectos, la cual contiene componentes de hardware y software libre para interactuar y hacer uso de recursos electrónicos de bajo costo.

Sensores Arduino: componentes electrónicos que permiten ejecutar una acción específica dependiendo de la necesidad del proyecto, estos componentes deben ser instalados en la placa Arduino y programados para verificar su funcionamiento.

Software Libre Arduino Nightly: software Libre que permite programar la placa de Arduino, con el fin de configurar los sensores y componentes en los diferentes pines.

AppInventor: programa gratuito en línea que permite generar proyectos de creación de aplicaciones móviles, basados en programación por bloques.

Xampp: software libre para gestión de bases de datos, enlazadas con código abierto, para simulaciones con páginas o aplicaciones.

Criptografía: elemento primordial de la Seguridad Informática que permite asegurar la información mediante procesos de encriptación de archivos generando claves, firmas digitales, certificados, que solo el propietario y a quien se remite, puedan tener acceso. De este modo se evita que los intrusos accedan fácilmente a la información encriptada.

Riesgo y control informático: la prevención es un pilar dentro de la seguridad informática el cual permite determinar los riesgos que puede haber en una empresa con respecto a los procesos que se realizan en una Organización

Análisis de riesgos: proceso en el cual se toman diferentes metodologías, con el fin de identificar las vulnerabilidades de las organizaciones con respecto al manejo de la seguridad de la información.

Sistemas de seguridad de información: Métodos, técnicas y sistemas físicos o lógicos, que permiten implementar barreras de control de acceso.

Aspectos éticos y legales: En la Seguridad Informática, se cuenta con un apoyo vital y es el apoyo de las Normas y leyes que permiten controlar los aspectos legales en cuanto a fraudes y demás delitos, y en cuanto a las normas, permiten llevar un protocolo de implementación llevando un proceso dado por la Norma, de esta forma se trabaja de forma organizada.

RESUMEN

En la Corporación de Educación Tecnológica Colsubsidio se implementó un salón de clases especializado en redes para la formación en el área de las TIC (Tecnologías de la Información y la Comunicación) en el Programa de Infraestructura Tecnológica, este salón cuenta con equipos de alto costo para las diferentes prácticas en redes donde se resguarda información y programas de las prácticas que realizan los estudiantes, por lo tanto, requieren de mayor control de acceso ya que pueden ser hurtados por la gran afluencia de público externo y personal interno sin autorización.

En el salón especializado se manejan dos cámaras de control de acceso, una en el pasillo y otra al interior del salón, mas no un sistema de alertas de seguridad, es así como el prototipo contribuye en asegurar los equipos que se encuentran en el salón, incluyendo la información que allí permanece, garantizando el apoyo a la seguridad con el sistema de alertas; se espera que con este prototipo se generen alertas sobre el ingreso no autorizado, permitiendo ser un aporte importante en pro de la seguridad de los equipos que están disponibles para la formación en redes los cuales tienen un costo elevado.

Según el Decano de la Facultad de Ingenierías Alejandro Castillo y el líder de la Línea de TIC Iván Vela, encargados y responsables del ambiente especializado, el prototipo es pertinente para el aseguramiento de los equipos informáticos y de redes que se encuentran dentro del ambiente y es un apoyo relevante a la seguridad de la información que manejan los Docentes en las diferentes cátedras.

Como resultado se busca obtener un prototipo implementado en el ambiente especializado de la Corporación de Educación Tecnológica Colsubsidio, en donde se ejecuten las pruebas necesarias de funcionamiento y en donde el encargado del ambiente verifique los resultados para dar el visto bueno sobre el objetivo de asegurar los equipos tecnológicos y de redes utilizados para las prácticas de las cátedras que allí se desarrollan, como también la información generada de estas prácticas mostrando la importancia de tener un valor agregado a la hora de proteger la infraestructura tecnología de la Corporación.

INTRODUCCION

La Seguridad de la Información y de equipos que hacen parte de la Infraestructura de las tecnologías de la información y la comunicación (TIC) se está convirtiendo en una necesidad y prioridad en las Empresas, por esta razón se requieren de sistemas de apoyo que permitan resguardar la información y protegerla, como también a los equipos tecnológicos que gestionan y ejecutan procesos sobre los datos.

Este proyecto permite proporcionar una nueva alternativa para las Empresas generando confianza sobre la protección de la información a nivel físico, teniendo un control y seguimiento constante sobre el personal que ingresa a sus instalaciones, por esta razón se trabajó sobre un prototipo que permite detectar el ingreso no autorizado de las personas al salón especializado de la CET, donde se encuentran equipos informáticos de alto costo, de este modo se establecen los objetivos para el diseño y la construcción, así como la implementación de una aplicación que por medio de una base de datos registre los diferentes eventos.

Se obtiene un prototipo funcional que, al detectar un acceso no autorizado, genera una alerta la cual quedará registrada en una base de datos, dando una solución a la corporación en cuanto al apoyo en la seguridad de los equipos, convirtiéndose en un valor agregado a los sistemas de control actuales. A nivel general, el funcionamiento, está basado en componentes electrónicos, como la placa Arduino que, por medio de sensores conectados y programación de la placa, proporcionan un enlace hacia una aplicación que permite detectar las intrusiones, la cual se desarrolla en software libre y esta a su vez permite generar los registros en una base de datos.

Este sistema proporciona un valor agregado para la seguridad del Salón 1201 de la Corporación de Educación Tecnológica Colsubsidio en donde se resguardan componentes tecnológicos muy costosos, por lo tanto, el prototipo aporta en gran medida, como sistema de alarma de intrusión, con el fin de generar confianza en la administración de los equipos y en caso de hurto, se genere la alerta en tiempo real. Se destaca que es insuficiente el sistema de cámaras y que la puerta no cuenta con sistemas de seguridad acordes a las necesidades de este tipo de salones.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En la actualidad, los controles se realizan por medio de sistemas de seguridad con cámaras, sensores de movimiento, sistemas biométricos, los cuales permiten controlar y monitorear el acceso no autorizado a los data center de las organizaciones o ambientes donde se encuentran equipos de redes o de cómputo, estos sistemas son eficientes con el propósito de mantener la integridad de la información, sin embargo, las características de estos sistemas permiten que los primeros en obtener la información de una intrusión sean los que resguardan la seguridad del edificio o del que vigila las cámaras.

Estos sistemas guardan el video y permiten identificar a las personas que accedieron a los diferentes salones del edificio en la sede principal de la Corporación, de manera no autorizada. Actualmente se buscan métodos más eficientes, ya que estos sistemas pueden ser burlados mediante engaños lo que impide que se maneje la información de manera eficaz al momento del ingreso a un *datacenter*, o ambientes con equipos de alto costo como en el caso de la CET donde se tienen salones con equipos informáticos y de comunicaciones de gran valor.

Por último, los sistemas que se manejan por medio de cámaras tienen un valor aproximado de más de $800.000 pesos sin incluir el costo del computador de vigilancia o resguardo de la información en caso de que la empresa no cuente con este equipo, lo que conlleva a que las empresas pequeñas, no tengan el presupuesto para adquirir estos equipos, por esta razón pueden tener una opción más económica al implementar el prototipo de detección de accesos no autorizados, como un valor agregado a los sistemas de seguridad que actualmente manejan en la Corporación.

1.2 PLANTEAMIENTO DEL PROBLEMA

En la Corporación de Educación Tecnológica Colsubsidio, hay una sede en Chapinero en donde se encuentran ubicados los salones para los diferentes programas que se ofrecen, en estos salones se asignan las cátedras de las diferentes carreras de formación, tres pertenecen a la Facultad de Ingenierías y Ciencias Básicas, la facultad cuenta con salones para cátedras transversales y para cátedras especializadas donde se resguardan elementos de gran valor monetario.

En el salón 1201, el cual pertenece al nivel 6 de la sede de chapinero, anteriormente era un ambiente básico el cual se utilizaba para el trabajo con los estudiantes, en clases como matemáticas, inglés, entre otros, las cuales no implicaba el uso de equipos tecnológicos especializados, con el tiempo este salón fue adaptado como espacio para las carreras de la Facultad de Ingeniería y Ciencias Básicas, donde se ubicaron equipos de cómputo con características optimas, además, equipos de redes, servidores, herramientas y elementos para prácticas de cátedras especializadas.

Respecto a lo anterior, se vio la necesidad de implementar un sistema de apoyo a la seguridad del ambiente especializado por el costo de los equipos que allí se encuentran, dando un aporte significativo a la seguridad del salón, ya que por medio del prototipo se dará a conocer en tiempo real la alerta al encargado de seguridad y a las personas responsables del ambiente, obteniendo una barrera más de acceso a los equipos de red.

Actualmente se cuenta con dos cámaras ubicadas de la siguiente forma: una en el pasillo del nivel 12 y una en el interior del salón 1202 en la parte superior de la puerta, además de una chapa estándar de ingreso, lo anterior no garantiza un 100% de seguridad, se pretende con este prototipo brindar un valor agregado para garantizar la seguridad de los equipos, en tiempo real y con datos de registro sobre las alertas de los accesos no autorizados.

1.3 FORMULACION DEL PROBLEMA

Los sistemas diseñados con el fin de evitar una intrusión proporcionan confianza sobre la generación de entornos más seguros, donde el acceso es controlado y registrado, con el fin de asegurar los componentes, elementos y equipos que hacen parte de los activos de las tecnologías de la información y comunicación de una Empresa.

Actualmente, los sistemas contra ingresos no autorizados están muy avanzados impidiendo el acceso de las personas no registradas, intrusos que buscan la forma de evadir la seguridad e ingresar a los espacios de interés para cometer delitos, de este modo el prototipo permite ser un plus para apoyar los diferentes sistemas de seguridad de la Corporación, aunque se evidencia resultados y permiten dar tranquilidad, son beneficiosos en la detección en tiempo real. Lo anterior no quiere decir que el dispositivo va a permitir reemplazar los sistemas actuales, el objetivo es que se logre una interacción entre el administrador encargado de los salones con equipos de cómputo y las alertas generadas en tiempo real cuando se evidencie un acceso no autorizado, a futuro puede ser un complemento de trabajo interdependiente para generar mayor seguridad como, por ejemplo, enlazarlo con la cámara para obtener datos más precisos.

¿Cómo la implementación de un prototipo funcional de detección de intrusos permite contribuir con el resguardo de la información física y digital del salón especializado de la CET Colsubsidio?

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Diseñar un prototipo que permita el control del acceso al salón especializado de redes ubicado en la CET Colsubsidio, registrando, almacenando y generando las alertas de ingresos no autorizados.

2.2 OBJETIVOS ESPECÍFICOS

- Identificar los componentes necesarios para la construcción del prototipo.
- Desarrollar una base de datos para los registros de las alertas establecidas.
- Construir un prototipo con los componentes establecidos para la ejecución de pruebas.
- Documentar las pruebas requeridas para que el dispositivo realice las acciones de seguridad.

3. JUSTIFICACIÓN

Luego de la verificación realizada en el aula especializada, se determina que la seguridad de dos cámaras (una en el pasillo y la otra dentro del salón) y que la puerta no tiene las chapas de seguridad adecuadas, se encuentra la necesidad de implementar un prototipo de seguridad que permita alertar de manera real al encargado del área de sistemas de la Cet o responsable del ambiente especializado, de manera silenciosa, y sin que el intruso observe que ha sido detectado, generando eficiencia en el proceso, ya que el dispositivo no estará ubicado en el aire si no a una altura menor, en donde al dar el paso o simplemente al abrir la puerta el intruso activará el dispositivo, y a la vez se enviara la alarma al dispositivo móvil del personal autorizado, generando la alerta.

Este prototipo permite dar a conocer la importancia de que se invierta en este tipo de dispositivos que acompañan los demás sistemas de seguridad y que es un valor agregado para el aseguramiento físico de los equipos de redes y de cómputo donde será implementado mediante un dispositivo con Arduino y sensores, el cual proporciona además de la generación de alertas, servicios complementarios como el registro de los ingresos al salón especializado en una base de datos, que a futuro pueda estar encriptada para la integridad de los mismos, alertas al dispositivo móvil en horarios no hábil, comunicación vía wifi con el dispositivo con los respectivos sensores y una app de activación del dispositivo para control de vigilancia en los momentos en que no se tenga presencia de personal en horarios no laborales.

Es importante destacar que este dispositivo puede ser un valor agregado a los sistemas de seguridad de la información existente en la compañía, que genere confianza y mayor control del acceso a los equipos físicos de control de procesos del ambiente especializado de la CET (servidores, centros de cableado, entre otros equipos de red).

Se destaca que la razón primordial del diseño del prototipo es aportar a la seguridad de los componentes de red del ambiente especializado de redes con el fin de garantizar el material educativo para los estudiantes que ejecutan sus prácticas y que dependen de estos recursos tecnológicos para su aprendizaje y conocimiento sobre el área de trabajo.

Este proyecto permite afianzar los conocimientos de seguridad informática y descubrir que sí se puede dar un aporte significativo a las organizaciones, además, de aplicar un sistema que puede dar buenos resultados a nivel de seguridad, lo cual permite mostrar apropiación sobre el conocimiento adquirido en la Universidad y de lo que se promueve en cuanto a trabajo autónomo.

El aprovechamiento tecnológico y el estar a la vanguardia, permiten asegurar la información de una Compañía. Diaz, et al[1] consideran que es un activo valioso, el cual debe protegerse, en donde vale la pena invertir generando disciplina en la seguridad no solo en las personas que trabajan para la organización sino para los clientes que interactúan con ella y que con confianza entregan sus datos.

[1] DIAZ, Andrés, et al. Implementación de un sistema de gestión de seguridad de la información. En: *Sistemas de gestión de seguridad de la información* [en línea]. Bogotá: Fundación Universitaria Konrad Lorenz, 2 p. [Consultado: 13 de abril de 2019]. Disponible en http://www.konradlorenz.edu.co/images/stories/articulos/SGSI.pdf

4. MARCO DE REFERENCIA

4.1 MARCO TEORICO

En la Seguridad Informática, se debe tener en cuenta los siguientes aspectos según Costas. “El concepto de CIDAN, las cuales son las características esenciales de protección de la Información (Confidencialidad, Integridad, Disponibilidad, Autenticación, No Repudio)”[2]

Estas características se refieren a la forma como se debe cuidar la información, aprender a cifrar los mensajes por medio de una contraseña, donde se puede realizar de manera simétrica o asimétrica. Básicamente simétrico se refiere a que con la misma clave puedo acceder al mensaje del receptor y el remitente y asimétrico en donde una clave es para que el emisor envié el mensaje y el receptor tiene otra clave para visualizarlo.

La seguridad física enfocada a la información es parte fundamental de una compañía, sin embargo, en ocasiones no se destinan los recursos necesarios generando vulnerabilidades y riesgo en la inversión en los recursos de protección de la información, es así como los equipos deben estar en áreas protegidas de manera física como es mencionado en el artículo digital de Gutiérrez[3] de la compañía *eset*, destacando la necesidad de garantizar que los equipos informáticos se encuentren en un ambiente seguro y con las medidas necesarias de protección.

Marrero[4] emplea el termino de seguridad física y lo aborda para referirse como la seguridad externa de los datos. Es un riesgo el cual no debe ser pasado por alto, se encuentran vulnerabilidades como el de que un empleado o exempleado cuando este puede acceder al área donde se encuentren equipos con información relevante,

---

[2] COSTAS SANTOS, Jesús. *Seguridad informática*. [en línea]. España: Ra-Ma. 2014. [Consultado: 18 de abril de 2019]. Disponible en: Base de datos UNAD – e-libro. https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/detail.action?docID=3228430

[3] GUTIERREZ AMAYA, Camilo. *La seguridad física como parte integral de la seguridad de la información*. Welivesecurity, 29 de enero de 2013. [Consultado: 25 de abril de 2019]. Disponible en https://www.welivesecurity.com/la-es/2013/01/29/seguridad-fisica-como-parte-integral-seguridad-informacion/

[4] MARRERO TRAVIESO, Yran. La Criptografía como elemento de la seguridad informática. En: *SCIELO: ACIMED* [en línea]. Ciudad de la Habana, nov-dic de 2003. vol. 11, nro. 6. [Consultado: 01 de mayo de 2019]. Disponible en http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012&lng=es&nrm=iso. ISSN: 1024-9435.

la cual puede ser copiada por diferentes medios y luego enviada por diferentes medios físicos y lógicos a los ciberdelincuentes o a la competencia. Una de las vulnerabilidades es que un empleado puede tener acceso a todos los sitios donde se encuentren equipos, para el encargado de seguridad es transparente y no va tener la mínima sospecha sobre un robo de información que se pueda cometer, como el empleado está autorizado ingresa y puede tomar la información sin ningún inconveniente, sin embargo, con los sistemas de seguridad de apoyo, se puede detectar las horas de ingreso y esto previene que si el servidor registra un proceso de copiado, de envío de información, o ingreso de un medio extraíble para robar la información, los sistemas registrarán la hora de acceso para luego reportar y evidenciar quién accedió al área para cometer el delito informático.

Conociendo lo anterior, el aseguramiento de manera física es un factor a tener en cuenta en las compañías y son las bases para comprender la importancia de proteger la información, la forma como se puede cifrar los mensajes, asignando las claves; no es conveniente manejar una misma clave para todas las cuentas, es importante tener varias y si es posible tener una por cuenta ya que si el intruso descubre la clave puede acceder a todos los servicios en donde esté inscrito, y sería de una manera fácil obtener todo el acceso.

La prevención de intrusiones es un tema fundamental que tienen en cuenta las organizaciones para implementar estrategias orientadas a evitar la pérdida de información y velando por su protección, ya que son varios los factores que hacen que un equipo este desprotegido, por ejemplo, un apagón donde un equipo que este encendido se apaga inmediatamente, en ese momento en caso de estar trabajando en un archivo y no se ha guardado el sistema no va a ser recuperado, es así, como se usan métodos de protección, en donde se puede apoyar con un sistema de UPS y reguladores de corriente eléctrica, las cuales soportan la carga después de un apagón por un tiempo determinado con los equipos prendidos dependiendo de las características, capacidades y estado del equipo, en ese tiempo el usuario tiene la disponibilidad de uso del recurso, sin embargo, se espera que no continúe trabajando, sino que en este tiempo guarde los archivos, cierre todas ventanas y apague los equipos.

Por otro lado, cuando se tiene un servicio de gestión sobre los usuarios dentro de la aplicación de celular la cual controla las alertas del prototipo, esto permite, crear y asignar la contraseña por cada cuenta, para que sea la persona autorizada la que ingrese a los servicios de la aplicación, de esta forma se restringe que ingrese

cualquier persona a la información de la Compañía, Roa[5] plantea que en las Empresas se ve muchas veces que solo asignan un usuario y contraseña por departamento, en donde las implicaciones son grandes, porque si uno de los usuarios del grupo ingresa y borra de manera accidental el archivo o el contenido, quien debe hacerse responsable es quien tenga los privilegios, y si este la dio sin pensar en las consecuencias pues se va a dar cuenta que a él es a quien le asignaron la responsabilidad, porque la base de datos registra la hora del acceso al salón.

De acuerdo con lo anterior, ese tipo de acciones pueden ser consideradas como un delito informático, es así como se requiere un control continuo en las aplicaciones, dando un parte de tranquilidad a los usuarios y a la compañía que confía en los datos registrados y en la Plataforma de acceso.

Las buenas prácticas de seguridad en la Información evitan que se den reprocesos en las compañías, evitando perdida de información, sin embargo, esto se puede evitar si los usuarios acatan las políticas de la Organización teniendo en cuenta la forma adecuada de gestionar la información y del manejo de esta.

La Norma ISO 27001 es una de las normas que actúa como marco referencial para un buen manejo en el sistema de seguridad de la información en las compañías, teniendo en cuenta las vulnerabilidades, la gestión de los riesgos sobre los activos, para luego dar a conocer los controles que se deben trabajar o implementar en la organización para asegurar la información, con el compromiso del personal y de quienes manejan todas las políticas y control de los diferentes procesos relacionados con el manejo adecuado de la información.

[5] ROA BUENDÍA, Jose Fabián. Seguridad informática. 2 ed. España: McGraw-Hill Interamericana. 2013, 9 p. ISBN: 978-84-481-8569-5.

4.2 MARCO CONCEPTUAL

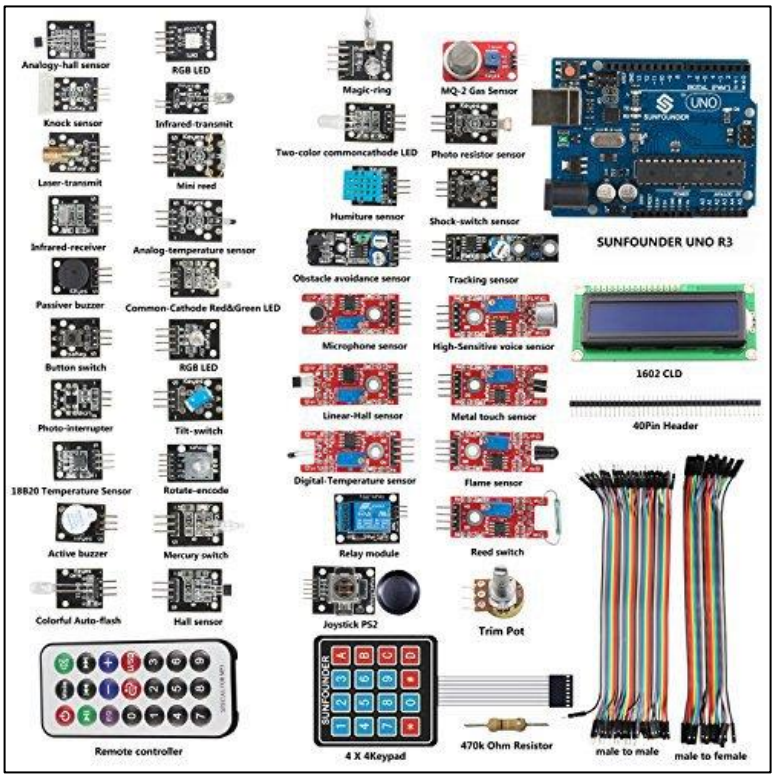
En este marco se describen los elementos, componentes y programas, que hacen parte a nivel general y especifico del desarrollo del proyecto. Se especifican componentes que, aunque no son parte del proyecto, permite dar claridad de la forma como se puede seleccionar una placa de Arduino, dependiendo la necesidad del proyecto, generalmente se conoce en el mercado la placa Arduino UNO, sin embargo, se evidencia gran variedad de placas, con diferentes funciones adaptables al objetivo que se busca. Desde placas para proyectos micro, hasta placas robustas adaptables a videojuegos.

4.2.1 Sensores: Cumplen la función de detección en el prototipo, con el fin de realizar los diferentes eventos programados, según las configuraciones desarrolladas. En el mercado se pueden encontrar diferentes tipos de sensores, de temperatura, movimiento, distancia, calor, entre otros. Para el proyecto aplicado se usaron, el sensor emisor laser, donde su función es la de emitir el haz de luz y el sensor receptor del haz de luz laser, en el proceso de configuración, se establece el evento o la acción en el proceso de interrupción, generando los diferentes eventos y alertas en la aplicación móvil. Los sensores cumplen un papel vital en la interacción con los diferentes proyectos, permitiendo hacer realidad casi que cualquier objetivo, facilitando los procesos de las organizaciones.

La adaptabilidad con la placa Arduino, hace que en el mercado se encuentren kits completos con variedad de sensores, lo mejor es que el costo es muy bajo siendo asequible para los que quieran probar diferentes opciones de proyectos, en cuanto a requerimientos y características existen sitios web con grupos de Arduino en diferentes medios, lo cual facilita la interacción generando apoyo para los objetivos que se quieran alcanzar.

Además de los sensores utilizados en el prototipo objeto del proyecto aplicado implementado en la Corporación, en la Figura 1, se encuentran variedad de componentes que permiten realizar diferentes proyectos ajustándose a las necesidades en las diferentes áreas donde se requiere optimizar los procesos o adquirir información de manera ágil con reportes automáticos de manera automatizada, generando informes periódicos o relacionando gráficos de soporte en apoyo a los resultados que se requieren adquirir, como de temperatura, presión, distancia, movimiento, y muchos más.

Figura 1. Tipos de sensores

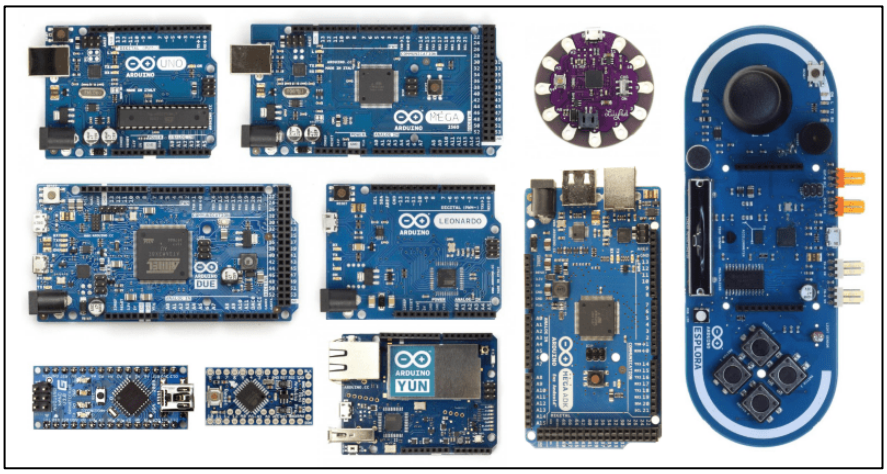


Fuente: Otros sensores [imagen]. En: Aprendiendo Arduino. 2018. [Consultado: 21 de marzo de 2019]. Disponible en: https://aprendiendoarduino.wordpress.com/2018/04/14/sensores-arduino-3/#comment-19063

4.2.2 Arduino UNO: Placa electrónica de hardware libre, programable, cumple la función de interconectar los diferentes componentes de acuerdo con la arquitectura de cada uno de sus pines.

Permite la interacción de componentes, esta placa puede ser configurable con el fin de programar las acciones, de este modo simular los resultados del código. Este código se programa mediante la aplicación Arduino nightly. En la Figura 2, se dan a conocer los diferentes tipos de placa que se pueden encontrar en el mercado dependiendo de las necesidades del proyecto y los requerimientos de este. Generalmente se pueden encontrar varios tamaños por comodidad y adaptación del dispositivo o prototipo a construir.

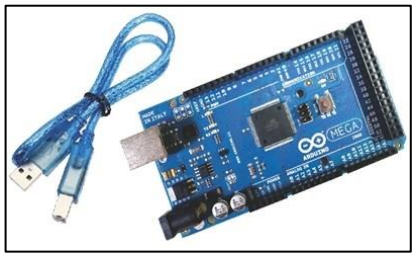
Figura 2. Tipos de placas Arduino



Fuente: Elegir la placa Arduino adecuada para tu proyecto [imagen]. En: patagoniatec. 2019. [Consultado: 30 de marzo de 2019]. Disponible en: https://saber.patagoniatec.com/2019/08/elegir-la-placa-arduino-adecuada-para-tu-proyecto/

4.2.3 Arduino MEGA: Este tipo de placa es más grande que el Arduino UNO, las características son diferentes en cuanto a que los pines de adaptabilidad de Hardware y de Software vienen en la parte de atrás. En la Figura 3, se puede evidenciar en detalle la estructura de la placa y la distribución de los componentes.

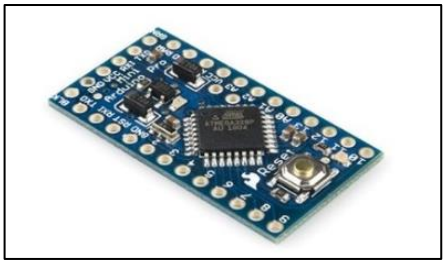
Figura 3. Arduino Mega



Fuente: Sin autor. Elegir la placa Arduino adecuada para tu proyecto [imagen]. En: patagoniatec. 2019. [Consultado: 06 de abril de 2020]. Disponible en: https://saber.patagoniatec.com/2019/08/elegir-la-placa-arduino-adecuada-para-tu-proyecto/

4.2.4 Arduino Pro Mini: tiene la misma funcionabilidad de un Arduino UNO, se adapta fácilmente a proyectos pequeños, ideal para robots. En la Figura 4, se evidencia el tamaño de la placa.

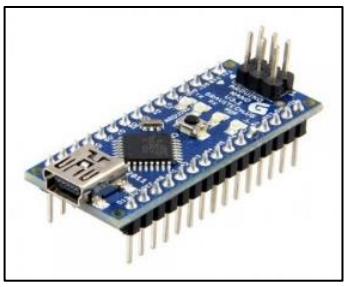
Figura 4. Arduino Pro Mini



Fuente: Elegir la placa Arduino adecuada para tu proyecto [imagen]. En: patagoniatec. 2019. [Consultado: 06 de abril de 2020]. Disponible en: https://saber.patagoniatec.com/2019/08/elegir-la-placa-arduino-adecuada-para-tu-proyecto/

4.2.5 Arduino NANO: Es una placa diseñada para trabajo en Protoboard evitando el uso de cables directos de la placa a los pines de un Arduino normal. En la Figura 5, se muestra la forma de los pines para adaptación en la Protoboard.

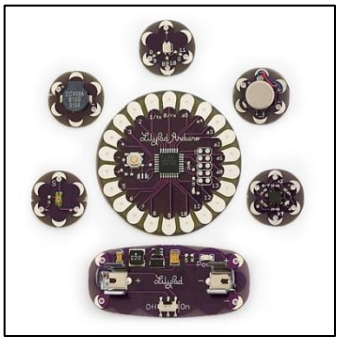
Figura 5. Arduino NANO



Fuente: Elegir la placa Arduino adecuada para tu proyecto [imagen]. En: patagoniatec. 2019. [Consultado: 06 de abril de 2020]. Disponible en: https://saber.patagoniatec.com/2019/08/elegir-la-placa-arduino-adecuada-para-tu-proyecto/

4.2.6 Arduino Lilypad: Se adaptan a la ropa, calzado, relojes, pulseras con el fin de crear diferentes proyectos denominados *wearables* traducido como vestibles. En la Figura 6, se destacan los diferentes módulos que se pueden adaptar a los diferentes accesorios, generalmente son usados para tomar información y resguardar datos sobre el trabajo físico que realizan las personas, también pueden ser usados para controlas objetos con el movimiento de las manos, entre otras funcionabilidades que facilitan la vida diaria de las personas en las diferentes actividades que ejecutan en los procedimientos laborales o en el hogar.

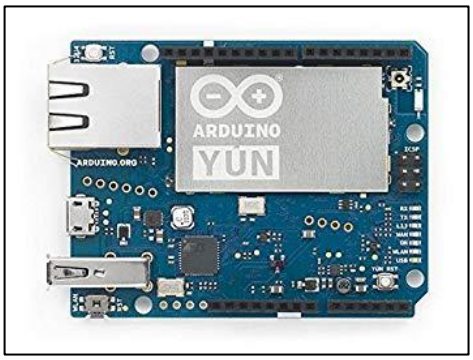
Figura 6. Arduino Lilypad



Fuente: Elegir la placa Arduino adecuada para tu proyecto [imagen]. En: patagoniatec. 2019. [Consultado: 06 de abril de 2020]. Disponible en: https://saber.patagoniatec.com/2019/08/elegir-la-placa-arduino-adecuada-para-tu-proyecto/

4.2.7 Arduino YUN: Placa desarrollada para trabajo con Linux y el internet de las cosas, sin embargo, no es considerada como una buena opción, debido a que tiene opciones avanzadas en la integración con la raspberry pi, la cual tiene mejor adaptación con software libre. En la Figura 7, se encuentra la estructura de la placa considerada como la competencia ideal para la integración con la automatización de procesos integrando cosas u objetos. Aún le falta terreno para llegar a ser tan potente como la raspberry pi, sin embargo, es una gran alternativa si se requiere reducir costos.

Figura 7. Arduino YUN.



Fuente: Elegir la placa Arduino adecuada para tu proyecto [imagen]. En: patagoniatec. 2019. [Consultado: 06 de abril de 2020]. Disponible en: https://saber.patagoniatec.com/2019/08/elegir-la-placa-arduino-adecuada-para-tu-proyecto/

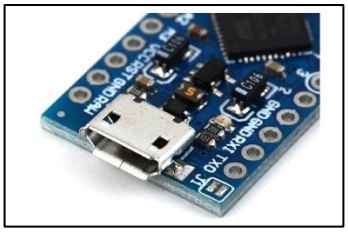
4.2.8 Arduino Leonardo: La ventaja de esta placa es que no requiere conversión serie a USB. Permite adaptar teclado y ratón. En la Figura 8, se muestran los diferentes componentes de la placa.

Figura 8. Arduino Leonardo.

Fuente: Elegir la placa Arduino adecuada para tu proyecto [imagen]. En: patagoniatec. 2019. [Consultado: 06 de abril de 2020]. Disponible en: https://saber.patagoniatec.com/2019/08/elegir-la-placa-arduino-adecuada-para-tu-proyecto/

4.2.9 Arduino Pro-Micro: Es una versión nano del Arduino Leonardo adaptado para *Protoboard.* En la Figura 9, se muestra en detalle el conector nativo de USB en él chip.

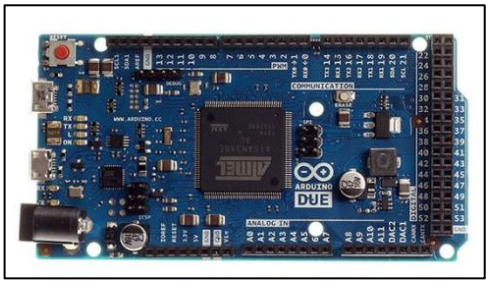
Figura 9. Arduino Pro-Micro.



Fuente: Elegir la placa Arduino adecuada para tu proyecto [imagen]. En: patagoniatec. 2019. [Consultado: 06 de abril de 2020]. Disponible en: https://saber.patagoniatec.com/2019/08/elegir-la-placa-arduino-adecuada-para-tu-proyecto/

4.2.10 Arduino DUE: Placa que trabaja con procesador de núcleo de 32 bits, lo que la hace más veloz y potente, sin embargo, se debe tener en cuenta que lo máximo de voltaje que soporta es de 3,3 V. En la Figura 10, se identifica él microprocesador.

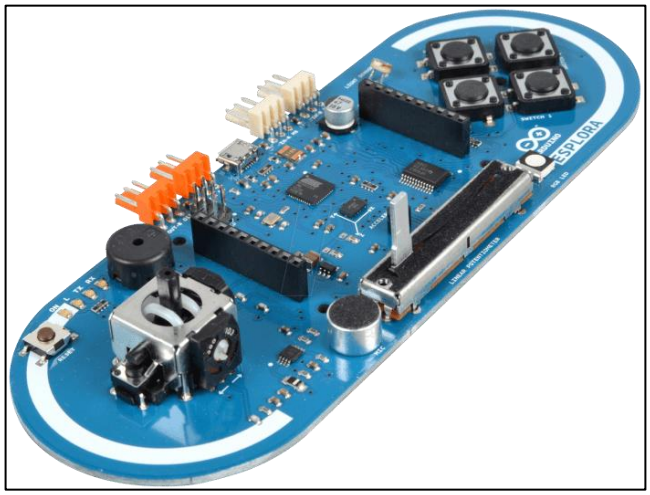
Figura 10. Arduino DUE.



Fuente: Elegir la placa Arduino adecuada para tu proyecto [imagen]. En: patagoniatec. 2019. [Consultado: 06 de abril de 2020]. Disponible en: https://saber.patagoniatec.com/2019/08/elegir-la-placa-arduino-adecuada-para-tu-proyecto/

4.2.11 Arduino Esplora: Esta placa permite programar sin tener muchos conocimientos en electrónica, la razón principal es porque tiene integrados varios sensores, lo cual facilita y ahorra tiempo. En la Figura 11, se visualizan los diferentes sensores y componentes de trabajo, es una de las placas más completas del mercado.

Figura 11. Arduino Esplora.



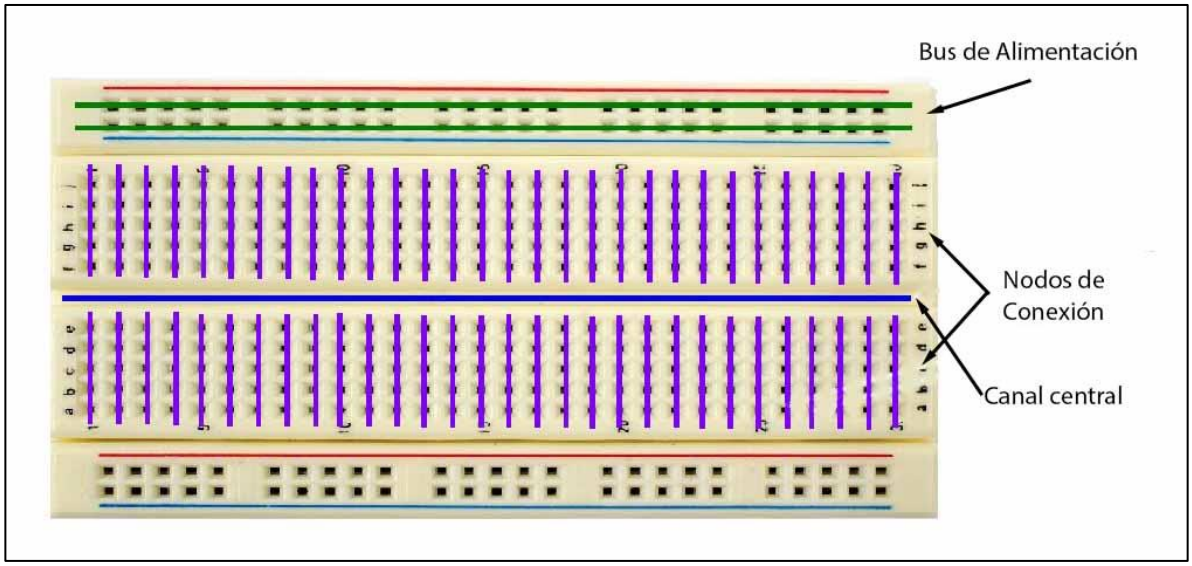
Fuente: Elegir la placa Arduino adecuada para tu proyecto [imagen]. En: patagoniatec. 2019. [Consultado: 06 de abril de 2020]. Disponible en: https://saber.patagoniatec.com/2019/08/elegir-la-placa-arduino-adecuada-para-tu-proyecto/

4.2.12 Protoboard: Placa para ejecución de pruebas de circuitos sin requerimiento de soldado, la cual permite conectar cualquier tipo de circuito, adaptado a las necesidades de cualquier tipo de proyecto a nivel electrónico.

Las placas se usan para cualquier tipo de experimentos y a mayor velocidad, ya que no requiere de un proceso de soldado, por lo tanto, los cables pueden ser retirados en cualquier momento, es importante realizar un diagrama previo de componentes con el fin de obtener mayor adaptación a la placa; también es necesario pelar los cables que van a hacer introducidos en los orificios para establecer contacto en el camino del circuito.

En la Figura 12, se describen las características en la *protoboard*, con el fin de conocer el estándar de conexión y los nombres de distribución, teniendo en cuenta el posicionamiento de los componentes que interactúan en el circuito. Se deben realizar los diferentes puentes de conexión para energizarla y de esta forma que el circuito obtenga el voltaje en cada uno de los componentes de prueba, en este proyecto quien proveía de corriente a la *protoboard*, era la placa Arduino.

Figura 12. *Protoboard* y características

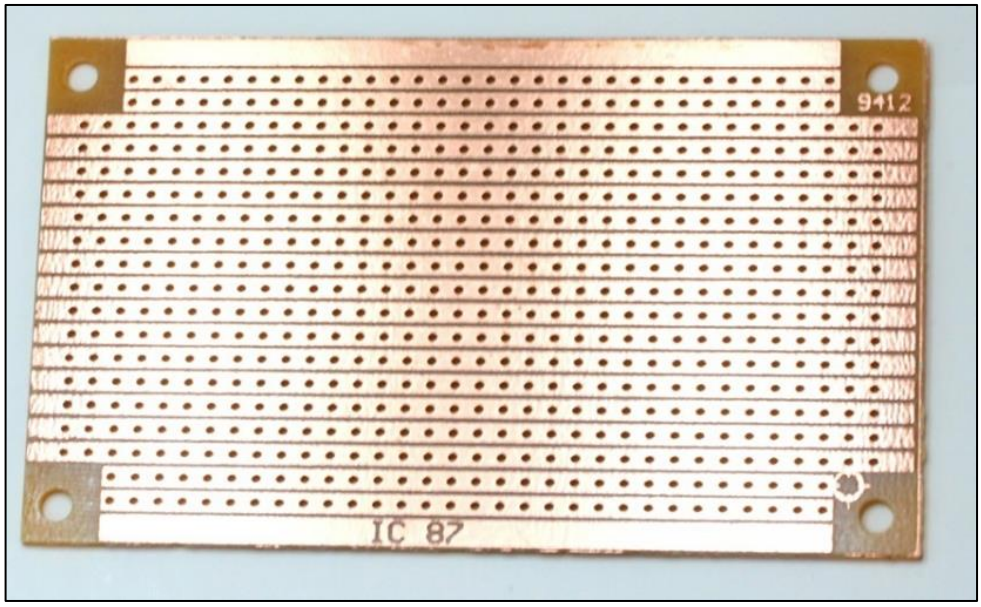


Fuente: DIOSDADO, Raúl. La *protoboard* [imagen]. En: zonamaker. 2018. [Consultado: 04 de abril de 2019]. Disponible en: https://www.zonamaker.com/electronica/intro-electronica/instrumentacion/la-protoboard

4.2.13 Baquela: Plástico sintético perforado, que permite ensamblar los circuitos de los componentes del prototipo, con los caminos de conexión proyectados y ejecutados según la distribución planteada. Generalmente se aplica el procedimiento de soldado después de la ejecución de pruebas en la protoboard, sin embargo, se requiere de práctica para realizar un buen procedimiento, porque en el caso de que queden dos puntos de soldadura unidos, generara que no funcione el circuito.

La Figura 13, muestra la forma de la baquela, con las diferentes perforaciones, las cuales permiten adaptar mediante el procedimiento de soldado el circuito y los caminos de interacción entre los componentes. Existen de diversos tipos y tamaños, de acuerdo con el requerimiento del proyecto, en este prototipo se adquirió una tarjeta estándar, la cual tiene el tamaño del interior de la caja donde quedó instalado el circuito junto con la placa Arduino, con el cableado y componentes en su interior.

Figura 13. Baquela

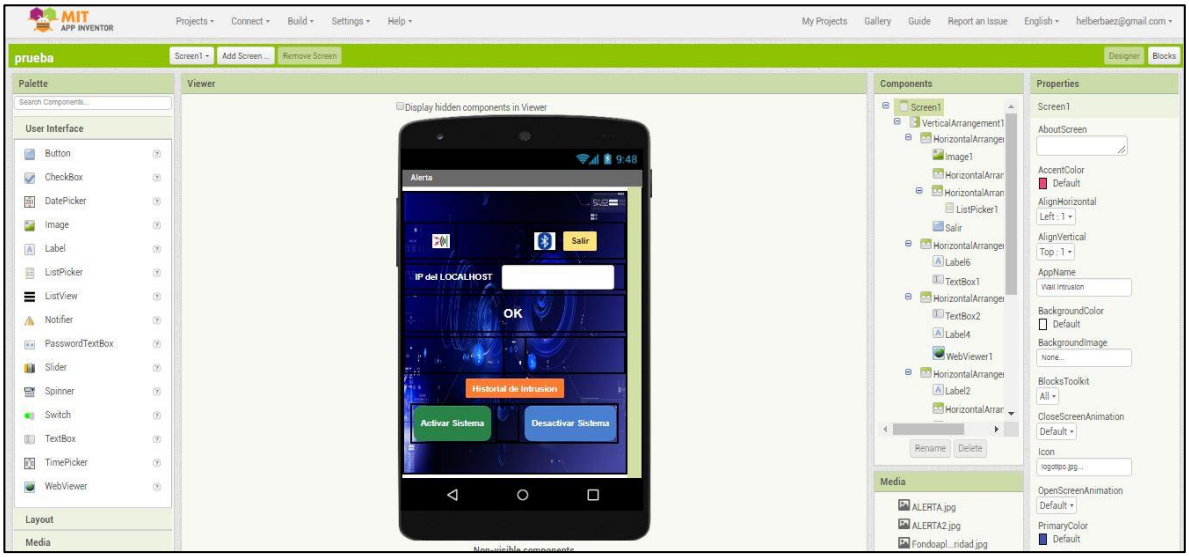


Fuente: DIOSDADO, Raúl. La protoboard [imagen]. En: zonamaker. 2018. [Consultado: 04 de abril de 2019]. Disponible en: https://www.zonamaker.com/electronica/intro-electronica/instrumentacion/la-protoboard

4.2.14 App inventor: Programa en línea que permite desarrollar aplicaciones mediante programación de bloques, tiene herramientas que permiten conectar dispositivos mediante bluetooth, wifi, a sistemas de bases de datos, el entorno gráfico es muy dinámico, la programación es relativamente sencilla, para realizar la navegación en los diferentes módulos de la aplicación, por último tiene la opción de generar el archivo de ejecución para que desde el celular se pueda instalar y luego realizar las diferentes pruebas de funcionabilidad de la aplicación.

En la Figura 14, se evidencia el diseño de uno de los módulos de la aplicación utilizando el programa con su entorno de trabajo, en donde al lado izquierdo se encuentran las diferentes herramientas y al lado derecho la configuración en cuanto estructura y forma de cada uno de los componentes de trabajo seleccionados

Figura 14. Entorno de trabajo app inventor



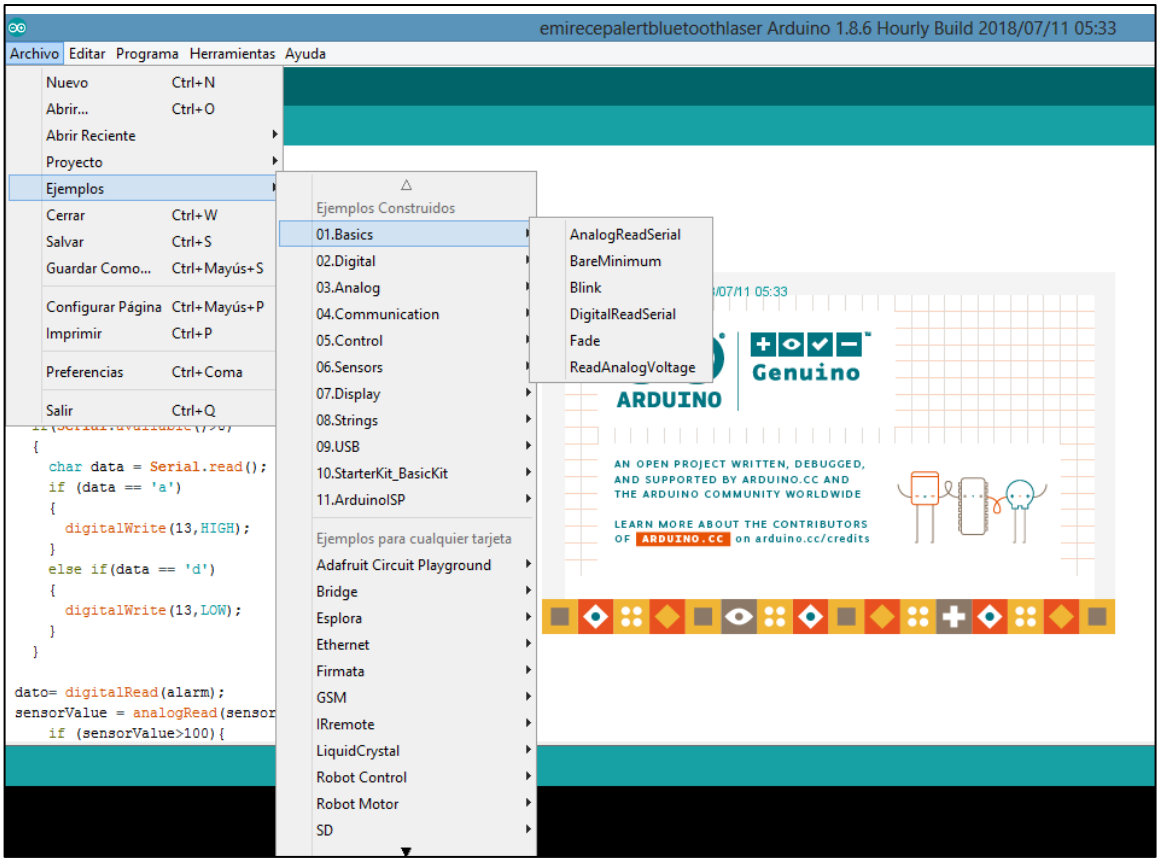
Fuente: el autor.

4.2.15 Arduino nightly: Software que permite configurar y programar la placa Arduino, según las necesidades y requerimientos frente al funcionamiento de los pines y componentes instalados, de este modo se realizan las diferentes pruebas de funcionamiento, identificando que la programación realizada y configuración se encuentran de manera correcta, así mismo cuenta con la herramienta de simulación para ver los resultados antes de compilar y ejecutar en la placa.

En la Figura 15, se visualiza el entorno de trabajo de este programa, donde se realizan las diferentes configuraciones de la placa, en cuanto a lo que se encuentra conectado en los pines, según la necesidad del proyecto. Es un IDE o entorno de desarrollo, donde se compilan y ejecutan las diferentes líneas de código programadas para los diferentes proyectos que se van a cargar en la placa de Arduino. El programa cuenta con códigos de ejemplo para la ejecución de pruebas, es necesario que el Arduino esté conectado, mediante un cable que generalmente

viene cuando se adquiere la placa en los mercados de electrónica, de este modo el programa reconocerá la placa instalada para la configuración del puerto de comunicación, para la compilación y cargue en la placa.

Figura 15. Entorno de trabajo de Arduino nightly

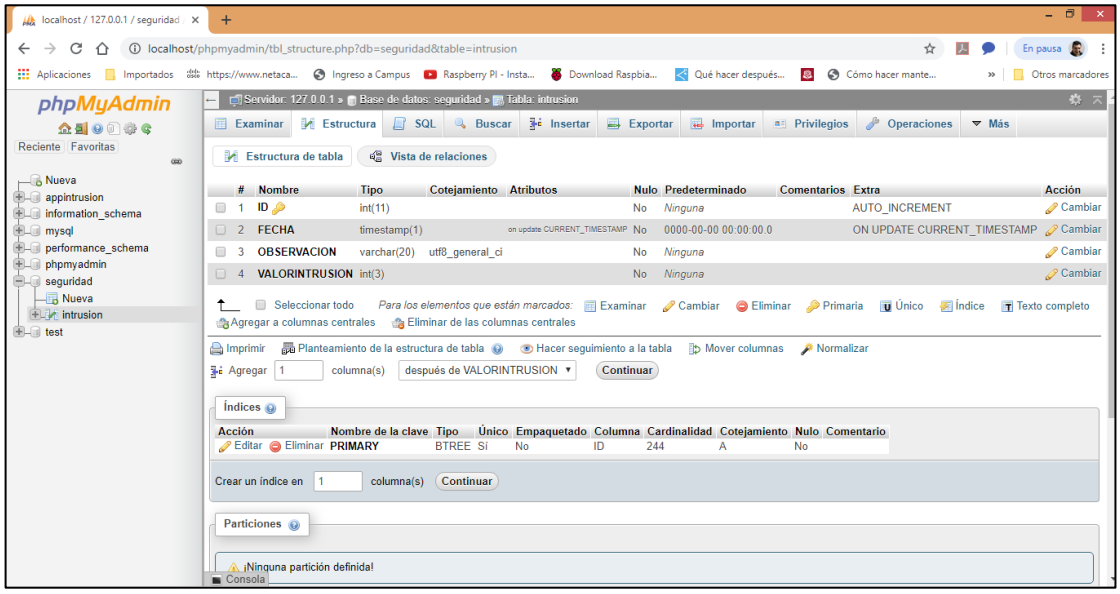


Fuente: el autor.

4.2.16 Phpmyadmin: Programa que permite la creación de la base de datos, con el fin de configurar las tablas donde se resguardan los registros de los diferentes eventos de intrusión o de estado normal del sistema, la conexión de la base de datos y registro se realiza mediante la dirección IP local del equipo y esta a su vez se conecta mediante un router sin restricción, con el fin de que se conecten sin ningún conflicto y de este modo se registren los eventos configurados en el procedimiento de accesos no autorizados.

En la Figura 16, se identifica el entorno del programa, en donde se evidencia las diferentes herramientas de creación de la base de datos, generación de registros, entre otros procedimientos que se pueden configurar en esta herramienta de registro de información. Es necesario que se habiliten los servicios en el panel de control de Xampp (Apache y MySQL), con el fin de que se genere la comunicación entre la base de datos y la aplicación, para la interacción y registro de datos entre la aplicación y la base de datos.

Figura 16. Entorno de trabajo de phpMyAdmin



Fuente: el autor.

4.2.17 Seguridad Informática: Medios, herramientas y técnicas que permiten la protección de la información, con el fin de resguardar uno de los activos más preciados de una organización. Se encuentran diferentes procedimientos y protocolos para asegurar el acceso a la información, es importante destacar que las empresas no solo deben preocuparse por la seguridad lógica, también es indispensable adoptar medidas de manera física, para esto se emplea una auditoria general la cual determina cuales son los vacíos en la seguridad de la red de la compañía mediante un análisis de vulnerabilidades, realizando ataques autorizados de acceso para determinar si se puede acceder a los equipos de red de la compañía.

4.2.18 Seguridad en la Información: Normas, metodologías, protocolos y auditorias que permiten evaluar las políticas de protección de la información en las organizaciones, aplicando el levantamiento de activos, identificación de servicios actuales y nuevos, identificación de vulnerabilidades, análisis de riesgos, dando a conocer la propuesta de controles sobre las vulnerabilidades encontradas.

Existen diversas metodologías para el análisis de riesgos en los sistemas de gestión de la seguridad de la información (Magerit, Octave, Mehari, NIST SP 800: 30, Coras, Cramm, Ebios) entre otras.

4.3 MARCO CONTEXTUAL

La Corporación de Educación Tecnológica Colsubsidio es una Institución de educación superior de formación en programas Técnicos laborales, Técnicos y Tecnólogos profesionales, además, tiene amplia gama de cursos a la medida según necesidades de la Compañía y las personas, ofrece formación en Idiomas, lo anterior gestionado por las facultades y las áreas encargadas de los servicios:

> **Misión**: Somos una institución de educación superior que forma personas competentes, autónomas, emprendedoras y éticas, a partir de acciones de docencia, investigación y proyección social. Para lograrlo, alineados con la filosofía de Colsubsidio, nos basamos en un enfoque de desarrollo humano integral, contribuyendo con la satisfacción de las necesidades de formación de la población, el crecimiento personal y profesional de nuestros colaboradores, el desarrollo competitivo de las organizaciones y el mejoramiento económico, ambiental, social y cultural del país.
>
> **Nuevos inicios**: En el año 2020 seremos reconocidos por la comunidad como una institución educativa que, desde sus acciones docente, investigativa y de relación con el sector externo apoya la protección social. Ofreceremos programas innovadores y pertinentes a las necesidades de las empresas y alineados con las estrategias de desarrollo socio económico del país. Seremos reconocidos como una opción educativa de calidad para poblaciones que tradicionalmente no cuentan con acceso a la educación superior. Nuestros egresados contarán con opciones efectivas de vinculación laboral a través de la red de empresas afiliadas a Colsubsidio.[6]

[6] CORPORACIÓN DE EDUCACIÓN TECNOLÓGICA COLSUBSIDIO, Nosotros CET Colsubsidio [sitio web]. Bogotá; [Consultado: 13 de abril de 2020]. Disponible en: https://cetcolsubsidio.edu.co/conoce-la-cet/nosotros-cet/

El Ambiente donde se enfocará la solución en respuesta a la necesidad de resguardar la información en pro del aseguramiento de la Infraestructura Tecnológica y Seguridad en Redes se encuentra ubicado en la Corporación de Educación Tecnológica (CET - Colsubsidio), Sede chapinero Calle 52 a no 9 – 76, en esta sede se cuenta con una estructura de 6 pisos y 12 niveles, cada nivel cuenta con 2 salones con nomenclatura según el nivel (Ejemplo: Nivel 2, Salón 201 y 202); en el Nivel 12 se encuentra el salón el 1201 y 1202, en el ambiente especializado ubicado en el Nivel 12 salón 1201, cuenta con una cámara de seguridad en el pasillo y en su interior se encuentran ubicados 20 equipos de cómputo, un rack de comunicación dotado con equipos de red, ups, entre otros elementos de comunicación y herramientas de trabajo para diseño y estructura de red.

Referente a los autores que han desarrollado proyectos similares, se encuentra a una comunidad denominada descubrearduino, quienes dan a conocer mediante un video tutorial la forma como se debe implementar un sistema laser, sin embargo, lo trabajan a nivel de hardware sin implementación de software ni sistema de alarmas de manera programática y sin bases de datos de registro de acceso.

También hay una Empresa llamada SCAITEC liderada por el Ingeniero Libardo Gómez, asesor de este Proyecto, quien se dedica a este tipo de soluciones a nivel empresarial y de hogar, trabajan con sistemas relacionados con la seguridad informática y de redes.

4.4 MARCO HISTORICO

Para este proyecto se tomará como marco histórico la evolución de la seguridad Informática en donde se destaca. Está enfocada a la seguridad de los procesos de la Empresa, priorizando los negocios de esta frente a la protección de la información. En los años 80 y 90, La seguridad se centraba en la protección de los equipos de los usuarios a nivel de sistemas operativos contra los virus informáticos. (Seguridad Lógica), ya con Internet la Seguridad se orienta a las redes, dando protección a servidores de aplicaciones, e implementando barreras como firewalls.

Anteriormente los Hackers se concentraban en realizar acciones sin ánimo de lucro, realizando procesos de afectación de los equipos mediante virus, sin embargo, en la actualidad consideran que la información es muy valiosa y los ataques se concentran en el acceso a la misma, extorsionando para recuperarla, o utilizarla a

favor de terceros y para implementar daños con el fin de dejar a las Empresas vulnerables sin más solución que acceder a las pretensiones de los atacantes.

Ante lo anterior, llegan las nuevas tecnologías de protección, contra intrusiones, monitoreos y ataques, algunas de estas son:

- ✓ Sistemas IDS (Intrusion Detection System). Monitorean y detectan accesos no permitidos.
- ✓ Sistemas IPS (Intrusion Prevention System). Previenen, detectan y bloquean ataques.
- ✓ Honeypot. Señuelos para atraer atacantes y analizar sus movimientos en la red.
- ✓ SIEM (Security Information and Event Management). Generador de alarmas y alertas, capaces de almacenar los registros.

Luego de esto, Grupo Control[7] describe el concepto de seguridad informática como aquel que evoluciona hacia la seguridad de la información donde se trabaja sobre normas y políticas de la organización para que hagan parte de los planes estratégicos de la Empresa, se debe trabajar en que las Compañías tienen que considerar la información, como un activo invaluable de su organización; en la actualidad se habla no de la evolución de la seguridad, si no en la integración, de la seguridad informática con sus medios y técnicas y la seguridad de la información con sus medidas organizativas.

4.5 MARCO LEGAL

Camelo[8] da a conocer en un compendio sobre el marco legal de la seguridad de la información en Colombia, la Ley 1273 del 05 de enero del 2009, donde indica que el enfoque de esta ley es la protección de la información y de los datos.

[7] GRUPO CONTROL. *Evolución de la Seguridad Informática*. Grupo control, 25 de febrero de 2019. [Consultado: 10 de mayo de 2019]. Disponible en https://www.grupocontrol.com/evolucion-de-la-seguridad-informatica.

[8] CAMELO, Leonardo. Marco legal de seguridad de la información en Colombia [blog]. En: S*eguridad de la información en Colombia*. 23 de febrero de 2010. [Consultado: 17 de mayo de 2019]. Disponible en http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html

Esta ley permite dar un panorama asertivo frente a lo que busca aplicarse en el proyecto, donde además de proteger la infraestructura tecnológica del salón 1201, también se van a manejar datos personales de personas que se van a registrar a la aplicación, los cuales deben mantenerse seguros y sin riesgo de ser usados de manera fraudulenta siendo víctimas de posibles delitos informáticos.

Como gestores de desarrollos se debe actuar bajo la ley y la reglamentación vigente, con el fin de proteger la información resguardada en las bases de datos, teniendo siempre presente la confianza que dan las personas al proporcionar la información para las pruebas pertinentes del prototipo.

4.6 MARCO TECNOLÓGICO

Los sistemas de seguridad de la información permiten ser un valor agregado para el resguardo de la información de las empresas, es importante destacar que no solo se debe invertir en la seguridad lógica para restringir el acceso por medio de las redes, también se debe tener una inversión considerable para la seguridad física, debido a que se ha comprobado que los mismos exempleados y empleados, están filtrando información de las compañías donde trabajan a la competencia, o con el fin de dañar a la Organización.

Pérez[9] hace referencia a que las TIC simplifican e incrementan la productividad, potencializando el avance de los sectores productivos. Este aporte es el comienzo hacia la visión del prototipo, con el fin de trabajar en un enfoque claro, estructurado en el aporte al mejoramiento continuo de los procesos de las organizaciones, de esta forma, se incentiva el uso de la tecnología generando confianza en los recursos automatizados, que apoyen constantemente la seguridad física y digital.

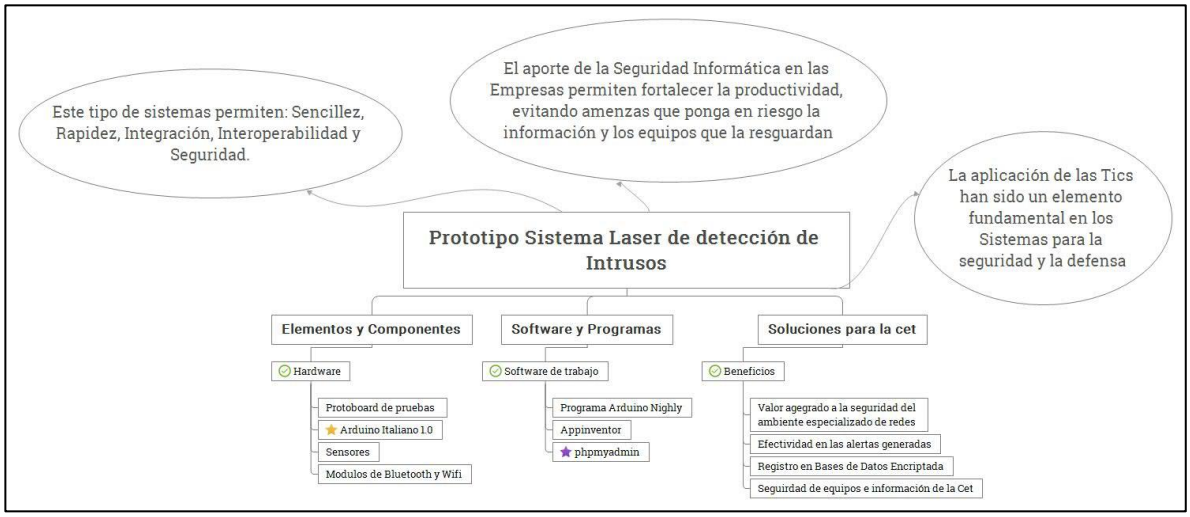
Las innovaciones tecnológicas pensadas para la industria abren la posibilidad de que se genere una interacción Universidad – Organizaciones, promoviendo la investigación en las instituciones para el aprovechamiento de los recursos en pro del desarrollo del País, la búsqueda de oportunidades y la inversión en la escuela, como factor esencial de la búsqueda interna de soluciones para las Compañías. Es una gran estrategia para impulsar la economía interna y la motivación de los

[9] PEREZ MARTINEZ, Felix. El papel de las TIC en los sistemas para la seguridad y la defensa. En: *Seguridad y Defensa.* Enero de 2006. [Consultado: 23 de mayo de 2019]. Disponible en https://www.coit.es/sites/default/files/archivobit/pdf/felixperez.pdf

estudiantes sería mucho mayor, porque desde la Universidad están desarrollando proyectos, conociendo previamente las necesidades de la Industria, obteniendo un acercamiento real de manera práctica.

A continuación, en la Figura 17, se describe mediante un diagrama los elementos tecnológicos que interactúan para el diseño del prototipo, lo que permite dar una visión hacia el objetivo planteado, teniendo en cuenta la descripción de componentes y los resultados esperados. Decubriendoarduino[10] muestra en su sitio web un prototipo similar, el cual es la base para el trabajado en este proyecto aplicado, se destaca que todas las personas que han desarrollado diferentes proyector con Arduino, al ser una plataforma de hardware libre, sienten ese compromiso de compartir sus avances, de este modo se logra compartir el conocimiento e interactuar con grandes profesionales del tema, por último los foros permiten dar a conocer las diferentes dudas sobre códigos y componentes, fallos en el proceso de generación de pruebas, son comunidades grandes, así como también se encuentran almacenes que ofrecen los productos electrónicos y se preocupan por ser muy específicos con las características .

Figura 17. Marco Tecnológico Desarrollo del Proyecto



Fuente: el autor.

[10] DESCUBREARDUINO Construye un sistema de seguridad con laser con Arduino [en línea]. Proyectos Arduino útiles, sencillos y avanzados. [Consultado: 20 de mayo de 2019]. Disponible en: https://descubrearduino.com/construye-sistema-seguridad-con-arduino/

5. METODOLOGÍA APLICADA AL PROYECTO

En el proyecto aplicado a la construcción de un prototipo funcional de control de acceso y alertas de intrusión, se trabajan con variables que son proporcionadas con el fin de generar los diferentes resultados, con base en lo anterior se relaciona la metodología a utilizar en cada una de las fases del desarrollo del proyecto lo que permite evidenciar las técnicas y herramientas de trabajo.

5.1 ESTRUCTURA METODOLÓGICA

La Investigación aplicada permite dar un enfoque frente a la realidad, relacionado con aquellas problemáticas que se evidencian en los procesos organizacionales y en donde se busca desarrollar el proyecto aplicando los parámetros de Alomía, Escallón y Ortegón[11] donde describen los diferentes procedimientos experimentales para lograr el objetivo de proponer una solución específica, teniendo en cuenta como principal eje el Método Experimental, el investigador controla las variables para realizar la delimitación de los resultados, basado en la metodología científica. Este método permite recolectar datos para ejecución de las mediciones logrando un control del resultado en la experimentación, el cual fue aplicado en las pruebas con el fin de obtener resultados sobre las variables dependientes proporcionadas, según el entorno y el ambiente de trabajo.

Las variables que se pueden ejecutar son de tipo dependientes (las que se miden y son el objeto de estudio del investigador) para el proyecto aplicado las variables dependientes son los resultados de la interrupción del haz de luz, los cuales pueden variar según la hora del día, del momento de la interrupción y la distancia entre el sensor laser emisor y el sensor receptor de fotocelda, las variables de tipo independientes (donde el investigador manipula para ver la relación con las variables dependientes), en este caso se tienen las que son modificadas para manipular la sensibilidad en la detección del haz de luz, no se puede descartar las variables extrañas que se puedan generar durante el procedimiento establecido dentro de la investigación, las cuales son ingresadas por medio de las bases de

[11] ALOMÍA ARCE, Hernan; ESCALLÓN S., Víctor y ORTEGÓN G., Katherine. guía metodológica para realización de proyectos de grado. En: *Departamento de ingeniería industrial.* 2006. [Consultado: 06 de junio de 2019]. Disponible en ftp://ftp.icesi.edu.co/leonardo/PGI/Guia%20Estudiantes.pdf

datos, que son de tipo entero, carácter y de texto.

Los pilares fundamentales que sustentan el método experimental son: La reproducibilidad y la falsabilidad, también se trabajará bajo el método cualicuantitativo, la cual nos permite analizar los datos para luego representarla por medio de tablas, de acuerdo con los registros y resultados que se den durante las pruebas del prototipo, estas tablas mostraran los registros de las bases de datos, como también los datos de las diferentes pruebas del prototipo en el momento de la detección del intruso.

Tomando como base lo descrito por la OBS Businees School[12] es importante que durante el desarrollo del Proyecto se trabaje con el siguiente enfoque teniendo en cuenta las fases descritas en la Tabla 1, se toma como referencia varios documentos, sin embargo, se enfoca en las fases de acuerdo con las necesidades del prototipo estructurados como se evidencia en la siguiente tabla.

Tabla 1. Fases del Proyecto

Fase	Descripción
Analizar	De acuerdo con las necesidades en seguridad física de la institución se empieza a estructurar el enfoque del proyecto
Planear	Generación y verificación de componentes específicos del prototipo
Diseñar	Se hace un diseño donde se plasma el funcionamiento para su creación en la ejecución
Pruebas	Luego de creado se realizan pruebas que permiten garantizar la funcionabilidad del prototipo
Evaluar	Se evalúa la efectividad y la recopilación de información mediante registros en la base de datos
Ejecución y Verificación para nuevas pruebas	En esta parte los posibles errores encontrados en la evaluación se corrigen para garantizar un proceso de registro y de alarmas eficiente.

Fuente: el autor.

[12] OBS BUSINEES. ¿Cuáles son las etapas de un proyecto? Te lo contamos en esta infografía. [en línea]. Noticias. [Consultado: 11 de junio de 2019]. Disponible en: https://obsbusiness.school/int/noticias/innovacion/cuales-son-las-etapas-de-un-proyecto-te-lo-contamos-en-esta-infografia

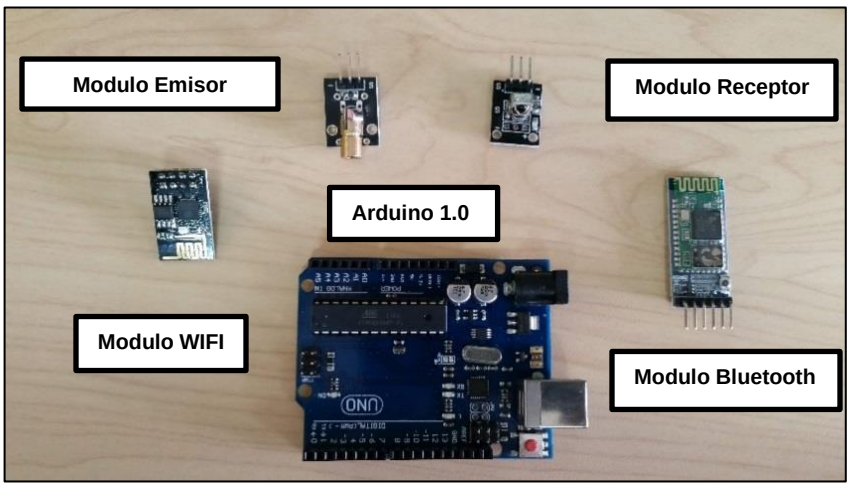
6. IDENTIFICACIÓN DE LOS COMPONENTES NECESARIOS PARA EL DISEÑO Y CONSTRUCCIÓN DEL PROTOTIPO

En la búsqueda de determinar cuáles serían los componentes adecuados para la construcción del prototipo de intrusión por medio de láser, se encuentra que la placa Arduino permite mediante sensores generar este tipo de resultados en donde se generan datos con respecto a un método de barrera de haz de luz, lo que incentivo a localizar cada componente con el fin de analizar su funcionamiento, conocer sus características, para luego realizar las diferentes pruebas, es así como en este apartado se evidencia la trazabilidad desde la búsqueda hasta las pruebas de funcionamiento de cada componente.

6.1 ANALISIS.

Se establecen los componentes necesarios para el desarrollo del proyecto como se evidencia en la Figura 18, donde se realiza un análisis de los requerimientos para el diseño del prototipo con el fin de proceder con la cotización y adquisición de estos con los proveedores de componentes electrónicos y sensores para Arduino. (Descubre Arduino, 2014)

Figura 18. Componentes de trabajo del Proyecto



Fuente: el autor.

Luego de validar los componentes y necesidades del proyecto se procede a realizar las diferentes cotizaciones y adquisición de los componentes, obteniendo como resultado los precios estimados relacionados en la Tabla 2.

Tabla 2. Tabla de Recursos de Hardware y Software

Hardware	**Software**
Arduino 1.0	Programa Arduino Nighly
Sensor Laser Emisor	Appinventor
Sensor Receptor (se cambia por modulo fotocelda)	phpmyadmin
Módulo de Bluetooth HC0	
Modulo Wifi ESP 8266	
Protoboard y Consumibles generales	

Fuente: el autor.

6.2 PLANEAR

Se consulta el *datachip* (características generales) de los componentes para conocer los diferentes voltajes y modo de conexión con el Arduino, de esta forma se realiza un trabajo de reconocimiento sobre la arquitectura de cada componente para establecer a que pines se deben conectar y de este modo proceder con la configuración de estos mediante el programa de configuración y código programable de Arduino *Night Light*.

6.2.1 Arquitectura Ficha Técnica Arduino 1.0 En la Tabla 3, se relacionan las características del microcontrolador utilizado para la construcción del dispositivo el cual proporciona la oportunidad de trabajar como hardware libre y a su vez viene con un entorno de desarrollo.

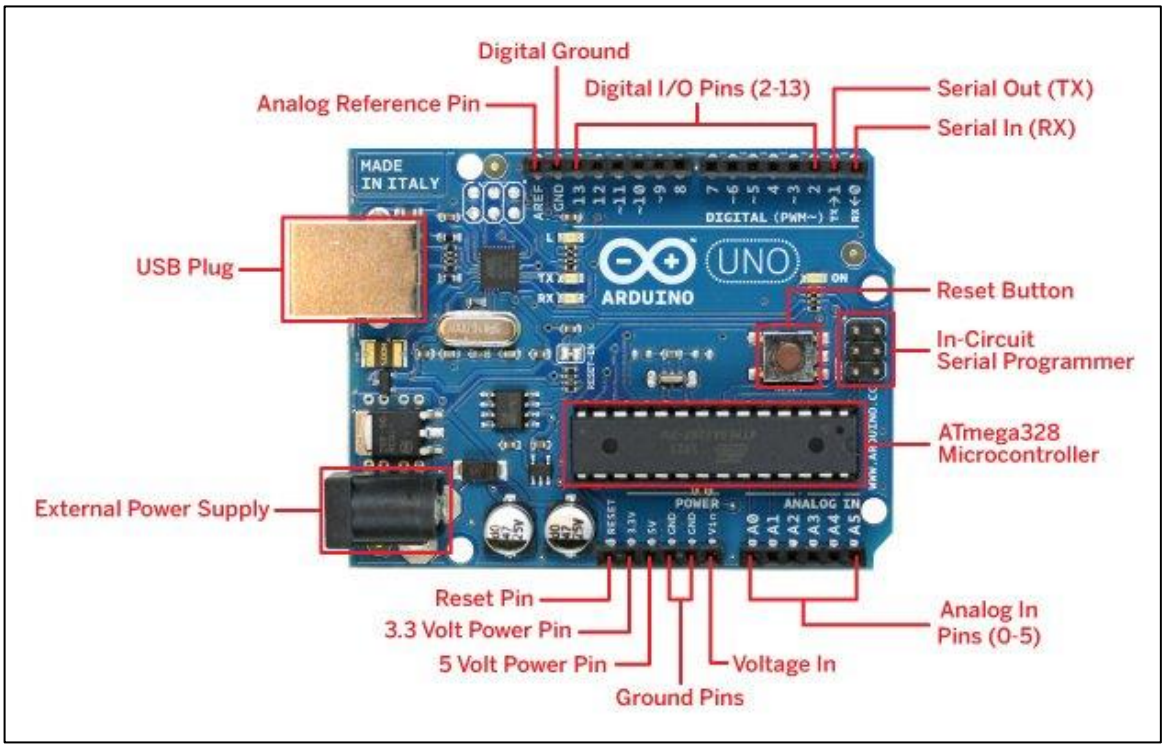
Tabla 3. Arquitectura Ficha Técnica Arduino 1.0

Componentes	Descripción
Microcontrolador	ATmega328P
Tensión de funcionamiento	5V
Voltaje de entrada (recomendado)	7-12V
Voltaje de entrada (límite)	6-20V
Pines de E / S digitales	14 (de los cuales 6 proporcionan salida PWM)
Pines de E / S digitales de PWM	6
Clavijas de entrada analógica	6
Corriente DC por Pin E / S	20 mA
Corriente DC para 3.3V Pin	50 Ma
Memoria flash	32 KB (ATmega328P) de los cuales 0,5 KB utilizados por el gestor de arranque
SRAM	2 KB (ATmega328P)
EEPROM	1 KB (ATmega328P)
Velocidad de reloj	16 MHz
LED_BUILTIN	13
Longitud	68.6 mm
Anchura	53.4 mm
Peso	25 g

Fuente: DESCUBREARDUINO. Arduino Uno REV 3 [en línea]. 2018. [Consultado: 16 de junio de 2019]. Disponible en: https://descubrearduino.com/arduino-uno/

6.2.2 Diagrama Especificaciones Generales Arduino 1.0 En la Figura 19 se muestran las diferentes especificaciones del Arduino Uno, con el fin de que se conozcan los requerimientos o especificaciones técnicas de los componentes que se pueden conectar y los voltajes que se manejan en los diferentes pines y conectores, teniendo clara la compatibilidad con la placa, de este modo se logra evitar cortos que se pueden generar la no tener este conocimiento previo.

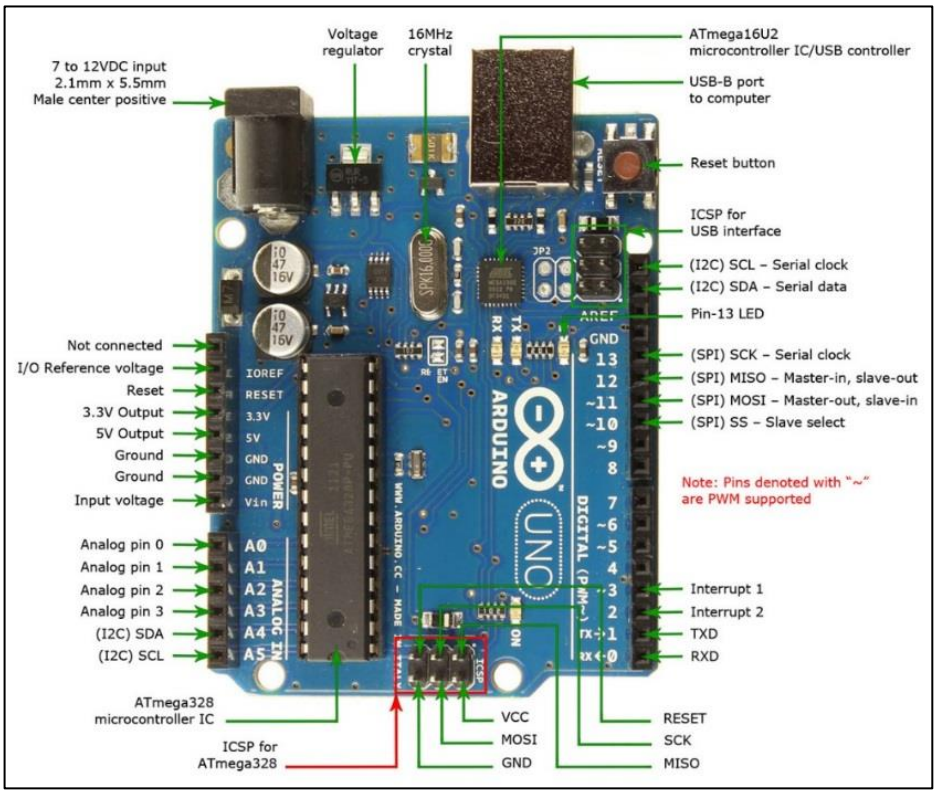
Figura 19. Especificaciones Generales Arduino 1.0



Fuente: Arduino 1.0 [imagen]. En: ROBOMART. 2009 - 2015. [Consultado: 22 de junio de 2019]. Disponible en: https://www.robomart.com/image/catalog/RM0058/02.jpg

6.2.3 Diagrama Eléctrico Específico Arduino 1.0 El diagrama eléctrico en la Figura 20, permite conocer las características de la placa y las especificaciones de cada uno de los pines con el fin de que sean coincidentes con la conexión de los componentes electrónicos a utilizar. Entre las especificaciones más destacadas, encontramos las salidas de voltaje de los pines de conexión, los pines análogos de conexión con los compontes, el puerto de comunicación con el equipo de cómputo donde se encuentra instalado el programa de configuración de la placa, y la conexión de corriente para que este no dependa de la corriente que pueda suministrar el computador, sino que se conecte directamente a una toma, para quedar energizado.

Figura 20. Diagrama Eléctrico Arduino 1.0



Fuente: Diagrama eléctrico Arduino 1.0 [imagen]. En: ROBOMART. 2009 - 2015. [Consultado: 22 de junio de 2019]. Disponible en: https://www.robomart.com/image/catalog/RM0058/01.jpg

6.2.4 Arquitectura Ficha Técnica Módulo Receptor PC COMPONENTES muestra las características del módulo:

- Rango de voltaje de funcionamiento 2.7V -5.5V
- Chip 1838 Receptor de infrarrojos
- Tamaño 6.4mm * 7.4mm * 5.1mm
- 90 ° ángulo de aceptación
- Frecuencia 37.9KHZ
- Distancia Máxima 18 metros[13]

[13] PC COMPONENTES. Módulo Receptor de Infrarrojos compatible con Arduino. [en línea]. Arduino. [Consultado: 30 de junio de 2019]. Disponible en: https://www.pccomponentes.com/m-dulo-receptor-de-infrarrojos-compatible-con-arduino

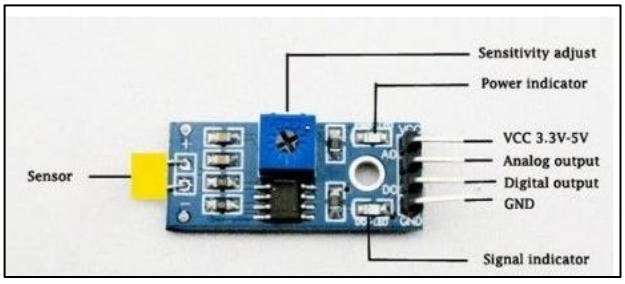
Nota: Este componente se descarta del prototipo ya que en las pruebas iniciales se encuentra que es un sensor receptor de infrarrojo utilizado principalmente para programación con controles remotos, mas no láser, generando dificultad en la recepción del láser para búsqueda de señal y aumento y disminución de voltaje, por lo tanto, es reemplazado primero por una fotocelda y posteriormente por un sensor receptor de fotocelda.

6.2.5 Arquitectura Ficha Técnica Fotocelda ELECTRONICAPLUGANDPLAY muestra las características del módulo fotocelda:

- Rango de variación: 10 KΩ - 1 MΩ.
- Tiempo de respuesta: De 20 a 30 milisegundos.
- Longitud de onda Respuesta Máxima: 540 nm.
- Voltaje Máximo: 150 V.
- Potencia Máxima: 100 mW.
- Fabricante: Senba Optical.[14]

6.2.6 Diagrama de conexión Modulo Sensor con Fotocelda con Arduino 1.0 En la Figura 21, vemos la arquitectura del sensor receptor de fotocelda donde encontramos las características y herramientas con los diferentes servicios de conexión que ofrece, adicional incluye el tipo de conexión en los 4 pines disponibles.

Figura 21. Diagrama de conexión Modulo Sensor con Fotocelda



Fuente: Modulo sensor con fotocelda [imagen]. En: MOVILTRONICS. [Consultado: 07 de julio de 2019]. Disponible en: https://moviltronics.com/tienda/modulo-sensor-con-fotocelda/

[14] ELECTRONICAPLUGANDPLAY. Fotocelda Sensor de Luz LDR-GL5528. [en línea]. Sensores y transductores. [Consultado: 03 de julio de 2019]. Disponible en: http://www.electronicaplugandplay.com/sensores-y-transductores/product/319-fotocelda-sensor-de-luz-ldr-gl5528

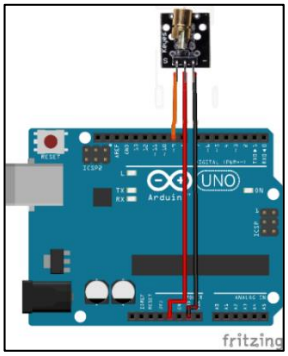
Nota: Se cambia la fotocelda por un módulo sensor con fotocelda.

6.2.7 Arquitectura Ficha Técnica Módulo Emisor MOVILTRONICS muestra las características del módulo emisor:

- Voltaje de funcionamiento: 5V
- Corriente: 30 - 40 mA
- Color: Rojo
- Longitud de onda: 650 nm
- Peso: 6,0 g
- Dimensiones: 2.8 cm x 1.5 cm x 0.8 cm[15]

6.2.8 Diagrama de conexión Modulo Emisor con Arduino 1.0 En la Figura 22, se encuentra el plano de conexión del módulo emisor laser, donde se evidencia como se debe conectar en la placa Arduino, de este modo verificamos la funcionalidad de este.

Figura 22. Diagrama de conexión Modulo Emisor



Fuente: Diagrama conexión modulo emisor. [imagen]. En: proyectos y tutoriales. [Consultado 16 de julio de 2019]. Disponible en: http://cursoarduino.proserquisa.com/wp-content/uploads/2016/10/Conexion.png

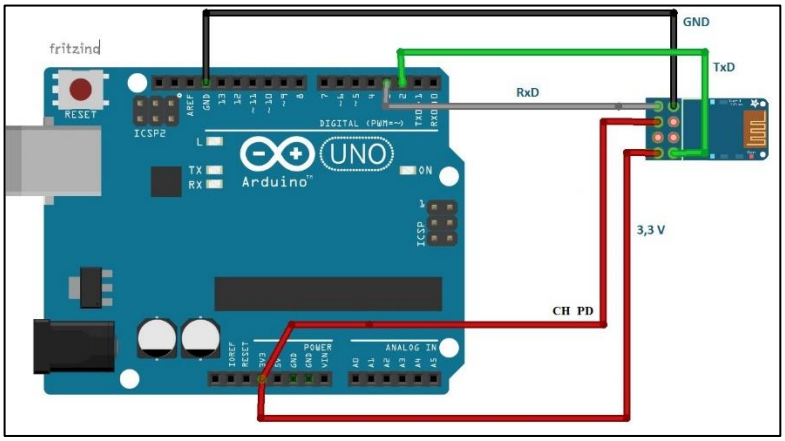
[15] MOVILTRONICS. Módulo Diodo Laser. [en línea]. Sensores. [Consultado: 12 de julio de 2019]. Disponible en: https://moviltronics.com.co/varios/224-modulo-diodo-laser-.html

6.2.9 Arquitectura Ficha Técnica Módulo Wifi Serial ESP8266: DUALTRONICA muestra las características del módulo wifi serial:

- Protocolos soportados: 802.11 b/g/n
- Alimentación: 3.3 - 3.6V más de este rango lo puede quemar, pero las entradas tx y rx soportan 5v
- Wi-Fi Direct (P2p), Soft Access Point
- Stack TCP/IP integrado
- PLL, reguladores y unidades de manejo de energía integrados
- Potencia de salida: +19.5dBm en modo 802.11b
- Sensor de temperatura integrado
- Consumo en modo de baja energía: <10 uA
- Procesador integrado de 32 bits, puede ser utilizado como procesador de aplicaciones[16]

6.2.10 Diagrama de conexión Modulo Wifi con Arduino 1.0 En la Figura 23, se encuentra el plano de conexión del módulo Wifi, donde se evidencia como se debe conectar en la placa Arduino, de este modo verificamos la funcionalidad en el momento de realizar pruebas con la aplicación de gestión del prototipo.

Figura 23. Diagrama de conexión Modulo Wifi



Fuente: Diagrama conexión modulo wifi. [imagen]. En: prometec. [Consultado 01 de agosto de 2019]. Disponible en: https://www.prometec.net/wp-content/uploads/2014/12/Buena1.jpg

[16] DUALTRONICA. Modulo Wifi ESP8266. [en línea]. Módulos. [Consultado: 23 de julio de 2019]. Disponible en: https://dualtronica.com/modulos/58-modulo-wifi-esp8266.html

Nota: En el prototipo inicial se desarrollaron pruebas de comunicación con el módulo de bluetooth, donde se evidencia que con este módulo funciona correctamente, sin embargo, a futuro la idea es programar el módulo Wifi, con el fin de mejorar el alcance del rango de comunicación.

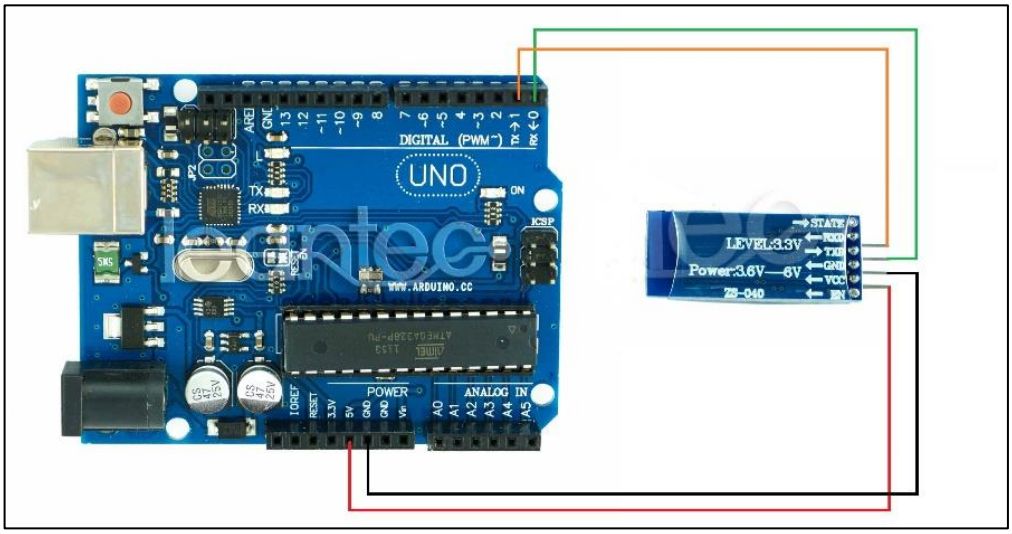
6.2.11 Arquitectura Ficha Técnica Módulo Bluetooth HC05: ELECTRÓNICO CALDAS muestra las características del módulo bluetooth:

- Especificación bluetooth v2.0 + EDR (Enhanced Data Rate)
- Puede configurarse como maestro, esclavo, y esclavo con autoconexión (Loopback) mediante comandos AT
- Chip de radio: CSR BC417143
- Frecuencia: 2.4 GHz, banda ISM
- Modulación: GFSK (Gaussian Frequency Shift Keying)
- Antena de PCB incorporada
- Potencia de emisión: ≤ 4 dBm, Clase 2
- Alcance 5 m a 10 m
- Sensibilidad: ≤ -84 dBm a 0.1% BER
- Velocidad: Asincrónica: 2.1 Mbps (max.) /160 kbps, sincrónica: 1 Mbps/1 Mbps
- Seguridad: Autenticación y encriptación (Password por defecto: 1234)
- Perfiles: Puerto serial Bluetooth
- Módulo montado en tarjeta con regulador de voltaje y 6 pines suministrando acceso a VCC, GND, TXD, RXD, KEY y status LED (STATE)
- Consumo de corriente: 50 mA
- El pin RX del módulo requiere resistencia de pull-up a 3.3 V (4.7 k a 10 k). Si el microcontrolador no tiene resistencia de pull-up interna en el pin Tx se debe poner externamente.
- Niveles lógicos: 3.3 V. Conectarlos a señales con voltajes mayores, como por ej. 5 V, puede dañar el módulo
- Voltaje de alimentación: 3.6 V a 6 V
- Dimensiones totales: 1.7 cm x 4 cm aprox.
- Temperatura de operación: -20 ºC a +75 ºC[17]

[17] ELECTRÓNICO CALDAS. HC – 05. [en línea]. Módulos. [Consultado: 06 de agosto de 2019]. Disponible en: https://www.electronicoscaldas.com/modulos-rf/452-modulo-bluetooth-hc-05.html

6.2.12 Diagrama de conexión Modulo Bluetooth con Arduino 1.0 En la Figura 24, se encuentra el plano de conexión del módulo Bluetooth, donde se evidencia como se debe conectar en la placa Arduino, de este modo verificamos la funcionalidad del este al realizar pruebas con la aplicación de gestión del prototipo.

Figura 24. Diagrama de conexión Modulo Bluetooth



Fuente: Diagrama conexión modulo bluetooth. [imagen]. En: leantec. [Consultado 15 de agosto de 2019]. Disponible en: https://leantec.es/img/cms/conexion%20bluetooth.jpg

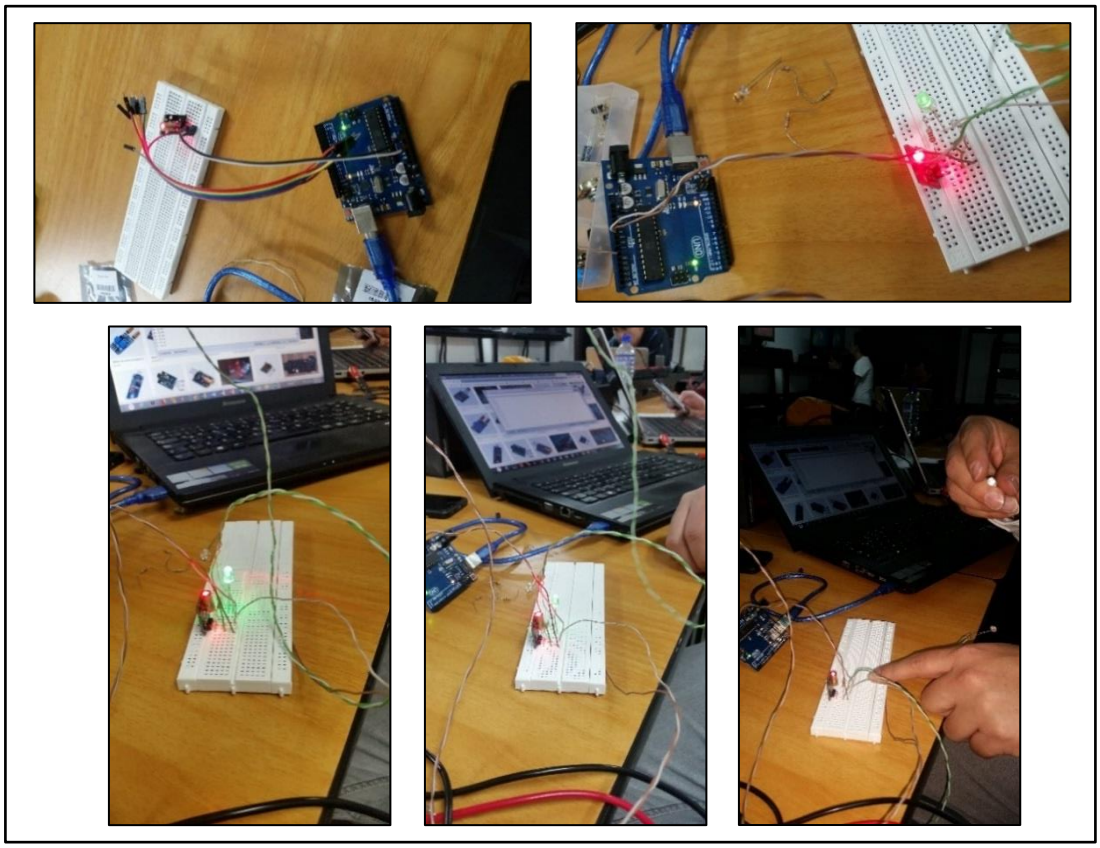
6.3 DISEÑAR

Se realizan las diferentes pruebas de funcionamiento de cada componente con el fin de verificar el estado de cada uno y si al cumplir con las normas de conexión, estas generen los resultados esperados, las pruebas son desarrolladas primero en la *protoboard*, con el fin de asegurar la funcionabilidad, para luego si pasar al proceso de creación del prototipo, soldando el circuito en la baquela estableciendo la ubicación correcta de cada componente, con el fin de que el módulo receptor de fotocelda, quedara en el sentido del módulo emisor láser, luego fueron adaptadas a la caja con los diferentes espacios de conexión entre componentes y con facilidad para poder realizar algún cambio en el interior, teniendo la precaución de que ningún

componente pudiera sufrir algún tipo de daño, en el momento de realizar la apertura de la caja.

6.3.1 Pruebas de Funcionamiento Modulo Emisor Laser En la Figura 25, encontramos las pruebas de funcionamiento del módulo emisor laser, donde se evidencia que el haz de luz se genera de manera correcta, obteniendo que el componente puede usarse sin inconveniente en el circuito.

Figura 25. Pruebas modulos sensor Emisor Láser.



Fuente: el autor.

7. DESARROLLO DE UNA BASE DE DATOS PARA LOS REGISTROS DE LAS ALERTAS ESTABLECIDAS.

El objetivo de este punto es crear la aplicación y la base de datos, para lograr establecer comunicación entre ellas, iniciando sesión, guardando registros, registrarse, entre otros servicios.

7.1 ANÁLISIS

Se Procede a identificar los módulos que va a contener la APP, junto con las imágenes de identificación y las diferentes opciones. (por medio de la Herramienta *appinventor*). Los módulos que tienen que ver con bases de datos son el módulo de registro y el módulo de ingreso (inicio de sesión), los datos ingresados quedan resguardados en la misma base de datos de la aplicación de manera temporal, con el fin de manejar la integridad de los datos, ya que no se recomienda que esta aplicación sea administrada por más de un usuario con privilegios, debido a que se está trabajando con información insensible de posibles delitos informáticos.

7.2 PLANEAR

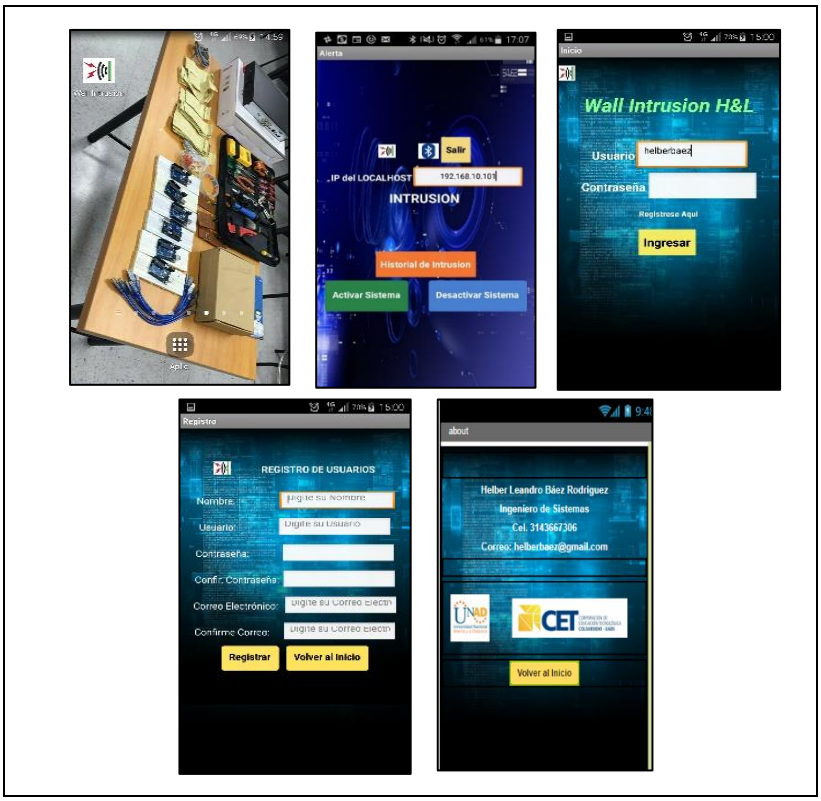
Posteriormente se procede a la estructuración de la aplicación y la base de datos de enlace para los procesos de registros de las intrusiones, usuarios, validación y autenticaciones. (por medio de la herramienta *appinvetor* y el gestor de base de datos *phpmyadmin*), se toma la determinación de que en la base de datos de *phpmyadmin* la cual almacena la información de manera local, se establezca que el módulo de intrusiones quede registrando los datos en esta base de datos, esto con el fin de que, en el caso de producirse una falla en el teléfono, los datos de intrusión no sufran ningún riesgo de pérdida de información.

7.3 DISEÑAR

Teniendo el dispositivo físico se crea la aplicación de gestión, por medio de la aplicación app inventor que permite crear por medio de las herramientas las diferentes opciones y se configura usando programación en bloques, de este modo se manejan las diferentes opciones como el de activación y encendido del sistema por medio de bluetooth, evidencia de alertas en caso de intrusión física, e inicio de sesión con usuario registrado.

7.3.1 Creación Aplicación Se crea la aplicación con los diferentes módulos de registro, inicio de sesión, módulo de intrusión, el acceso desde el celular a la aplicación con el respectivo logo que identifica a la aplicación y el módulo informativo de instituciones y logos. En la Figura 26, se evidencia el contenido de cada módulo en la aplicación con sus respectivos campos.

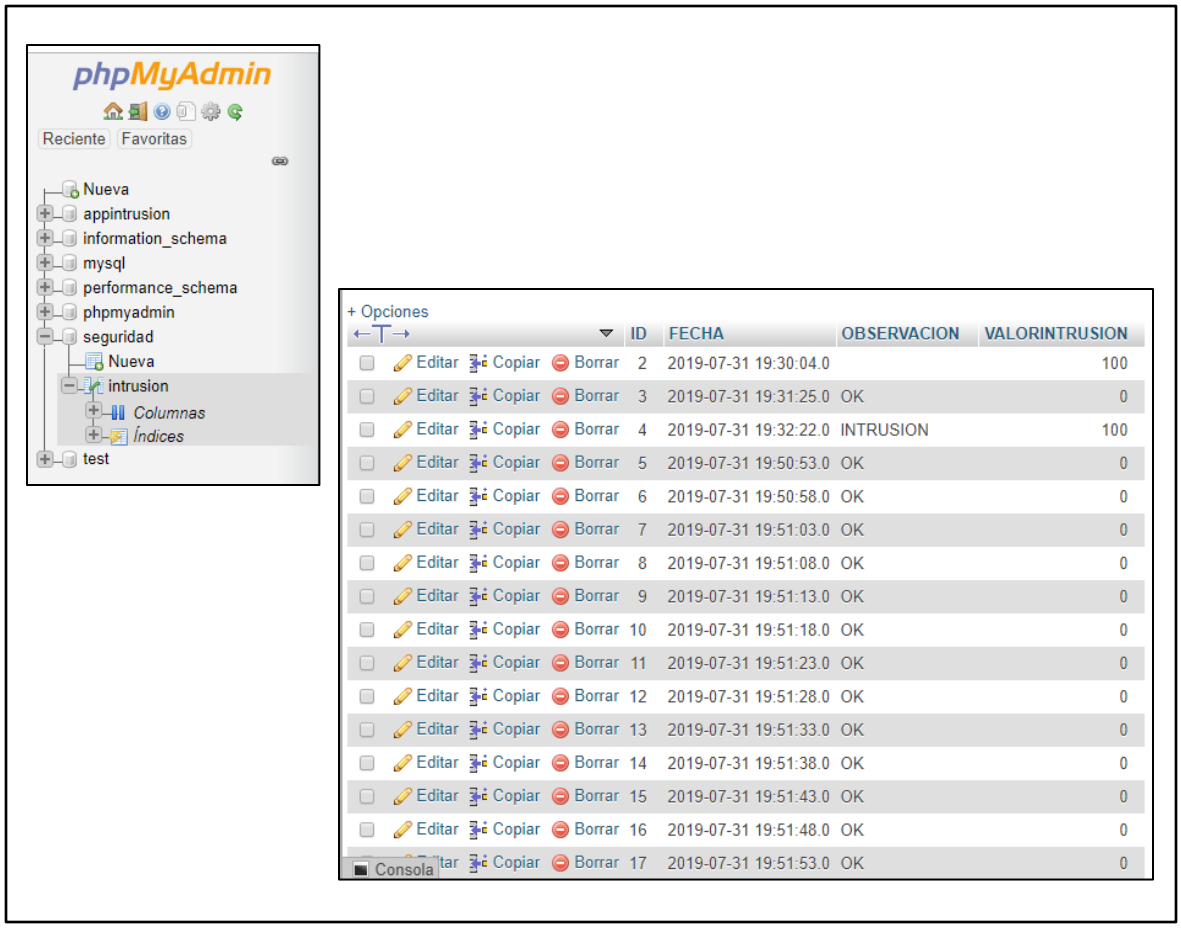
Figura 26. Aplicación de gestión del dispositivo



Fuente: el autor.

7.3.2 Creación Base de Datos y Tablas En la herramienta phpmyadmin (gestor de bases de datos a través de la web con el programa Xamp), en la Figura 27, se crea la base de datos denominada “seguridad” y una tabla de registro de intrusiones denominada “Intrusión”, donde se encuentran los diferentes campos denominados (ID, Fecha, Observación, Valor Intrusión), de esta forma se estructura la base de datos para relacionar los diferentes registros de accesos no autorizados al salón 1201.

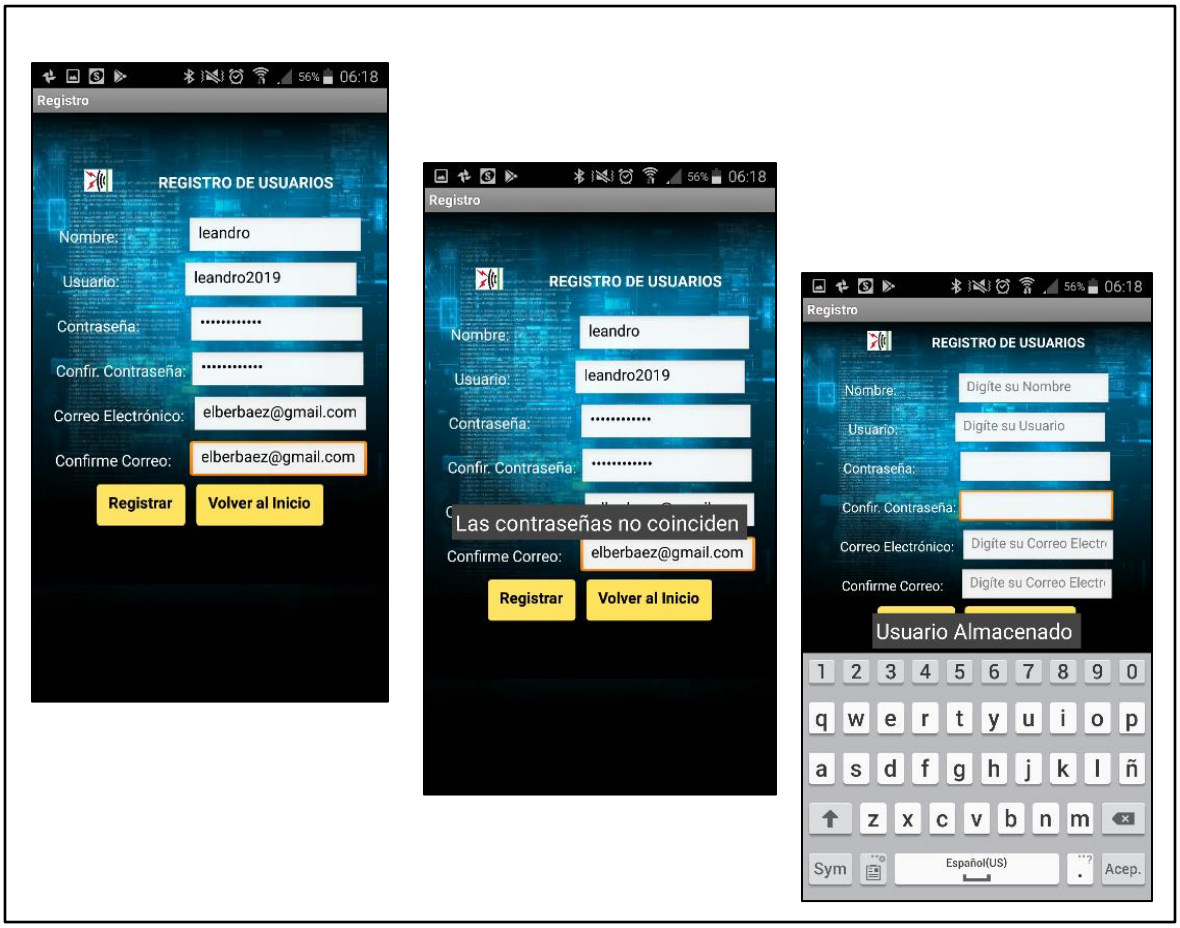
Figura 27. Creación de Base de Datos y Tablas



Fuente: el autor.

Con el fin de proporcionar funcionalidad a la aplicación, se establecen los diferentes parámetros para guardar los registros de usuarios de manera interna, de este modo se logra interactuar de manera eficaz sin caídas recurrentes o fallos, en la Figura 28, se evidencia la generación de un nuevo registro de usuario y el almacenamiento interno de la información, con los diferentes campos necesarios para un registro básico de personas en la aplicación manejando alertas en el caso de que la contraseñas suministradas no coincidan en los dos ingresos solicitados y por último una alerta de que el usuario fue almacenado de manera correcta.

Figura 28. Procedimiento de Registro de Usuarios.



Fuente: el autor.

Luego el registro es verificado en la aplicación, se procede a iniciar sesión, donde la aplicación identifica si el usuario creado se encuentra habilitado o no, para iniciar sesión según los datos registrados en el paso anterior, en la Figura 29, se encuentra la evidencia del procedimiento de verificación de acceso, si se valida correctamente el usuario, ingresa al módulo de intrusión.

Figura 29. Comprobación e Inicio de Sesión.

Fuente: el autor.

En la Figura 30, se observa la forma en que se registran las intrusiones, en donde el primer procedimiento es el acceso al modulo, se digíta la dirección ip del equipo a donde se encuentra alojada la base de datos de registro de accesos no autorizados, se activa el sistema, para iniciar con el proceso de pruebas, y de este modo se empiezan a registrar las intrusiones en la tabla correspondiente.

Figura 30. Estructura y Registro de Tabla Intrusiones

Fuente: el autor.

8. CONSTRUCCIÓN DEL PROTOTIPO CON LOS COMPONENTES ESTABLECIDOS PARA LA EJECUCIÓN DE PRUEBAS.

8.1 MONTAJE Y VERIFICACIÓN

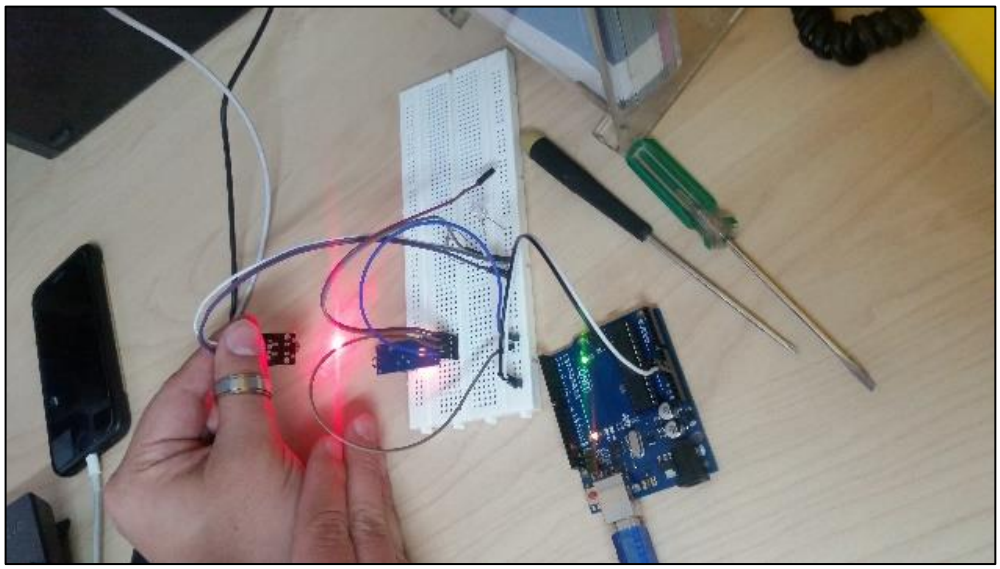
Se verifica el sitio donde va a quedar instalado el dispositivo. En la Figura 31, se evidencia el lugar donde va a quedar instalado el prototipo funcional, como se ve en la imagen, los equipos son de un alto costo y lo que se encuentra en las cajas son herramientas de telecomunicaciones como antenas, teléfonos ip, firewall, entre otros. Estos equipos se usan para prácticas de los estudiantes sobre montaje y configuración de redes, los Docentes realizarán los diferentes procedimientos para mantener en óptimas condiciones el salón, puede ocurrir que se intenten sabotear la configuración realizada y que la sala pierda conectividad, generando que la información quede expuesta.

Figura 31. Sitio de Pruebas.

Fuente: el autor.

8.1.1 Prueba de componentes en *protoboard* En la Figura 32, se refleja la estructura inicial en *protoboard* con el fin de verificar que cada componente cumpla su función, de este modo se realizan pruebas preliminares sobre la comunicación del módulo emisor láser junto con el módulo receptor de fotocelda, con el fin de verificar la interacción entre los sensores, con el haz de luz emitido por el láser.

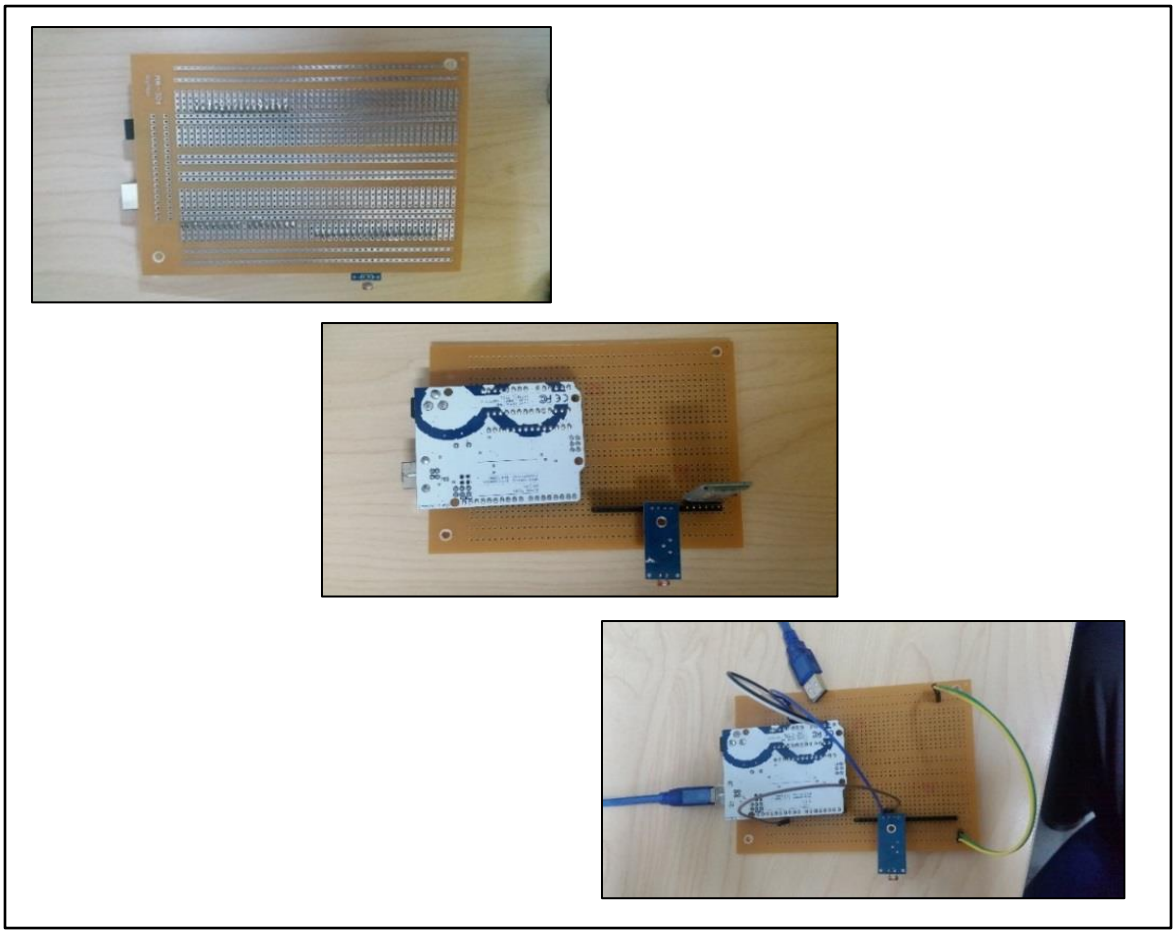
Figura 32. Prueba de Intrusión con *Protoboard*



Fuente: el autor.

Luego de probar el circuito en la *protoboard*, se realiza el ensamble en la baquela como se puede evidenciar en la Figura 33, donde los los componentes son soldados de manera adecuada, para evitar malas conexiones y cortos; estos puntos de soldadura tienen que quedar de forma adecuad con el fin de que el circuito funcione correctamente, no pueden quedar unidos, para no generar problemas de cortos o un mal funcionamiento en la interacción de los diferentes componentes, en este proceso de soldado se dapataron unos conectores los cuales facilitan que no necesariamente los componentes tengan que estar soldados directamente en la baquela, si no que se puedan manipular y ser retirados en cualquier momento para verificaciones posteriores o nuevas configuraciones, lo cual ha sucedido con el modulo Bluetooth, donde cada vez que se requiere realizar una actualización de la programación del arduino, se debe retirar el modulo Bluetooth, para luego cargar la actualización y posteriormente conectarla para el buen funcionamiento del prototipo.

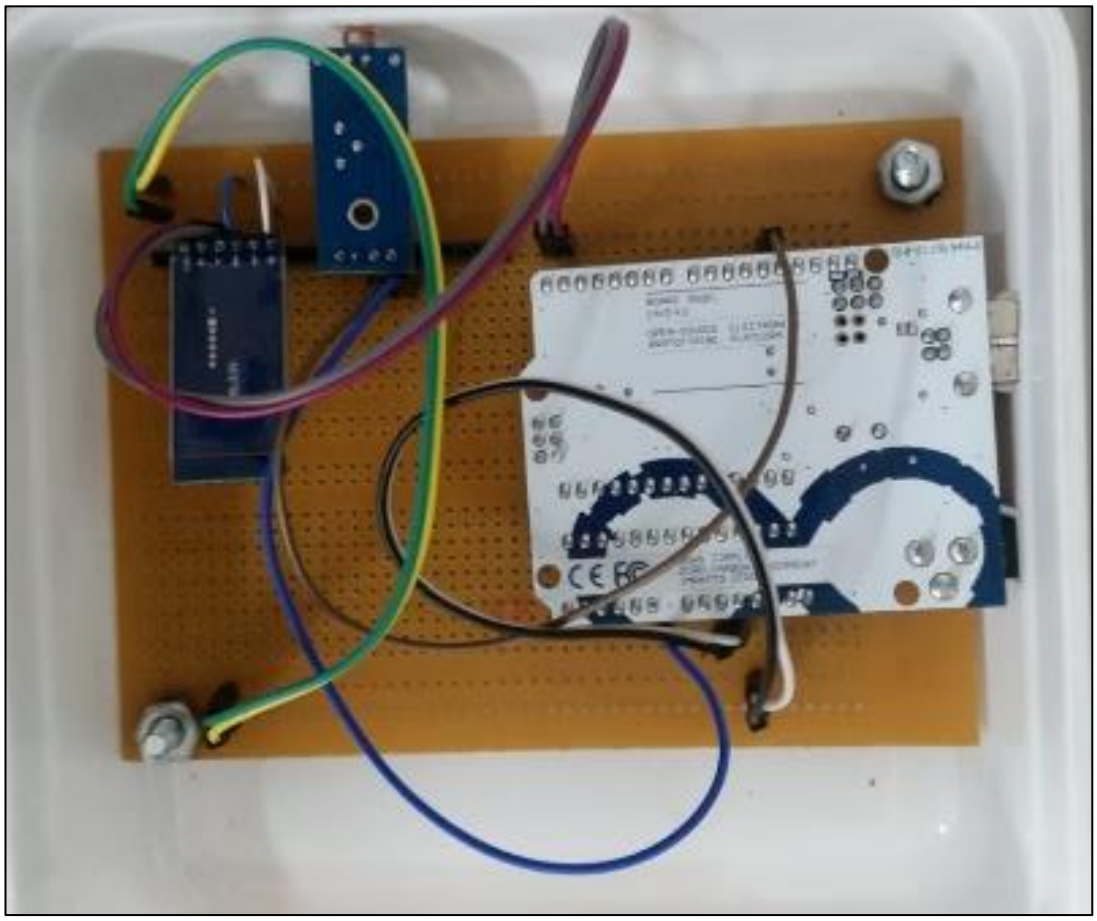
Figura 33. Adecuación de los Componentes y del Circuito a la Baquela.



Fuente: el autor.

Se deja la baquela en la caja utilizada para proteger el circuito de manera ordenada posicionando los componentes de tal forma que el sensor receptor de fotocelda pueda estar en línea con el receptor láser y con el fin de que se vea estético como se muestra en la Figura 34, en la baquela se encuentra asegurada a la caja por medio de unos tornillos, los cables y los componentes cuentan con espacio, en el caso de que se cierre la tapa de la caja, no afecte ningún componente o se tengan problemas de desconexión.

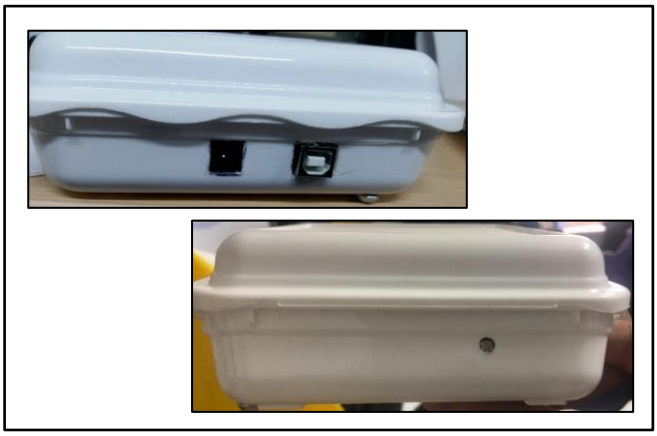
Figura 34. Conexión de Modulo Bluetooth e Instalación Baquela en la Caja.



Fuente: el autor.

Se realizan las respectivas adaptaciones como se evidencia en la Figura 35, con el fin de que se pueda manipular para las diferentes conexiones externas, recepción del haz de luz, cerrando la tapa para que los componentes no queden expuestos y de este modo estén asegurados. Los cortes de adecuación de entradas son cuidadosamente abiertos, con el espacio justo para las diferentes conexiones (cable de datos, cable de adaptador de corriente, y por último el área del módulo de receptor fotocelda), el cual recibe el haz de luz por parte del módulo emisor láser, es el punto más importante porque si no es liberado, va a tener una interrupción y no realizara ninguna interacción con el láser.

Figura 35. Adaptación para Conexión de Componentes.



Fuente: el autor.

En la Figura 36, se evidencia la instalación del prototipo funcional en el salón 1201, en la parte derecha se ubica la caja con los diferentes componentes adaptados a las necesidades del proyecto, y al lado izquierdo se ubica el emisor laser, se puede ver como el haz de luz está apuntando al receptor de fotocelda ubicado en la caja del lado derecho.

Figura 36. Prototipo Instalado en el Salón 1201

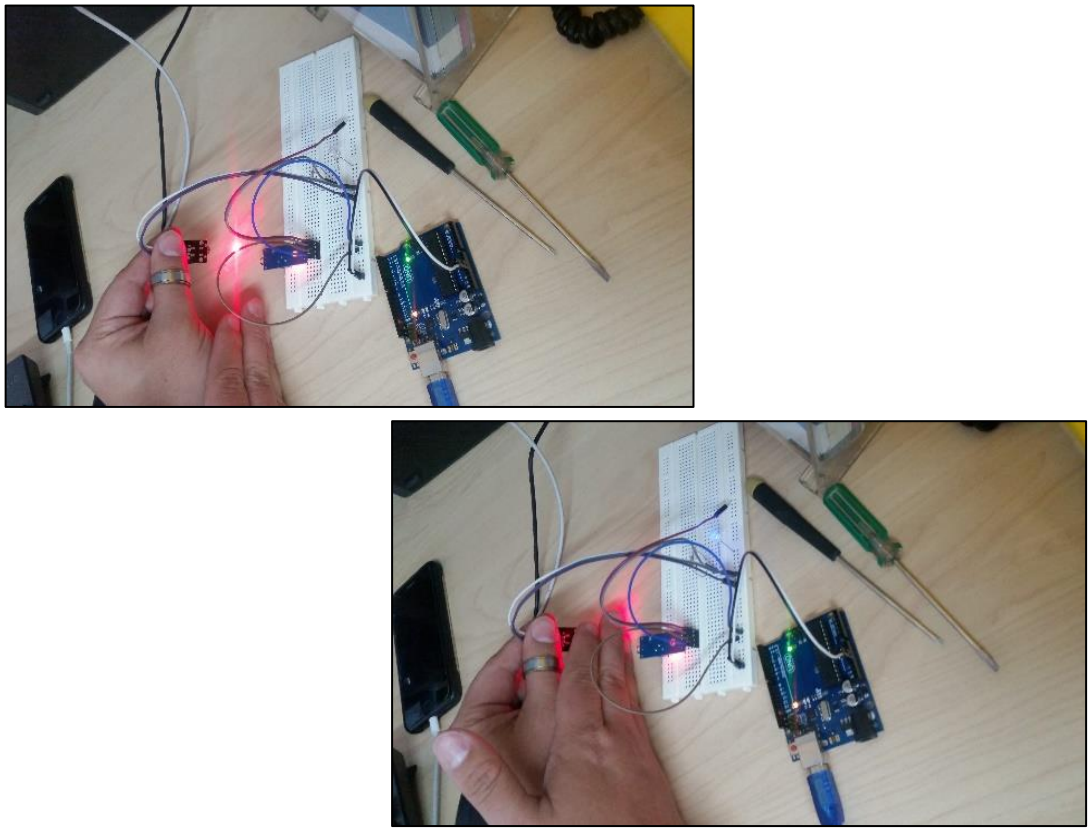
Fuente: el autor.

9. DOCUMENTACIÓN DE PRUEBAS REQUERIDAS PARA QUE EL DISPOSITIVO REALICE LAS ACCIONES DE SEGURIDAD.

9.1 EVALUACIÓN DE RESULTADOS SOBRE LAS PRUEBAS REALIZADAS

Las pruebas que se muestran a continuación se desarrollaron sobre los resultados obtenidos de la interacción del sensor emisor laser con el receptor de fotocelda, en la Figura 37, se evidencia la interacción entre los sensores de manera física con la configuración realizada en la placa para el encendido del haz de luz y la transmisión al receptor de fotocelda.

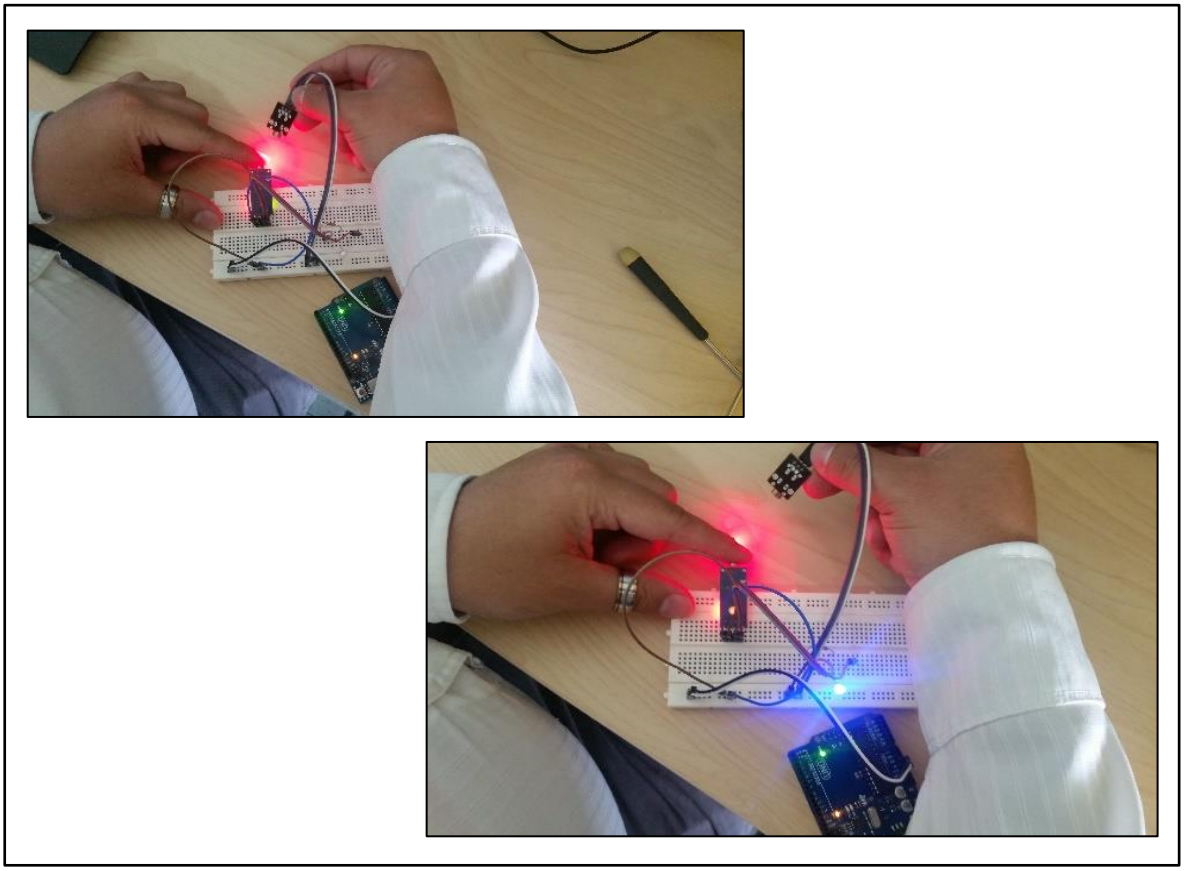
Figura 37. Prueba de Intrusión con *Protoboard*



Fuente: el autor.

Se obtiene como resultado en la Figura 38, que al interrumpir el paso del laser entre el modulo emisor y el receptor, se enciende y se apaga el led, evidenciando el optimo funcionamiento de los dos sensores.

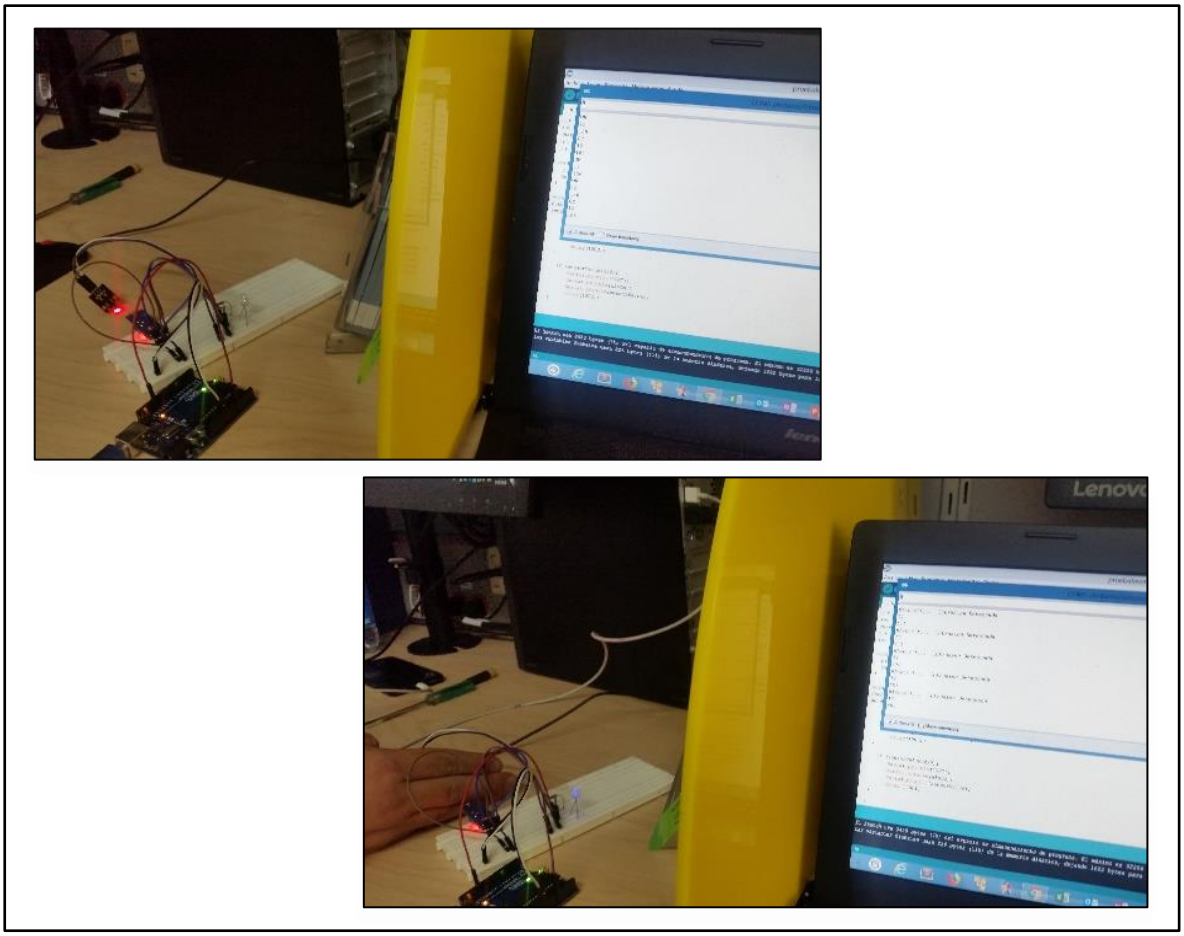
Figura 38. Nuevas Pruebas de Intrusión con *Protoboard*



Fuente: el autor.

Como resultado en la Figura 39, se logra identificar las diferentes intrusiones comprobando el funcionamiento del circuito, se realiza la programación del arduino en el programa con los mensajes de alerta obteniendo que al bloquear el laser muestra el mensaje “alerta, intrusión detectada” y al dar el paso muestra u mensaje de “ok” lo que indica que no hay intrusión detectada.

Figura 39. Programando el Arduino.



Fuente: el autor.

En la aplicación móvil Figura 40, se configura para manipular el dispositivo desde el celular por medio del Bluetooth obteniendo la activación y la desactivación del módulo laser, por medio de los botones activar sistema que al ser presionado se enciende el módulo emisor láser emitiendo el haz de luz hacia el módulo de receptor de fotocelda y desactivar sistema que al ser presionado se apaga el módulo emisor láser dejando de emitir el haz de luz, cuando interactúa la aplicación con el prototipo permite evidenciar los resultados sobre los mensajes de alerta de igual modo que en aparte anterior.

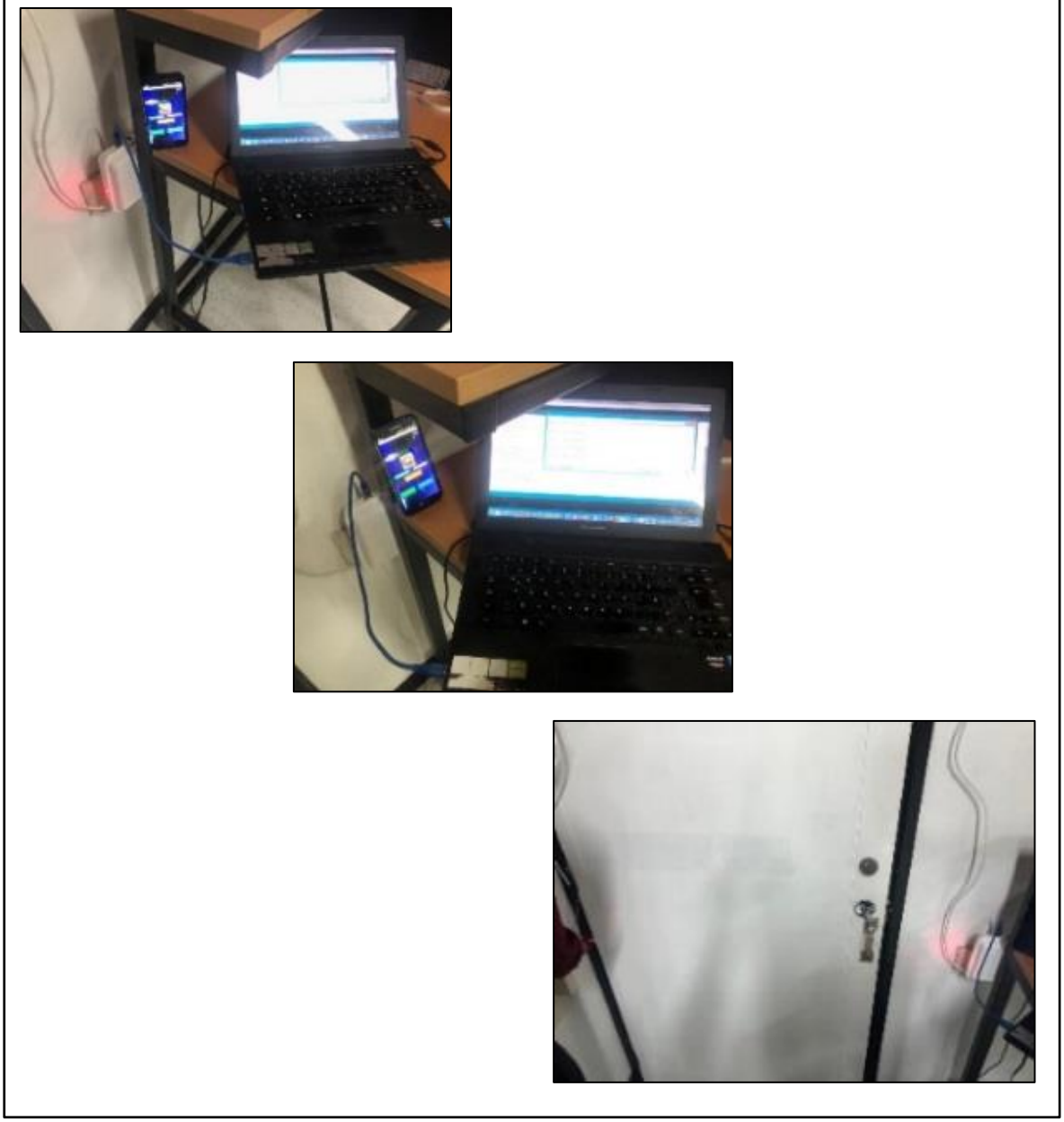
Figura 40. Pruebas de Interacción con la Aplicación.

Fuente: el autor.

9.2 EJECUCIÓN Y VERIFICACIÓN PARA NUEVAS PRUEBAS

Se realizan pruebas necesarias para verificar el funcionamiento en el sitio (salón 1201) donde queda instalado el prototipo, este proceso se realiza junto con la aplicación donde se evidencia como se van generando las alertas, también es importante y es el objetivo de este paso, como se muestra en la Figura 41, la interacción entre el emisor láser y el receptor de fotocelda, hace que se impriman en pantalla los valores generados por el sensor receptor de fotocelda, con respecto a la cantidad de luz recibida por haz de luz del emisor teniendo en cuenta la distancia entre los dos componentes.

Figura 41. Pruebas de Resultados Prototipo Instalado.



Fuente: el autor.

Los valores obtenidos muestran en la Tabla No 4, en donde se evidencia los datos específicos para ajustar la programación de los módulos con respecto a la intensidad de luz y sensibilidad del sensor para la detección de la intrusión. Es importante destacar que cualquier evento que se presenta puede generar variación en el resultado, como la intensidad de luz, la puerta cerrada, y la hora, como conclusión sobre el análisis de los datos, se establece que entre menor sea la luz del día, aumenta la intensidad del haz de luz del emisor láser, de ahí la razón por la cual los valores aumentan.

Tabla 4. Valores Adquiridos Sobre las Pruebas en Sitio.

Pruebas ejecutadas entre las 17:00 y 18:00 horas (Salón 1201) 14 de agosto de 2019	Luz Encendida	Luz Apagada	Puerta Cerrada (Sin Luz)
	426	483	744 – 762
	Datos análogos de código binario detectado por el módulo sensor de fotocelda sobre la cantidad de luz recibida.		
Pruebas ejecutadas entre las 18:00 y 19:00 horas (Salón 1201) 04 de septiembre de 2019	Luz Encendida	Luz Apagada	Puerta Cerrada (Sin Luz)
	527	615	790 – 815
	Datos análogos de código binario detectado por el módulo sensor de fotocelda sobre la cantidad de luz recibida.		

Fuente: el autor.

Se realizan las pruebas finales de registro de intrusiones con la interacción del dispositivo, la aplicación y la base de datos como se evidencia en la Figura 42, donde primero se configura un router sin restricciones, con el fin de que la red no genere barreras en el transporte de datos, ya que el firewall que controla la seguridad de la red de la institución, no permite la interacción entre los equipos, generando dificultades en la comunicación de los mismos, como el hecho de que no guarden los datos de los eventos en la base de datos.

Figura 42. Instalación *router* sin restricciones

Fuente: el autor.

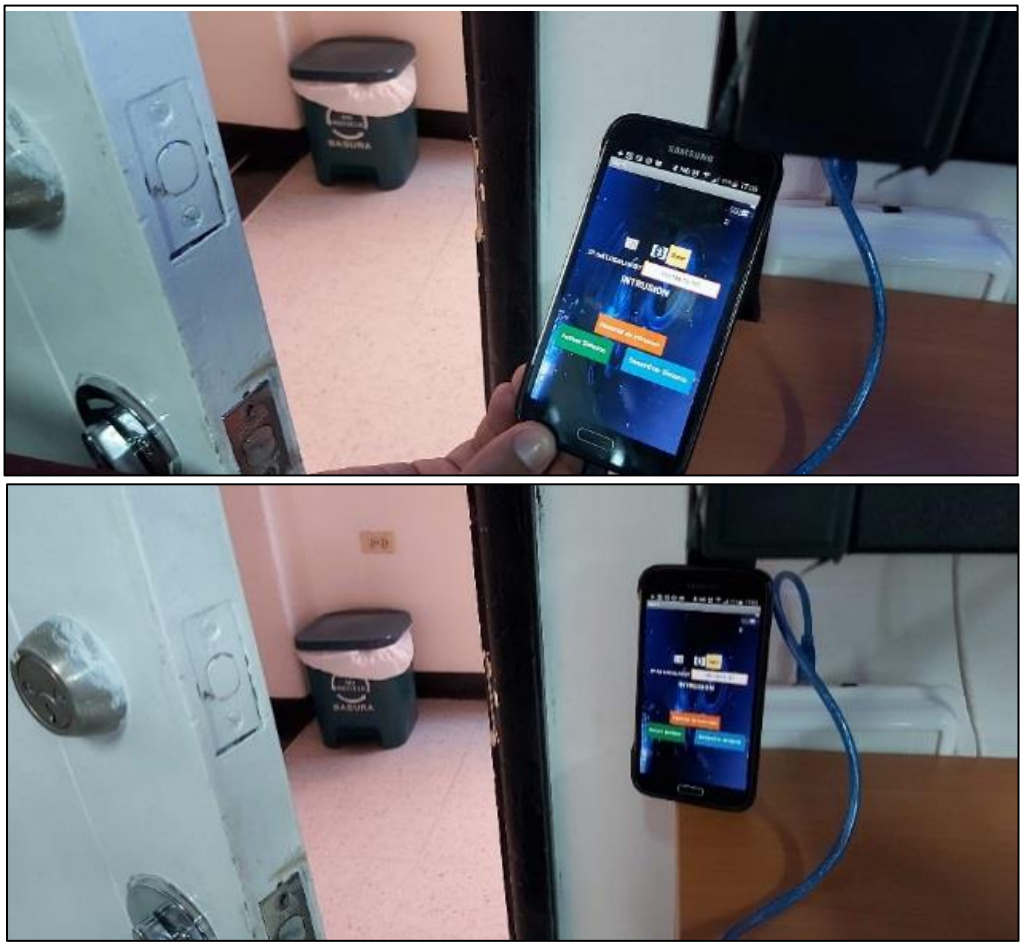
Con el prototipo instalado, se procede a realizar las pruebas de apertura y cierre de la puerta, en el figura 43, se evidencian los resultados de cada procedimiento, donde en el cierre de la puerta se obtiene un “ok” como resultado de la alerta, significa que cuando no hay intrusión, en la aplicación se genera una alerta de que todo el estado del sistema esta “ok” que no hay intrusiones detectadas, y que el dispositivo esta activado, operativo y funcionando.

Figura 43. Pruebas de verificación de alerta sin intrusión

Fuente: el autor.

Luego se observa en la Figura 44, como al momento de realizar la apertura de la apuerta donse se interrumpe el haz de luz del laser, se obtiene un mensaje de alerta en la aplicación denominado como “intrusión”, esta es la parte vital del funcionamiento del prototipo, la cual indica que se esta generando la alerta en la apertura de la puerta, realizado todo el ciclo planteado en el objetivo, generando los diferentes registros en la base de datos, aportanto a la seguridad de la información de la Corporación, en el salón destinado para tal fin.

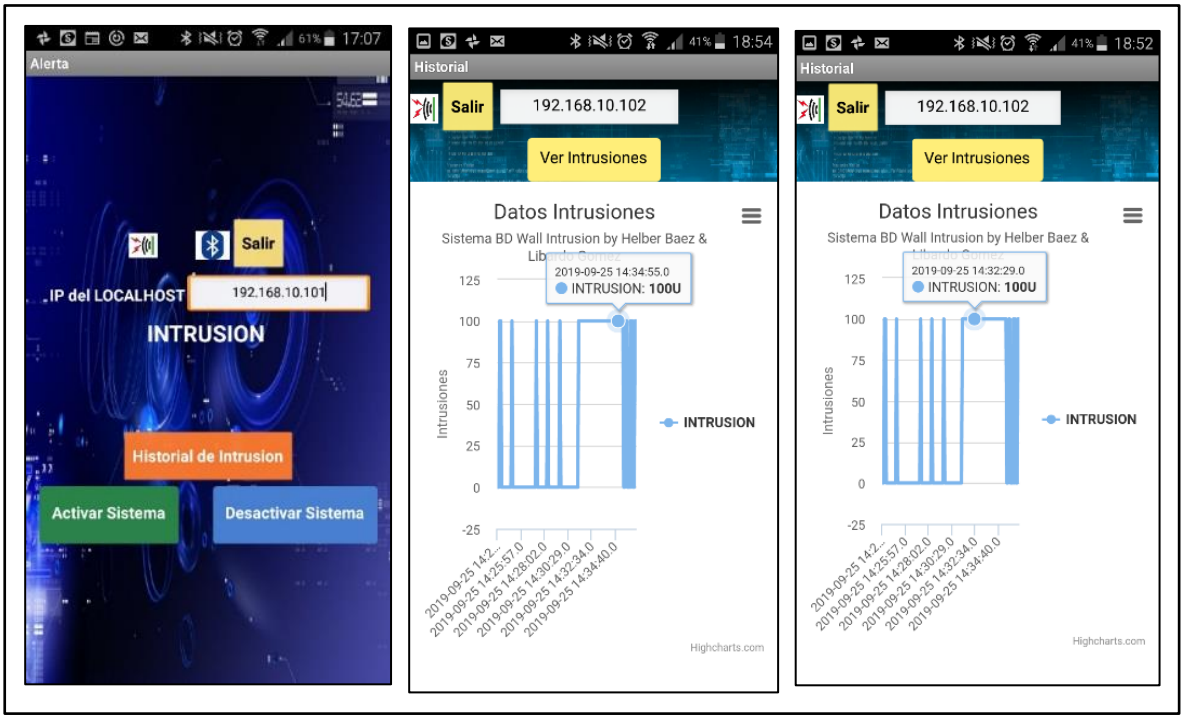
Figura 44. Pruebas de verificación de alerta con intrusión



Fuente: el autor.

Por último en la Figura 45, al ingresar al modulo de historial de intrusión, se encuentra la gráfica donde muestra el historial de intrusiones con la información respectiva, sobre la estadistica de estados de accesos y fechas. Es importante aclarar que la gráfica muestra los dos estados y de esta forma se evidencia que en los espacios en blanco no se visualza ninguna intrusión, mientras que en los picos mas altos, son las intrusiones registradas por el prototipo de los accesos que no fueron autorizados y los cuales se dieron en el momento en que fue activado el dispositivo.

Figura 45. Modulo de historial de intrusiones



Fuente: el autor.

Se recomienda que los usuarios y la Corporación que tengan acceso a la información generada por el prototipo lo asuman con transparencia, responsabilidad, compromiso y planteen la normatividad necesaria con el fin de darle el manejo adecuado a los registros que son los resultados que va arrojando el prototipo sobre los ingresos al salón 1201, estableciendo las políticas adecuadas, enfocada al ámbito de seguridad de la información.

Sobre los resultados de las pruebas:

1. Es importante que antes de adquirir los componentes, se evalué el funcionamiento y si estos resultados permiten cumplir con los requerimientos, de este modo se hace una inversión necesaria para la construcción del prototipo, generando confianza en el desarrollo del proyecto.

2. A nivel físico se recomienda generar conciencia sobre el cuidado del prototipo mientras que esté en funcionamiento en el salón 1201.

3. La estabilidad en el desarrollo de las pruebas, evidencia resultados exitosos sobre la alerta de intrusión, mostrando el óptimo funcionamiento de los diferentes sensores que interactúan en el circuito del prototipo.

A Nivel de Usuario:

1. Realizar copias de Seguridad cada 6 meses, generalmente las compañías organizan y administran muy bien este proceso, en algunas empresas se está implementado un servicio en donde los usuarios guardan la información directamente en el servidor por medio de trabajo en la nube con tecnología citrix, los sistemas operativos se cargan directamente desde el servidor y el usuario trabaja con un Receptor. En caso de no ser así, es importante guardar la información correctamente en el sitio establecido por la empresa ya que también existen programas que realizan backups directamente desde la carpeta del usuario al servidor, sin embargo, como Usuario se debe asumir la responsabilidad sobre la información que genera y tratar de tener una copia propia en el caso de que se presente un evento inesperado con el Servidor, para esto es importante la organización de los archivos

2. Las contraseñas de sus cuentas o de acceso a las aplicaciones en lo posible deben ser alfanuméricas.

A nivel de Empresa:

1. Mantener las políticas de que siempre que se realice un formateo e instalación de sistema operativo, dejar una participación exclusiva para los datos y redireccionar la ruta de los documentos a esa carpeta. (esto en el caso de que la Empresa no tenga Servidor.

2. En el caso de que en la Organización se manejen servidores, es importante verificar los roles autorizaciones y el acceso, como también realizar auditorías

periódicas donde se identifique el estado de la información y si se están trabajando con el protocolo y sin abusar de los privilegios.

La seguridad en las bases de datos representa un tema sensible en las compañías, TICBEAT hace referencia a que “el 96% de los datos sustraídos en el 2012 provenían de las bases de datos.”[18], este y otros datos donde se pierden millones de registros hacen que se dé una alarma en las organizaciones para que inviertan en la Seguridad de sus centros de Datos.

Es importante que se preste la atención a esta problemática y la materia da las pautas necesarias para que, como primera medida, se conozcan los tipos de bases de datos sus principales vulnerabilidades y métodos de control, los cuales permiten contribuir en la seguridad de cada proceso en las Empresas.

El interés por muchos hackers y cibercriminales, se enfocan en el robo de información, de ingresar a grandes bases de datos, irrumpir en las transacciones, entre otras actividades criminales que ponen en riesgo la información de las Empresas y Usuario, algo muy delicado que se debe contrarrestar, es así como las compañías deben invertir en la seguridad de sus datos, tomar medidas de control, auditar cada cambio, no descuidar la administración, y no confiarse sobre las personas que acceden a las Bases de Datos.

La información que se gestiona en las Bases de Datos son un factor de trabajo esencial para las compañías, por este motivo es importante darles un buen manejo y sobre todo protegerlas, porque hay que velar por la integridad de los datos, que no exista redundancia, que las credenciales estén siempre activas, pedir siempre autorización, dividirlas en módulos, para tener un control sobre que usuarios ingresan en cada módulo y si cuentan con la autorización para realizar las tareas que realizan en cuanto a gestión y alimentación de las Bases de Datos.

Lo Expuesto anteriormente es un llamado para que los datos de las intrusiones detectadas por el prototipo o accesos no autorizados, los cuales quedan resguardados en la base de datos en *phpMyAdmin,* sean tenidos en cuenta dentro de las políticas de seguridad de la Compañía, evitando que esta información quede vulnerable.

[18] Verizon (Data Breach). Las 10 grandes amenazas de seguridad en las bases de datos. “Citado por:” TICBEAT. 17 de abril de 2013 [en línea]. Tecnología. [Consultado: 28 de septiembre de 2019]. Disponible en: http://www.ticbeat.com/tecnologias/10-grandes-amenazas-seguridad-bases-datos/

10. CONCLUSIONES

El proyecto aplicado sobre el prototipo de seguridad partió sobre la idea de generar una alternativa para implementar una barrera de seguridad para el acceso no autorizado, esto se cumplió desde la búsqueda de componentes, diseño y creación del circuito, hasta la instalación en el salón 1201, aunque algunos componentes no eran acordes a los requerido, el ejercicio de buscar un plan b y nuevas alternativas fue satisfactorio, generando mayor conocimiento sobre el tema.

Se trabaja sobre una alternativa constante y confiable de generación de registros en la base de datos, la cual debe ser compatible con el programa utilizado para el desarrollo de la aplicación, encontrando varias barreras como el error de comunicación entre la base de datos y la aplicación, sin embargo, se logra generar los registros de acuerdo con el objetivo planteado inicialmente.

Las pruebas y los resultados obtenidos permitieron evidenciar que cumplen con los requerimientos y las necesidades de la institución generando satisfacción por parte de las personas encargadas de la administración del salón, por ende, la aprobación de la instalación, generando confianza y motivación en cada fase del proyecto, a su vez se encuentra el interés de los estudiantes por adquirir conocimiento sobre el trabajo desarrollado en el salón 1201.

Las expectativas se cumplieron, fue un reto muy grande ya que es un prototipo que no existe en el mercado y la documentación no es suficiente para el desarrollo del dispositivo, lo que genera mayor investigación y análisis sobre las estrategias para el cumplimiento de cada objetivo.

11. RECOMENDACIONES

Teniendo en cuenta el trabajo sobre el cumplimiento del objetivo general y los objetivos específicos, se obtienen resultados que permiten la instalación del prototipo en el salón 1201 para el uso de la Corporación de Educación Tecnológica Colsubsidio, para las diferentes pruebas y puesta punto. Con el fin de generar un buen uso y manejo del prototipo se establecen las siguientes recomendaciones:

- Se deben generar políticas de uso y manipulación del prototipo, con el fin de que no sufra ningún tipo de daño en su estructura y en los componentes. La ubicación mirándolo desde el interior es: al lado izquierdo de la puerta el emisor láser y al lado izquierdo la caja con el receptor conectado a la placa y demás componentes, conlleva a que las personas que ingresen durante el día lo quieran manipular o que accidentalmente por movimientos de las mesas lo golpeen, por esta razón pueden tomar varias opciones, como la de ubicarlo en la parte superior, o protegerlo con una caja metálica, entre otras alternativas que pueda tomar la organización para garantizar la protección.

- Es importante trabajar en el cuidado del entorno donde se encuentra instalado evitando el traslado dentro del salón, marcándolo con mensajes para impedir la manipulación no autorizada, con políticas de control para verificar su funcionamiento a diario.

- Velar por la protección de los componentes y la caja ubicada en la puerta de acceso al salón 1201, en lo posible ubicar la caja en una especie de estructura con candado para que no sufra ningún daño.

- Asignar un administrador para el control de intrusiones y que este actor dé aviso en caso de una intrusión en tiempos no autorizados, este rol cumple un papel importante, será la persona que tendrá instalada la aplicación para el control de acceso, identificando las intrusiones que se puedan dar, tiene la opción de apagar y encender el sistema cuando sea requerido y, por último, dará aviso en caso de una intrusión no autorizada, que detecte en su celular.

- El administrador tendrá la responsabilidad de activar y desactivar el sistema según las políticas generadas por la Corporación, estas políticas deben ser claras porque de esto depende el manejo del prototipo, de la aplicación y lo más

importante, de la seguridad de la información, activo vital para la Corporación, quien a su vez debe velar por el control del prototipo instalado en el salón 1201.

- La base de datos debe ser controlada por una persona con conocimiento en el tema de manejo de base de datos en phpmyadmin, debido a que tiene la responsabilidad de identificar los eventos de intrusiones, con el fin de generar los respectivos informes para la corporación, administrador o quien designe la compañía puede que esta competencia también la pueda tener el administrador, sería lo mejor para centralizar la información de manera más organizada.

- La Corporación establecerá el control del manejo del dispositivo una vez instalado, puede ser usado como apoyo a la seguridad o con fines pedagógicos si así lo requiere. Es importante que quien imparta la formación a los estudiantes, tenga el conocimiento sobre electrónica, Arduino, programación en bloques, bases de datos, para que de este modo pueda dar a conocer el funcionamiento del dispositivo de manera adecuada, dándole el enfoque correcto.

- La Corporación debe generar políticas del manejo adecuado de la información generada de las intrusiones y posteriormente los registros que quedaran alojados en las bases de datos, ya que estos registros pueden ser manipulados indebidamente con el fin de encubrir un acceso no autorizado.

BIBLIOGRAFÍA

ALOMÍA ARCE, Hernan; ESCALLÓN S., Víctor y ORTEGÓN G., Katherine. guía metodológica para realización de proyectos de grado. En: Departamento de ingeniería industrial. 2006. [Consultado: 06 de junio de 2019]. Disponible en ftp://ftp.icesi.edu.co/leonardo/PGI/Guia%20Estudiantes.pdf

CAMELO, Leonardo. Marco legal de seguridad de la información en Colombia [blog]. En: Seguridad de la información en Colombia. 23 de febrero de 2010. [Consultado: 17 de mayo de 2019]. Disponible en http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html

CORPORACIÓN DE EDUCACIÓN TECNOLÓGICA COLSUBSIDIO, Nosotros CET Colsubsidio [sitio web]. Bogotá; [Consultado: 13 de abril de 2020]. Disponible en: https://cetcolsubsidio.edu.co/conoce-la-cet/nosotros-cet/

COSTAS SANTOS, Jesús. Seguridad informática. [en línea]. España: Ra-Ma. 2014. [Consultado: 18 de abril de 2019]. Disponible en: Base de datos UNAD – e-libro. https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/detail.action?docID=3228430

DESCUBREARDUINO Construye un sistema de seguridad con laser con Arduino [en línea]. Proyectos Arduino útiles, sencillos y avanzados. [Consultado: 20 de mayo de 2019]. Disponible en: https://descubrearduino.com/construye-sistema-seguridad-con-arduino/

DIAZ, Andrés, et al. Implementación de un sistema de gestión de seguridad de la información. En: Sistemas de gestión de seguridad de la información [en línea]. Bogotá: Fundación Universitaria Konrad Lorenz, 2 p. [Consultado: 13 de abril de 2019]. Disponible en http://www.konradlorenz.edu.co/images/stories/articulos/SGSI.pdf

DUALTRONICA. Modulo Wifi ESP8266. [en línea]. Módulos. [Consultado: 23 de julio de 2019]. Disponible en: https://dualtronica.com/modulos/58-modulo-wifi-esp8266.html

ELECTRONICAPLUGANDPLAY. Fotocelda Sensor de Luz LDR-GL5528. [en línea]. Sensores y transductores. [Consultado: 03 de julio de 2019]. Disponible en: http://www.electronicaplugandplay.com/sensores-y-transductores/product/319-fotocelda-sensor-de-luz-ldr-gl5528

ELECTRÓNICO CALDAS. HC – 05. [en línea]. Módulos. [Consultado: 06 de agosto de 2019]. Disponible en: https://www.electronicoscaldas.com/modulos-rf/452-modulo-bluetooth-hc-05.html

GRUPO CONTROL. Evolución de la Seguridad Informática. Grupo control, 25 de febrero de 2019. [Consultado: 10 de mayo de 2019]. Disponible en https://www.grupocontrol.com/evolucion-de-la-seguridad-informatica.

GUTIERREZ AMAYA, Camilo. La seguridad física como parte integral de la seguridad de la información. Welivesecurity, 29 de enero de 2013. [Consultado: 25 de abril de 2019]. Disponible en https://www.welivesecurity.com/la-es/2013/01/29/seguridad-fisica-como-parte-integral-seguridad-informacion/

MARRERO TRAVIESO, Yran. La Criptografía como elemento de la seguridad informática. En: SCIELO: ACIMED [en línea]. Ciudad de la Habana, nov-dic de 2003. vol. 11, nro. 6. [Consultado: 01 de mayo de 2019]. Disponible en http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012&lng=es&nrm=iso. ISSN: 1024-9435.

MOVILTRONICS. Módulo Diodo Laser. [en línea]. Sensores. [Consultado: 12 de julio de 2019]. Disponible en: https://moviltronics.com.co/varios/224-modulo-diodo-laser-.html

OBS BUSINEES. ¿Cuáles son las etapas de un proyecto? Te lo contamos en esta infografía. [en línea]. Noticias. [Consultado: 11 de junio de 2019]. Disponible en: https://obsbusiness.school/int/noticias/innovacion/cuales-son-las-etapas-de-un-proyecto-te-lo-contamos-en-esta-infografia

PC COMPONENTES. Módulo Receptor de Infrarrojos compatible con Arduino. [en línea]. Arduino. [Consultado: 30 de junio de 2019]. Disponible en: https://www.pccomponentes.com/m-dulo-receptor-de-infrarrojos-compatible-con-arduino

PEREZ MARTINEZ, Felix. El papel de las TIC en los sistemas para la seguridad y la defensa. En: Seguridad y Defensa. Enero de 2006. [Consultado: 23 de mayo de 2019]. Disponible en https://www.coit.es/sites/default/files/archivobit/pdf/felixperez.pdf

ROA BUENDÍA, José Fabián. Seguridad informática. 2 ed. España: McGraw-Hill Interamericana. 2013, 9 p. ISBN: 978-84-481-8569-5.

VERIZON, (Data Breach). Las 10 grandes amenazas de seguridad en las bases de datos. “Citado por:” TICBEAT. 17 de abril de 2013 [en línea]. Tecnología. [Consultado: 28 de septiembre de 2019]. Disponible en: http://www.ticbeat.com/tecnologias/10-grandes-amenazas-seguridad-bases-datos/