PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE ESMERALDAS

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y CONTABLES

SISTEMAS Y COMPUTACIÓN

TESIS DE GRADO

"CREACIÓN DE UN DISPOSITIVO PARA LA PROTECCIÓN Y SEGURIDAD DE LOS CPU EN EL LABORATORIO DE COMPUTACIÓN DE LA PUCESE, MONITOREADO POR UN SISTEMA INFORMÁTICO"

Previo al grado académico de

INGENIERA EN SISTEMAS Y COMPUTACIÓN

AUTOR:

ESTUPIÑÁN SUÁREZ SUSANA TATIANA

ASESOR:

ING. MANUEL NEVÁREZ

ESMERALDAS 2015

"Trabajo de tesis aprobado luego de haber dado cumplimiento a los requisitos exigidos por el reglamento de Grado de la PUCESE previo a la obtención del título de Ingeniero de Sistemas y Computación".

…….

PRESIDENTE TRIBUNAL DE GRADUACIÓN

…….

LECTOR 1

…….

LECTOR 2

…….

DECANO DE LA FACULTAD/DIRECTOR DE ESCUELA

…….

DIRECTOR DE TESIS

AUTORÍA

“Yo, SUSANA TATIANA ESTUPIÑÀN SUÀREZ, declaro que la presente investigación enmarcada en el actual trabajo de tesis es absolutamente original, autentica y personal.

En virtud que el contenido de ésta investigación es de exclusiva responsabilidad legal y académica del autor y de la PUCESE.

_____

SUSANA TATIANA ESTUPIÑÀN SUÀREZ

0802943019

DEDICATORIA

Dedico mi tesis de grado con amor y dedicación:

A Dios, por darme salud, fuerzas y perseverancia para poder superar todos los obstáculos, que se me han presentado a lo largo de mi vida, por permitir vivir cosas buenas y malas, gracias a eso soy una persona de bien.

Como no dedicárselo a mis dos Madres; Nora e Irma que han estado junto a mí a lo largo de esta carrera y de mi vida con sus consejos y enseñanzas para que sea una persona con principios, mi hermano José Enrique enseñándome que un fracaso no es un obstáculo para superarse, apoyándome y con amor y oración superar los inconvenientes de la vida.

Porque no dedicárselo a mis demás familiares y amigos que siempre han estado pendientes de mis logros y fracasos, enseñándome que la vida es de superación y constancia para lograr lo que deseamos.

AGRADECIMIENTO

Primeramente gracias a Dios, por darme la vida y llegar hasta donde ahora he llegado, a mis padres, hermano y primos que han estado conmigo dándome fuerzas para cada día salir adelante con cada uno de los consejos dados.

A los docentes de la PUCESE, por los conocimientos brindados y valores infundidos a lo largo de mi carrera universitaria, sembrando en mí, el aspecto humano y social.

A mi asesor de Tesis, el Ing. Manuel Nevárez por todo el esfuerzo y apoyo brindado que con paciencia y dedicación a contribuido que esta tesis tenga sustento teórico, al Ing. Xavier Quiñonez por ser parte del grupo de lector para darle un aval a la tesis, gracias por cada momento compartido en las aulas de clase, y porque no agradecerle al Ing. David Rodríguez, por sugerirme el tema de tesis, aparte de ser Docente es amigo el cual con sus consejo y enseñanzas ha formado de mí una persona de principios.

CONTENIDO

DEDICATORIA iv

AGRADECIMIENTO v

CONTENIDO vi

RESUMEN 1

INTRODUCCIÓN 3

CAPÍTULO I: FUNDAMENTOS TEÓRICOS 4

1.1 PUCESE 4

1.1.1 Historia 4

1.1.2 Misión 5

1.1.3 Visión 5

1.1.4 Valores 5

1.1.5 Organigrama 6

1.1.6 Infraestructura 7

1.2 SISTEMA 8

1.2.1 Definición 8

1.2.2 Sistema Informático (SI) 8

1.2.3 Sistema De Información 9

1.3 DESARROLLO DE SOFTWARE 10

1.3.1 Definición 10

1.3.2 Proceso 10

1.4 LOS MICROCONTROLADORES 12

1.4.1 Definición 12

1.4.2 Características de los Microcontroladores 12

1.4.3 Clasificación de los Microcontroladores 13

1.4.4 Desarrollo con Microcontroladores 17

1.5 DISEÑO DE HARDWARE 18

1.5.1 Diseño de PCB o tarjetas electrónicas 18

1.5.2 Componentes Electrónicos 18

1.5.3 Cajas de Protección 19

1.5.4 Aplicaciones con Microcontroladores 24

1.6 CPU 25

1.6.1 Importancia 25

1.6.2 Protección 26

1.6.3 Medidas De Seguridad 26

1.7 BASES DE DATOS 27

1.7.1 Definición 27

1.7.2 Sistema de gestor de Base de Datos 27

1.8 SENSORES 29

1.8.1 Definición 29

1.8.2 Redes de Sensores 30

1.8.3 Diseño de una Red de Sensores 30
1.8.4 Sistema de monitoreo de sensores 32
1.8.4.1 Inalámbrico 32
1.8.4.2 Aplicaciones 32
1.9 DISPOSITIVO USB 33
1.9.1 Definición 33
1.9.2 Funcionamiento 33
1.9.3 Clasificación 33
1.9.4 Modo de Transferencia 34
1.9.5 Cómo se realiza la transferencia de información 35
1.10 COMUNICACIÓN ENTRE DISPOSITIVOS 35
1.10.1 Comunicación Serial 35
1.10.2 Comunicación por USB 36
1.10.3 Comunicación por Radiofrecuencia 37
CAPITULO II 39
2 DIAGNÓSTICO 39
2.1 ANTECEDENTES DIAGNÓSTICO 39
2.2 OBJETIVOS DIAGNÓSTICO 40
2.3 VARIABLES DEL DIAGNÓSTICO 40
2.3.1. Jefe del departamento 40
2.3.2. Infraestructura 40

2.3.3. Encargados del Laboratorio 41

2.3.4. Usuarios del Laboratorio 41

2.3.5. Dispositivos y Central de Monitoreo 41

2.4. INDICADORES O SUBASPECTOS 41

2.4.1. Número de equipos dentro del laboratorio de computación 41

2.4.2. Número de máquinas más frecuentes a utilizar 41

2.4.3. Fácil Manejo 42

2.5. MATRIZ DIAGNOSTICA 42

2.6. MECÁNICA OPERATIVA 44

2.6.1. Población o Universo 44

2.6.2. Muestra 45

2.6.3. Información Primaria 46

2.6.3.1. Observación 46

2.6.3.2. Encuesta 46

2.6.3.3. Entrevistas 46

2.6.4. Información Secundaria 47

2.7. TABULACIÓN Y ANÁLISIS DE LA INFORMACIÓN 47

2.7.1. Encuesta dirigida al personal docente que da clases en el laboratorio de computación de la PUCESE 47

2.7.2. Encuesta dirigida al personal administrativo de la PUCESE 54

2.7.3. Análisis de la entrevista a la encargada del laboratorio de computación . 60

2.7.4. Análisis de la entrevista al jefe de sistemas 60
2.8. FODA 61
2.8.1. Fortalezas 61
2.8.2. Debilidades 61
2.8.3. Oportunidades 61
2.8.4. Amenazas 62
2.9. ESTRATEGIAS FA, FO, DO, DA 62
2.10. DETERMINACIÓN DEL PROBLEMA DIAGNOSTICO 65
CAPITULO III: 66
3 ANTECEDENTES 66
3.1 JUSTIFICACIÓN 67
3.2 OBJETIVOS DE LA PROPUESTA 68
3.2.1 OBJETIVOS GENERALES 68
3.2.2 OBJETIVOS ESPECIFICOS 68
3.3 SOLUCIÓN INFÓRMATICA 68
3.3.1 Requerimientos del sistema 69
3.4 DESARROLLO 70
3.4.1 Diseño de Software 70
3.4.2 Sqlite 71
3.4.3 Diseño de hardware 73
3.4.4 Instalación y Verificación del Sistema 77

3.4.5 Instalación de las Antenas Modificadas 77

3.4.6 Instalación de las Etiquetas DR 77

3.5 MANUAL DE USUARIO 78

3.5.1 Interface de bienvenida 78

3.5.2 Interfaz de configuración 79

3.5.3 Interfaz de registro 80

3.5.4 Interfaz Arduino 81

CAPITULO IV 82

4 ANTECEDENTES 82

4.1 Impacto Institucional 83

4.2 Impacto Social 84

4.3 Impacto Económico 86

4.4 Impacto Tecnológico 87

4.5 Matriz General 88

CAPITULO V 90

5 CONCLUSIONES Y RECOMENDACIONES 90

5.1 CONCLUSIONES 90

5.2 RECOMENDACIONES 91

6 BIBLIOGRAFIA 92

ANEXOS 96

- Anexo 1 97

- Anexo 2 99
- Anexo 3 101
- Anexo 4 102
- Anexo 5 103

Gráfico 1. Organigrama Institucional 6

Gráfico 2. Proceso del Desarrollo de Software 10

Gráfico 3. Relación pregunta Nº1 48

Gráfico 4. Relación pregunta Nº2 49

Gráfico 5. Relación pregunta Nº3 50

Gráfico 6. Relación pregunta Nº4 51

Gráfico 7. Relación pregunta Nº5 52

Gráfico 8. Relación pregunta Nº6 53

Gráfico 9. Relación pregunta Nº1 Administrativo 54

Gráfico 10. Relación pregunta Nº2 Administrativo 55

Gráfico 11. Relación pregunta Nº3 Administrativo 56

Gráfico 12. Relación pregunta Nº4 Administrativo 57

Gráfico 13. Relación pregunta Nº5 Administrativo 58

Gráfico 14. Relación pregunta Nº6 Administrativo 59

Gráfico 15. Tabla de Registro 71

Gráfico 16. Tabla Usuario 72

Gráfico 17. Etiquetas DR 74

Gráfico 18. Panta de Inicio 78

Gráfico 19. Información del Desarrollador 78

Gráfico 20. Detalle de los incidentes 79

Gráfico 21. Pantalla de Configuración 80

Gráfico 22. Resumen de los sucesos 80

Gráfico 23. Puertos COM 81

Tabla 1. Matriz Diagnostica 42

Tabla 2. Tabulación pregunta Nº1 para Docente 47

Tabla 3. Tabulación pregunta Nº2 para Docente 48

Tabla 4. Tabulación pregunta Nº 3 para Docente 49

Tabla 5. Tabulación Pregunta Nº 4 para Docente 50

Tabla 6. Tabulación pregunta Nº 5 para Docente 51

Tabla 7. Tabulación pregunta Nº 6 para Docente 52

Tabla 8. Tabulación pregunta Nº 1 para Administrativo 54

Tabla 9. Tabulación pregunta Nº 2 para Administrativo 55

Tabla 10. Tabulación pregunta Nº 3 para Administrativo 56

Tabla 11. Tabulación pregunta Nº 4 para Administrativo 57

Tabla 12. Tabulación pregunta Nº 5 para Administrativo 58

Tabla 13. Tabulación pregunta Nº 6 para Administrativo 59

RESUMEN

En el mundo de la informática y la tecnológica los sistemas de seguridad física han ido evolucionando a medida que las empresas e instituciones educativas han tenido la necesidad de protección y seguridad de sus equipos tecnológicos que poseen, el proyecto permitió la creación de un dispositivo para la protección y seguridad de los equipos de computación en el laboratorio principal de la PUCESE, se diseñó un sistema informático de monitoreo, siendo esta implementación de gran importancia para la institución educativa. El sistema sirvió como complemento a las cámaras que se encuentran en el laboratorio, así el departamento de sistemas tuvo control de sus equipos que conforman el laboratorio de computación, es por aquello que esta investigación planteó como objetivo la implementación de un sistema de monitoreo que permita controlar la seguridad física y protección de los equipos, ligada a la utilización del software libre, de esta manera aportar en diversas aéreas donde se pueda aplicar esta nueva tecnología y que mejor manera hacerlo con la dotación de un software para aquello.

En el diagnostico se confirma la existencia del problema, en donde se tomó como metodología de investigación la entrevista, encuesta y observación, con un nivel de investigación de carácter descriptiva y de campo, donde se tuvo como muestra 123 trabajadores entre docentes y administrativos, el análisis de las entrevistas mostró la importancia de la implementación del sistema en el laboratorio y de esta manera controlar los equipos tecnológicos. Se consideró que este proyecto es de gran utilidad y posee un gran potencial, ya que en un futuro puede ser implementado en otras aéreas que requieran de un sistema de control y monitoreo de los equipos dentro de la PUCESE.

ABSTRACT

In the world of computer and technological systems of physical security have been evolving as companies and educational institutions have the need for protection and security of their technological equipment they have, the project enabled the creation of a device for safety and security of computer equipment in the main lab PUCESE, a computer monitoring system was designed, with the implementation of major importance to the school. The system served as a complement to the cameras found in the laboratory, and the IT department had control of their teams that make the computer lab, that's what this research raised the objective of implementing a monitoring system that allows control the physical safety and security equipment, connected with the use of free software in this way contribute in diverse areas where we can apply this new technology and what better way to do it with the provision of software for that.

In diagnosing the problem exists, where it was used as research methodology interview, survey and observation, with a level of research of descriptive character and field, where it was to sample 123 workers between teachers and administrators, is confirmed analysis of interviews showed the importance of implementing the system in the laboratory and thus control technological equipment. It was felt that this project is very useful and has great potential as a future can be implemented in other areas that require a control system and monitoring equipment within the PUCESE.

INTRODUCCIÓN

En la actualidad vemos como la tecnología y la seguridad de equipos tecnológicos avanza para mejoras tantas educativas y a nivel empresarial llevando al éxito cada una de estas entidades, sin embargo anteriormente en el laboratorio de computación no era lo suficiente la seguridad de los equipos tecnológicos mediante las cámaras instaladas, porque existía inconvenientes con los hurto de mouse que son los más vulnerables, siendo que se descompense el uso del equipo tecnológico, es por aquello que diseña un dispositivo para la protección y seguridad de los equipos del laboratorio de computación de la PUCESE, monitoreado por un sistema informático, llegando a cubrir las necesidades y requerimientos para la mejora del laboratorio.

En el proceso de la investigación se analiza el tema de software y hardware libre, sistema de seguridad, base de datos y los dispositivos de seguridad, detallando definiciones, importancias y usos. Cabe argumentar que uno de los temas más transcendentales a investigar es la herramienta de software JAVA y dispositivos de seguridad referente a hardware Arduino con una conexión vía bluetooth, para que pueda existir una comunicación con la antena anti-hurto AM. Se especifica este tipo de antena mencionada anteriormente, porque es la más apropiada entre los tipos existentes (AM, RF Y EM), dependiendo también del área a implementarse, cada una de estas antenas tiene asociadas sus propias etiquetas para un mejor funcionamiento de las mismas. Se describieron métodos de investigación, como la entrevista, para ver la factibilidad y viabilidad que existía al implementar este tipo de seguridad en el laboratorio, enlazado con una encuesta el cual permitió analizar de una mejor manera y notar que tan importante es la adquisición de un sistema el cual permita controlar el hurto de los equipos tecnológicos dentro del laboratorio de computación dando un plus a una mejor infraestructura tecnología.

La implementación de este sistema de seguridad electrónica para el control de los equipos tecnológicos dentro del laboratorio es relevante en la PUCESE, pues es así que podría implementar en lugares como la biblioteca para el control de los libros que son prestados a estudiantes para la realización de consultas, porque no también decir que es un sistema innovador así otras empresas podrán adquirirlos y proteger sus equipos ante algún hurto de aquellos.

CAPÍTULO I: FUNDAMENTOS TEÓRICOS

1.1 PUCESE

1.1.1 Historia

"La Sede de Esmeraldas de la PUCE, tuvo en Monseñor Ángel Barbisotti su mentalizador, quien, según el boletín oficial del Vicariato Apostólico de Esmeraldas, llamado APERTURA, del año 1984, en el artículo escrito por el Padre Juan Meloni se expresa que al llegar Monseñor Enrique Bartolucci como nuevo Obispo de Esmeraldas, se entusiasma por la idea de su predecesor y comenta esta iniciativa con el Padre Meloni, quien puso a caminar el proyecto de la Iglesia de Esmeraldas recogiendo las intenciones de Monseñor Ángel Barbisotti, mismas que las había asumido el nuevo Obispo de Esmeraldas Monseñor Bartolucci, y que se concretaban en una opción de educación superior propuesta por la Iglesia de esta provincia a la juventud.

El P. Meloni comenta que existieron algunos encuentros con los miembros de la Conferencia Episcopal Ecuatoriana, diálogos con el rector de la matriz, hasta que en la segunda mitad del mes de julio de 1980, el Obispo de Esmeraldas presenta oficialmente a Rector de la PUCE el pedido de la creación de la Sede.

Con la presencia del Gran Canciller de la PUCE y otras autoridades de Quito, del Vicariato Apostólico de Esmeraldas, el 5 de junio de 1981, se inaugura solemnemente el primer año académico de la Sede.

A la fecha de su creación, la PUCESE tenía como recursos económicos propios 156.00 sucres (moneda oficial de la época) y funcionaba en un aula del Instituto Normal Superior No. 8, que había cedido en calidad de préstamo. El P. Juan Meloni, Rector del Instituto, también fue encargado del Pro-Rectorado de la naciente Sede y compartía su despacho para las dos instituciones de la Iglesia.

La primera biblioteca de la PUCESE fue donada por los provinciales combonianos de México y España" (PUCESE, 1990).

1.1.2 Misión

Formar continua, personalizada e integralmente a seres humanos con sentido emprendedor social, ético, crítico y autocrítico, a la luz del evangelio, capaces de liderar y generar transformaciones en orden a una provincia solidaria, justa, pacífica y que respeta la biodiversidad, desarrollando propuestas científicas, innovadoras y sostenibles (PUCESE, 2013).

1.1.3 Visión

La PUCESE será una institución educativa en búsqueda permanente de la excelencia académica, con carreras acreditadas, apoyada en la estructura de trabajo por áreas de conocimiento; estrechamente vinculada a organizaciones de los sectores educativos, productivos, de salud y medioambientales de Esmeraldas, como provincia costera; participando en redes de investigación, intercambio y formación de estudiantes y docentes con instituciones de educación superior nacionales e internacionales, a través de trabajo cooperativo en propuestas de transformación social (PUCESE, 2013).

1.1.4 Valores

- Armonía
- Justicia
- Solidaridad
- Dignidad
- Conciencia y responsabilidad social
- Servicio
- Respeto
- Capacidad crítica y autocritica
- Iniciativa (emprendimiento)
- Trabajo en equipo
- Equidad

1.1.5 Organigrama

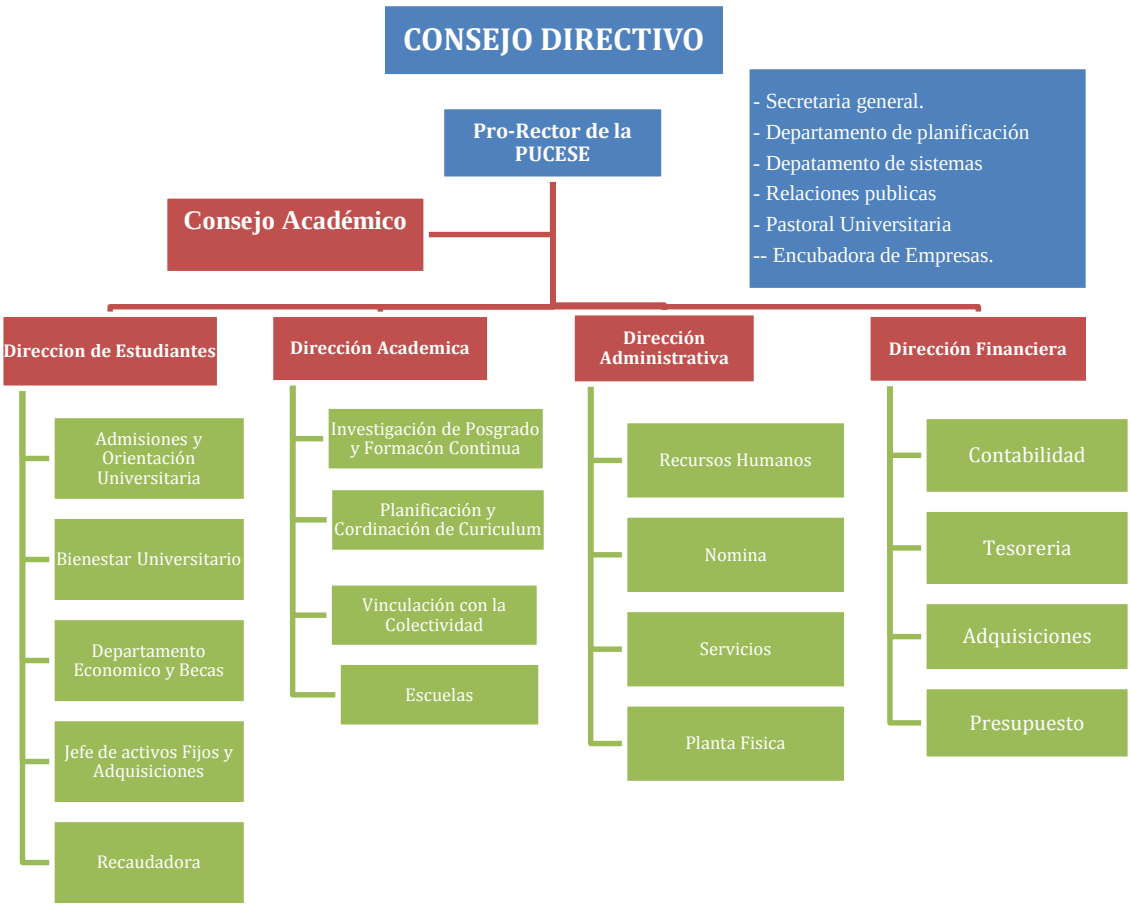


Gráfico 1. Organigrama Institucional

Fuente: Pagina Web Pucese

1.1.6 Infraestructura

La PUCESE cuenta con una infraestructura arquitectónica y tecnológica para el desarrollo y bienestar de la comunidad esmeraldeña, permitiendo a los estudiantes realizar sus actividades de una manera rápida y precisa.

Se cabe recalcar que la Infraestructura es un elemento que se considera muy necesario para el funcionamiento de una organización.

1.1.6.1 Infraestructura Arquitectónica

La PUCESE cuenta con dos grandes infraestructuras arquitectónicas ubicadas en las calles Espejo y Subida a Santa Cruz, en la parte céntrica se encuentran ubicados dos edificios; el primero la distribución de las aulas de las escuelas de: Ingeniería en Sistemas y Computación, Diseño Gráfico, Lingüística, Comercio Exterior, Contabilidad y Auditoría, Educación Inicial; en el segundo se encuentran los diferentes departamentos administrativo, los laboratorios de computación, laboratorio de lingüística, laboratorio de Diseño Gráfico, biblioteca, sala de audiovisuales.

1.1.6.2 Infraestructura Tecnológica

La infraestructura tecnológica es la base primordial de cualquier empresa que permite la optimización de sus recursos, el aumento de su valor y una respuesta más rápida a los requerimientos del mercado.

Considerando la PUCESE con una buena infraestructura tecnológica, posee de laboratorios condicionados para el desempeño de los estudiantes permitiendo tener una excelencia académica.

1.2 SISTEMA

1.2.1 Definición

Un sistema es un conjunto de partes o elementos organizados y relacionados que interactúan entre sí para lograr un objetivo. Los sistemas reciben (entrada) datos, que proveen (salida) información.

El ambiente es el medio externo que envuelve física o conceptualmente a un sistema. El sistema tiene interacción con el ambiente, del cual recibe entradas y al cual se les devuelven salidas. El ambiente también puede ser una amenaza para el sistema (Alegsa, 1998).

1.2.2 Sistema Informático (SI)

Un sistema informático es un conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso. Sus partes son: hardware, software y las personas que lo usan.
Un sistema informático puede formar parte de un sistema de información; en este último la información, uso y acceso a la misma, no necesariamente está informatizada (Alegsa, 1998).

1.2.2.1 Estructura Del Sistema Informático

Los sistemas informáticos suelen estructurarse en subsistemas:

- **Subsistema físico:** asociado al hardware. Incluye entre otros elementos la CPU, memoria principal, la placa base, periféricos de entrada y salida, etc.

- **Subsistema lógico:** asociado al software y la arquitectura. Incluye al sistema operativo, el firmware, las aplicaciones y las bases de datos.

1.2.3 Sistema De Información

Es un conjunto de elementos los cuales interactúan entre sí con el fin de proporcionar información para la toma de decisiones en una empresa para cubrir una necesidad u objetivo.

Los (SI) realizan cuatro actividades básicas; entrada, almacenamiento, procesamiento y salida de información; a continuación se detallara cada una de ellas.

- **Entrada de Información:** Es el proceso mediante el cual el Sistema de Información toma los datos que requiere para procesar la información. Las entradas pueden ser manuales o automáticas. Las manuales son aquellas que se proporcionan en forma directa por el usuario, mientras que las automáticas son datos o información que provienen o son tomados de otros sistemas o módulos.

- **Almacenamiento de Información:** El almacenamiento es una de las actividades o capacidades más importantes que tiene una computadora, ya que a través de esta propiedad el sistema puede recordar la información guardada en la sección o proceso anterior. Esta información suele ser almacenada en estructuras de información denominadas archivos. La unidad típica de almacenamiento son los discos magnéticos o discos duros y los discos compactos (CD-ROM).

- **Procesamiento de Información:** Es la capacidad del Sistema de Información para efectuar cálculos de acuerdo con una secuencia de operaciones preestablecida. Estos cálculos pueden efectuarse con datos introducidos recientemente en el sistema o bien con datos que están almacenados.

- **Salida de Información**: La salida es la capacidad de un Sistema de Información para sacar la información procesada o bien datos de entrada al exterior. Las unidades típicas de salida son las impresoras, terminales, cintas magnéticas y los plotters, entre otros. Es importante aclarar que la salida de un Sistema de Información puede constituir la entrada a otro Sistema de Información o módulo (BERMUDEZ, VARGAS IZQUIERDO, & SUAREZ RIVERA, 2010).

1.3 DESARROLLO DE SOFTWARE

1.3.1 Definición

Es un programa que permite el Desarrollo de Aplicaciones. Se conoce por IDE (Integrated Development Environment, por sus siglas en inglés). Se utiliza para hacer programas en diferentes lenguajes por ejemplo (C++, Java, Python, Lisp, etc).

Cuando se va desarrollar un software intervienen muchos individuos como lo es el cliente, quien es el que tiene el problema en su empresa y desea que este sea solucionado, para esto existe el analista de sistema quien es el encargado de hacerle llegar todos los requerimientos y necesidades que tiene el cliente a los programadores, quienes son las personas encargadas de realizar lo que es la codificación y diseño del sistema para después probarlo e instalarlo al cliente. Es así como intervienen varias personas ya que una sola no podría determinar todo lo necesario que requiere el cliente (PADILLA, 2008).

1.3.2 Proceso

Un proceso para el desarrollo de software, también es denominado ciclo de vida del desarrollo de software, una estructura aplicada al desarrollo de un producto de software. Hay varios modelos a seguir para el establecimiento de un proceso para el desarrollo de software, cada uno de los cuales describe un enfoque diferente para diferentes actividades que tienen lugar durante el proceso (TRUJILLO GRANADOS & MERCHAN MILLAN, 2012).

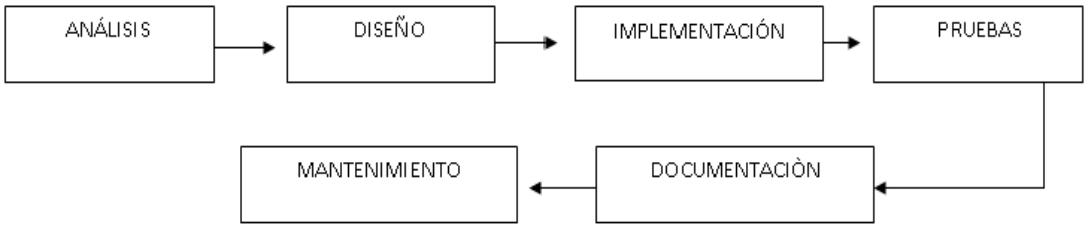


Gráfico 2. Proceso del Desarrollo de Software

Fuente: Autor

- **Análisis.-** En esta etapa se debe entender y comprender de forma detallada cual es la problemática a resolver, verificando el entorno en el cual se encuentra dicho problema, de tal manera que se obtenga la información necesaria y suficiente para afrontar su respectiva solución. Esta etapa es conocida como la del QUÉ se va a solucionar.

- **Diseño.-** Una vez que se tiene la suficiente información del problema a solucionar, es importante determinar la estrategia que se va a utilizar para resolver el problema. Esta etapa es conocida bajo el CÓMO se va a solucionar.

- **Implementación.-** Partiendo del análisis y diseño de la solución, en esta etapa se procede a desarrollar el correspondiente programa que solucione el problema mediante el uso de una herramienta computacional determinada.

- **Pruebas.-** Los errores humanos dentro de la programación de los computadores son muchos y aumentan considerablemente con la complejidad del problema. Cuando se termina de escribir un programa de computador, es necesario realizar las debidas pruebas que garanticen el correcto funcionamiento de dicho programa bajo el mayor número de situaciones posibles a las que se pueda enfrentar.

- **Documentación.-** La documentación en un proyecto de software es importante porque permite conservarla historia, facilita la utilización por parte del usuario, garantiza la permanecía y disminuye los costos de operación y de ejecución del proyecto como tal.

- **Mantenimiento.-** Una vez instalado un programa y puesto en marcha para realizar la solución del problema previamente planteado o satisfacer una determinada necesidad, es importante mantener una estructura de actualización, verificación y validación que permitan a dicho programa ser útil y mantenerse actualizado según las necesidades o requerimientos planteados durante su vida útil. Para realizar un adecuado mantenimiento, es necesario contar con una buena documentación del mismo (E.J, 2003).

1.4 LOS MICROCONTROLADORES

1.4.1 Definición

Es un circuito integrado programable, capaz de ejecutar las órdenes grabadas en su memoria. Está compuesto de varios bloques funcionales, los cuales cumplen una tarea específica, a continuación algunas de sus partes.

- **Memoria ROM** (Memoria de sólo lectura)
- **Memoria RAM** (Memoria de acceso aleatorio)
- **Líneas de entrada/salida (I/O)** También llamados puertos
- **Lógica de control** Coordina la interacción entre los demás bloques

El funcionamiento de los micros controladores está determinado por el programa almacenado en su memoria. Este puede escribirse en distintos leguajes de programación. Además, la mayoría de los micros controladores actuales pueden reprogramarse repetidas veces.

1.4.2 Características de los Microcontroladores

- **Unidad de Procesamiento Central (CPU):** Típicamente de 8 bits, pero también las hay de 4, 32 y hasta 64 bits con arquitectura Harvard, con memoria/bus de datos separada de la memoria/bus de instrucciones de programa, o arquitectura de von Neumann, también llamada arquitectura Princeton, con memoria/bus de datos y memoria/bus de programa compartidas (TORRITI, 2007).
- **Memoria de Programa:** Es una memoria ROM (Read-OnlyMemory), EPROM(Electrically Programable ROM), EEPROM (Electrically Erasable/ProgramableROM) o Flash que almacena el código del programa que típicamente puede ser de 1 kilobyte a varios megabytes.
- **Memoria de Datos:** Es una memoria RAM (Random Access Memory) que típicamente puede ser de 1, 2 4, 8, 16, 32 kilobytes.
- **Generador del Reloj:** Usualmente un cristal de cuarzo de frecuencias que genera una señal oscilatoria de entre 1 a 40 MHz, o también resonadores o circuitos RC.

- **Interfaz de Entrada/Salida:** Puertos paralelos, seriales (UARTs, Universal Asynchronous Receiver/Transmitter), I2C (Inter-Integrated Circuit), Interfaces de Periféricos.
- **Otras opciones:**
    - **Conversores Análogo-Digitales** (A/D, analog-to-digital) para convertirun nivel de voltaje en un cierto pin a un valor digital manipulable por el programa del micro controlador.
    - **Moduladores por Ancho de Pulso** (PWM, Pulse-WidthModulation) para generar ondas cuadradas de frecuencia fija pero con ancho de pulso modificable.

1.4.3 Clasificación de los Microcontroladores

Los Microcontroladores son circuitos los cuales están diseñados para usarse como controlador que ayuda a monitorear y controlar una maquina o una variedad de aplicaciones de control.

1.4.3.1 Según la longitud del Bus de Datos

Micro controladores de 8 bits, 16bits y 32 bits a mayor longitud del bus de datos, mayor será la eficiencia del micro controlador en operaciones con datos grandes. Pero al mismo tiempo la complejidad del chip y por ende su costo también aumentará. Por ejemplo, para los dispositivos multimedia, que procesan datos de vídeo y audio, un bus de datos de 8 bits sería insuficiente. Hoy en día los micros controladores de 8 bits encuentran mayor aplicación y están, de lejos, mucho más difundidos en aplicaciones de la gente aficionada. (ESPINOZA, 2007)

1.4.3.2 Según el set de instrucciones

- **Con Instructions Cisc (Complex Instruction Set Computer).-** El set de instrucciones **CISC** es inherente a los primeros micros controladores que aparecieron en el mundo, los cuales estaban inspirados en los procesadores de los grandes computadores de la época. Es complejo porque consta de muchas instrucciones, complicadas y difíciles de recordar a la hora de programar en

lenguaje ensamblador. Además, al crecer el número de instrucciones también crecerán los códigos de las instrucciones, lo cual deriva en una mella en la eficiencia del micro controlador (SANCHEZ ROSERO & NINACURI GUACHI, 2013).

- **Con Instrucciones Risc (Reducid Instruction Set Computer).-** Estos micros controladores cuentan con instrucciones sencillas y en un número mínimo. Ello permite que la programación en ensamblador sea una labor cómoda y esté al alcance de todos. Sin embargo, cuando se desarrollan proyectos mucho más complejos, el uso del lenguaje ensamblador se torna cada vez más engorroso. Entonces se prefiere optar por los compiladores de alto nivel, para los cuales un set RISC no es obstáculo.

1.4.3.3 Según su Arquitectura Interna

- **Microcontrolador con Arquitectura De Von Neumann.-** Tan simple como verlo en el diagrama estos micros controladores tienen una memoria única que constituye tanto el segmento de memoria de programa como el de datos. Con un solo bus de comunicación entre dicha memoria y el procesador no es posible realizar diversos accesos a la vez.

- **Microcontrolador con Arquitectura Harvard.-** En esta estructura los micros controladores disponen de dos memorias, una que contiene el programa y otra para almacenar los datos. De este modo el CPU puede tener acceso simultáneo a ambas memorias utilizando buses diferentes. Más específicamente, el CPU puede leer la siguiente instrucción de programa mientras está procesando los datos de la instrucción actual. Actualmente todos los micros controladores se inclinan por esta arquitectura

1.4.3.4 Según el Fabricante

Hay muchas marcas de micro controladores en el mercado. A veces un mismo tipo de micro controlador lo suelen proveer diversos fabricantes, por lo que ésta no es una clasificación estrictamente metódica (ESPINOZA, 2007).

- **Pci Micro O Pic De Microchip.-** Son los micros controladores que han fascinado al mundo en los últimos años. Su facilidad de uso, comodidad y rapidez en el desarrollo de aplicaciones, abundante información y libre disposición de herramientas software proporcionada por Microchip le han permitido ganar terreno rápidamente en el mercado de los micro controladores a nivel mundial, hasta convertirse en los micro controladores más vendidos en la actualidad.

- **Microcontrolador Avr De Atmel.-** Uno de los productos estrella de Atmel son micro controladores **AVR**. Comparado con otros microcontroladores de 8 bits, en distintos modelos por supuesto. Optimizado para acelerar el tiempo de lanzamiento del producto, puertos configurables como E/S pin a pin, interfaces de comunicación serial RS232 e I2C, módulos generadores de onda PWM.
  Este hándicap inicial se invierte cuando se utiliza un compilador de alto nivel, ya que los *AVR* fueron diseñados para un óptimo trabajo con el lenguaje C (ATMEL, 2013).

- **Microcontrolador Arduino.-** Arduino es una plataforma de código abierto basado en prototipos de electrónica flexible y fácil de usar hardware y software. Diseñada para facilitar el uso de la electrónica en proyectos multidisciplinares.
  El hardware consiste en una placa con un micro controlador Atmel AVR y puertos de entrada/salida. Los micros controladores más usados son el Atmega168, Atmega328, Atmega1280, ATmega8 por su sencillez y bajo coste que permiten el desarrollo de múltiples diseños. Por otro lado el software consiste en un entorno de desarrollo que implementa el lenguaje de programación y el cargador de arranque que corre en la placa (SANCHEZ ROSERO & NINACURI GUACHI, 2013).

- **Microcontrolador de Fresscale.-** Hace muchos años Motorola era uno de los fabricantes de Microcontroladores con mayores ventas en el mundo. En esos tiempos el trabajo con micros controladores era una actividad casi exclusiva de los considerados gurúes de la microelectrónica y que contaban con suficientes medios para acceder a las herramientas necesarias. Lo cierto es que con el tiempo Motorola empezó a perder su liderazgo y ha preferido ceder la franquicia a Freescale.

- **Los Módulos Basic Stamp de Parallax.-** Los Basic Stamp nos son una nueva familia de microcontrolador; son módulos montados sobre otros micros controladores. Cuentan con un micro controlador, un circuito oscilador, el circuito de interface con el puerto serie de la computadora, una memoria externa para almacenar el programa y un regulador de tensión; todo en una pequeña tarjeta directa fácilmente conectable a las computadoras. Una vez cargado el programa, el módulo está listo para ser insertado en el circuito de aplicación, incluso si está armado en un simple breadboard.

  Los programas se desarrollan íntegramente en un lenguaje Basic adaptado. El programa se carga en la EEPROM serial y el micro controlador del Basic Stamp tiene que interpretarlo.

- **Microcontroladores 8051 de INTEL.-** Intel era otro de los gigantes de los Microcontroladores y µPs. Sus productos más conocidos eran los famosos 8051, 80151 y 80251, pero actualmente ya no tiene interés en fabricarlos. En su lugar, fueron otras compañías, como Atmel, Philips, Infineon, Dallas, entre otros, las que tomaron la posta y fabrican algunas partes compatibles.
  No se puede afirmar qué marca de Microcontrolador es mejor o peor. Es decir, si tomamos un Microcontrolador cualquiera, siempre podremos encontrar un modelo de otro fabricante que pueda sustituirlo en una determinada aplicación.

1.4.4 Desarrollo con Microcontroladores

El proceso de desarrollo de una aplicación basada en micro controladores se compone delas siguientes etapas principales, las cuales se explican en más detalle en las siguientes subsecciones (TORRITI, 2007)**.**

- **Desarrollo de software:** Esta etapa corresponde a la escritura y compilación/ensamblaje del programa que regir a las acciones del µC y los sistemas periféricos conectados a este.
- **Programación del µC:** En esta etapa el código de máquina correspondiente al programa desarrollado en la etapa anterior se descarga en la memoria del µC.
- **Prueba y velicación:** Por último, el µC debe conectarse al circuito base y someterse a pruebas para verificar el funcionamiento correcto del programa.

1.4.4.1 Desarrollo de software

En esta etapa consiste en escribir y compilar/ensamblar el programa que determinará las acciones del µC y su funcionamiento. Existen distintas maneras de desarrollar el programa, dependiendo del lenguaje inicial que se utiliza para escribir el programa.

1.4.4.2 Programación del µC

Este proceso corresponde a utilizar un programa en el PC que toma el código ensamblado (.hex, .o, .bin, .coff) para el µC específico, y lo envía mediante algún puerto (serial, paralelo, USB, etc.) a un dispositivo que lo escribe en la memoria del µC. Se acostumbra denominar programador tanto al software como al hardware involucrado para este propósito, lo cual puede prestarse a confusión. El software programador a veces recibe también el nombre de downloader, ya que su propósito es descargar o transferir desde el PC al µC el código ensamblado.

1.4.4.3 Prueba y Validación

Una vez programado el µC, se puede instalar en el circuito final para comprobar su adecuado funcionamiento. Existen herramientas de software que permiten simular el comportamiento de un µC, muy útiles cuando el programa alcanza cierta complejidad.

Para resolver problemas en un circuito real, el instrumento más utilizado es el analizador lógico.

1.5 DISEÑO DE HARDWARE

En todo sistema sea el más pequeño se requiere de un diseño de hardware, porque es el que complementa al diseño de software. El hardware es la parte la cual podemos tocar es el producto final de lo que se ha requerido.

1.5.1 Diseño de PCB o tarjetas electrónicas

El PCB (del inglés Printed Circuit Board) es una superficie constituida por caminos o pistas de material conductor laminadas sobre un sustrato no conductor. El circuito impreso se utiliza para conectar eléctricamente a través de los caminos conductores, y sostener mecánicamente por medio del sustrato, un conjunto de componentes electrónicos (ALLAN, 2002).

1.5.2 Componentes Electrónicos

- **Resistencias.-** La **resistencia** de un circuito eléctrico determina según la llamada **ley de Ohm** cuánta corriente fluye en el circuito cuando se le aplica un voltaje determinado. La unidad de resistencia es el ohmio, que es la resistencia de un conductor si es recorrido por una corriente de un amperio cuando se le aplica una tensión de 1 voltio. La abreviatura habitual para la resistencia eléctrica es R, y el símbolo del ohmio es la letra griega omega, Ω. En algunos cálculos eléctricos se emplea el inverso de la resistencia, 1/R, que se denomina conductancia y se representa por G. La unidad de conductancia es siemens, cuyo símbolo es S.

- **Diodos.-** Componente electrónicos que permite el paso de la corriente en un solo sentido. Los primeros dispositivos de este tipo fueron los **diodos** de tubo de vacío, que consistían en un receptáculo de **vidrio** o de **acero** al vacío que contenía dos electrodos: un cátodo y un ánodo. Ya que los electrones pueden fluir en un solo sentido, desde el cátodo hacia el ánodo, el diodo de tubo de vacío se podía utilizar en la rectificación. Los diodos más empleados en los circuitos electrónicos actuales

son los diodos fabricados con material semiconductor. El más sencillo, el diodo con punto de contacto de germanio, se creó en los primeros días de **la radio**, cuando la señal radiofónica se detectaba mediante un cristal de germanio y un cable fino terminado en punta y apoyado sobre él. En los diodos de germanio (o de silicio) modernos, el cable y una minúscula placa de cristal van montados dentro de un pequeño tubo de vidrio y conectados a dos cables que se sueldan a los extremos del tubo.

- **Capacitores.-** En electricidad y electrónica, un condensador o capacitor es un dispositivo que almacena energía eléctrica, es un componente pasivo. Está formado por un par de superficies conductoras en situación de influencia total (esto es, que todas las líneas de campo eléctrico que parten de una van a parar a la otra), generalmente en forma de tablas, esferas o láminas, separados por un material dieléctrico (siendo este utilizado en un condensador para disminuir el campo eléctrico, ya que actúa como aislante) o por el vacío, que, sometidos a una diferencia de potencial, adquieren una determinada carga eléctrica, positiva en una de las placas y negativa en la otra (siendo nula la carga total almacenada).

- **Transistores.-** Los transistores se componen de semiconductores. Se trata de materiales, como el silicio o el germanio, dopados (es decir, se les han incrustado pequeñas cantidades de materias extrañas), de manera que se produce un exceso o una carencia de electrones libres. En el primer caso, se dice que el semiconductor es del tipo n, y en el segundo, que es del tipo p. Combinando materiales del tipo n y del tipo p se puede producir un diodo. Cuando éste se conecta a una batería de manera tal que el material tipo p es positivo y el material tipo n es negativo, los electrones son repelidos desde el terminal negativo de la batería y pasan, sin ningún obstáculo, a la región p, que carece de electrones.

1.5.3 Cajas de Protección

La caja general de protección eléctrica conecta a los clientes a la red de la empresa distribuidora, normalmente en baja tensión. Además de realizar físicamente la conexión, delimita la propiedad y responsabilidad entre la empresa distribuidora y el cliente, y contiene fusibles para evitar que averías en la red del cliente se extiendan a la red de la

distribuidora y, por tanto, que afecten a otros clientes. Estas cajas general de protección son muy importantes, porque por medio de estas se regula la influencia del polvo, agua etc. a los dispositivos electrónicos.

- **Protección IP.-** El Grado de protección IP hace referencia al estándar internacional IEC 60529 Degrees of Protection, utilizado con mucha frecuencia en los datos técnicos de equipamiento eléctrico y/o electrónico. Especifica un efectivo sistema para clasificar los diferentes grados de protección aportados a los mismos por los contenedores que resguardan los componentes que constituyen el equipo. Mediante la asignación de diferentes códigos numéricos, el grado de protección del equipamiento puede ser identificado de manera rápida y con facilidad, cuando un equipamiento tiene como grado de protección las siglas: **IP67** (ROLDAN VILORIA, 2010)

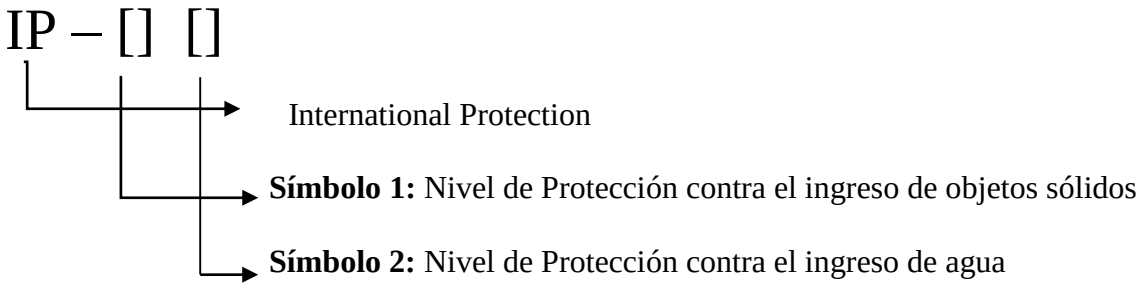
- Las letras **IP** identifican al estándar (una antigua herencia de la terminología International Protection).

- El valor **6** en el primer dígito numérico describe el nivel de protección ante polvo, en este caso: "El polvo no debe entrar bajo ninguna circunstancia"

- El valor **7** en el segundo dígito numérico describe el nivel de protección frente a líquidos (normalmente agua).

Como regla general se puede establecer que cuando mayor es el grado de protección IP, más protegido está el equipamiento.

- **Nomenclatura Estándar IEC 60529**



- **Primer Digito (IP * X)**

Nivel	Tamaño del objeto entrante	Efectivo contra
0	—	Sin protección
1	<50 mm	El elemento que debe utilizarse para la prueba (esfera de 50 mm de diámetro) no debe llegar a entrar por completo.
2	<12.5 mm	El elemento que debe utilizarse para la prueba (esfera de 12,5 mm de diámetro) no debe llegar a entrar por completo.
3	<2.5 mm	El elemento que debe utilizarse para la prueba (esfera de 2,5 mm de diámetro) no debe entrar en lo más mínimo.
4	<1 mm	El elemento que debe utilizarse para la prueba (esfera de 1 mm de diámetro) no debe entrar en lo más mínimo.
5	Protección contra polvo	La entrada de polvo no puede evitarse, pero el mismo no debe entrar en una cantidad tal que interfiera con el correcto funcionamiento del equipamiento.
6	Protección fuerte contra polvo	El polvo no debe entrar bajo ninguna circunstancia

- **Segundo Digito (IP X*)**

Nivel	Protección frente a	Método de prueba	Resultados esperados
0	Sin protección.	Ninguno	El agua entrará en el equipamiento.
1	Goteo de agua	Se coloca el equipamiento en su lugar de trabajo habitual.	No debe entrar el agua cuando se la deja caer, desde 200 mm de altura respecto del equipo, durante 10 minutos (a razón de 3-5 mm3 por minuto)
2	Goteo de agua	Se coloca el equipamiento en su lugar de trabajo habitual.	No debe entrar el agua cuando de la deja caer, durante 10 minutos (a razón de 3-5 mm3 por minuto). Dicha prueba se realizará cuatro veces a razón de una por cada giro de 15º tanto en sentido vertical como horizontal, partiendo cada vez de la posición normal de trabajo.
3	Agua nebulizada. (spray)	Se coloca el equipamiento en su lugar de trabajo habitual.	No debe entrar el agua nebulizada en un ángulo de hasta 60º a derecha e izquierda de la vertical a un promedio de 10 litros por minuto y a una presión de 80-100kN/m2 durante un tiempo que no sea menor a 5 minutos.
4	Chorros de agua	Se coloca el equipamiento en su lugar de trabajo habitual.	No debe entrar el agua arrojada desde cualquier ángulo a un promedio de 10 litros por minuto y a una presión de 80-100kN/m2 durante un tiempo que no sea menor a 5 minutos.

5	Chorros de agua.	Se coloca el equipamiento en su lugar de trabajo habitual.	No debe entrar el agua arrojada a chorro (desde cualquier ángulo) por medio de una boquilla de 6,3 mm de diámetro, a un promedio de 12,5 litros por minuto y a una presión de 30kN/m2 durante un tiempo que no sea menor a 3 minutos y a una distancia no menor de 3 metros.
6	Chorros muy potentes de agua.	Se coloca el equipamiento en su lugar de trabajo habitual.	No debe entrar el agua arrojada a chorros (desde cualquier ángulo) por medio de una boquilla de 12,5 mm de diámetro, a un promedio de 100 litros por minuto y a una presión de 100kN/m2 durante no menos de 3 minutos y a una distancia que no sea menor de 3 metros.
7	Inmersión completa en agua.	El objeto debe soportar sin filtración alguna la inmersión completa a 1 metro durante 30 minutos.	No debe entrar agua.
8	Inmersión completa y continúa en agua.	El equipamiento eléctrico / electrónico debe soportar (sin filtración alguna) la inmersión completa y continua a la profundidad y durante el tiempo que especifique el fabricante del producto con el acuerdo del cliente, pero siempre que resulten condiciones más severas que las especificadas para el valor 7.	No debe entrar agua

1.5.4 Aplicaciones con Microcontroladores

Cada vez existen más productos que incorporan un micro controlador con el fin de aumentar sustancialmente sus prestaciones, reducir su tamaño y coste, mejorar su fiabilidad y disminuir el consumo.

Algunos fabricantes de micro controladores superan el millón de unidades de un modelo determinado producidas en una semana. Este dato puede dar una idea de la masiva utilización de estos componentes.

Los Microcontroladores están siendo empleados en multitud de sistemas presentes en nuestra vida diaria, como pueden ser juguetes, horno microondas, frigoríficos, televisores, ordenadores, impresoras, módems, el sistema de arranque de nuestro coche, etc. Y otras aplicaciones con las que seguramente no estaremos tan familiarizados como instrumentación electrónica, control de sistemas en una nave espacial, etc. Una aplicación típica podría emplear varios micros controladores para controlar pequeñas partes del sistema. Estos pequeños controladores podrían comunicarse entre ellos y con un procesador central, probablemente más potente, para compartir la información y coordinar sus acciones, como, de hecho, ocurre ya habitualmente en cualquier PC.

Los micros controladores se encuentran por todas partes:

- **Sistemas de comunicación:** en grandes automatismos como centrales y en teléfonos fijos, móviles, fax, etc.
- **Electrodomésticos:** lavadoras, hornos, frigoríficos, lavavajillas, batidoras, televisores, vídeos, reproductores DVD, equipos de música, mandos a distancia, consolas, etc.
- **Industria informática:** Se encuentran en casi todos los periféricos; ratones, teclados, impresoras, escáner, etc.
- **Automoción: climatización**, seguridad, ABS, etc.
- **Industria:** Autómatas, control de procesos, etc
- **Sistemas de supervisión, vigilancia y alarma:** ascensores, calefacción, aire acondicionado, alarmas de incendio, robo, etc.

- **Otros:** Instrumentación, electro medicina, tarjetas (smartcard), sistemas de navegación, etc.

La distribución de las ventas según su aplicación es la siguiente:

- Una tercera parte se absorbe en las aplicaciones relacionadas con los ordenadores y sus periféricos.
- La cuarta parte se utiliza en las aplicaciones de consumo (electrodomésticos, juegos, TV, vídeo, etc.)
- El 16% de las ventas mundiales se destinó al área de las comunicaciones.
- Otro 16% fue en aplicaciones industriales.
- El resto de los micro empleado controladores vendidos en el mundo, aproximadamente un 10% fueron adquiridos por las industrias de automoción.

1.6 CPU

CPU, abreviatura de **Central Processing Unit** (unidad de proceso central), se pronuncia como letras separadas. La CPU es el cerebro del ordenador. A veces es referido simplemente como el procesador **o** procesador central, la CPU es donde se producen la mayoría de los cálculos. En términos de potencia del ordenador, la CPU es el elemento más importante de un sistema informático.

1.6.1 Importancia

Nuestra evolución como seres humanos ha hecho que se produzcan muchos cambios y avances con el fin de mejorar cada día más nuestra calidad de vida. Gracias a nuestra búsqueda de satisfacer necesidades, a través del tiempo han aparecido infinidades de productos que nos facilitan la vida y nos permiten agilizar nuestro día a día.

Hemos desarrollado la tecnología y con ella la aparición de un mundo digital donde la computadora tiene un auge que crece de manera impresionante, ya que posee la potencia del manejo automatizado de la información. La razón principal por la que las empresas pierden clientes es la mala atención, o la indiferencia, por parte de cualquiera delos miembros del personal de la empresa, por esa razón los servicios técnicos ya no deben preocuparse sólo por dar una reparación de calidad, sino que, si realmente quieren

retener a sus clientes, deben lograr calidad en la atención a los mismos. Según estudios sobre el tema, un 68% de los clientes perdidos fueron mal atendidos, acarreando malas referencias y mala calidad en atención.

1.6.2 Protección

Las computadoras son dispositivos vulnerables. Son vulnerables al polvo, los golpes, la electricidad estática, el calor y los fluidos. Cuando una computadora se coloca en una Dataflex o Caja de Protección para CPU, la mayoría de las amenazas antes mencionadas desaparecen.

Además, el constante ruido generado por los ventiladores internos de la computadora se reduce significativamente. De este modo, las Protection Cases cumplen con dos propósitos. Crean un entorno más cómodo y seguro para el usuario y la computadora.
Tener una computadora en casa u oficina hoy en día es muy habitual, no hace falta de ningún experto en tecnología para poderla manipular y disfrutar de las maravillas de funcionalidades que esta nos ofrece, por ello; si es necesario seguir directrices para mantener el computador en el mejor estado posible.

El cuidar los equipos de cómputos en especial el CPU es de mucha importancia, porque en él se encuentran la unidad de disco y el chip partes importantes de este, hace que funcione de una manera eficaz optimizando los recursos para el usuario. Hay que tener en cuenta que el CPU es muy sensible ante vulnerabilidades del ambiente y el mal uso que los usuarios le den, provocando que la información se dañe sin poderla recuperar.

1.6.3 Medidas De Seguridad

La seguridad de equipos tecnológicos como el CPU en una organización o en el hogar, es de sumo valor ya que por medio de este se podrá alcanzar los objetivos planteados dentro de ellos dándole una satisfacción al usuario.

Existen organizaciones que no cuentan con una adecuada seguridad para estos CPU, es por ello la incidencia de los robos, en ocasiones la empresa no se hace cargo de estos hurtos si el CPU no es parte de dicha entidad, estableciendo así una inseguridad hacia los usuarios.

La informática cuenta con muchos riesgos, es por eso que se crean técnicas para proteger a los equipos informáticos, estos problemas pueden ser intencionales u ocasionales cuales pueden afectar al funcionamiento del hardware.

Algunos puntos que se debe tomar en cuenta sobre la seguridad de los CPU

- Deben estar en un lugar fresco y con el mueble adecuado para ellos.
- La corriente eléctrica deber ser estable y confiable.
- Debe de estar cubierto con fundas especiales para el cuidado del polvo.
- NO debe de estar en el piso, si no en el mueble donde se encuentran los otros equipos.
- NO se debe consumir alimentos ni bebidas dentro del lugar donde se encuentra el CPU.

1.7 BASES DE DATOS

1.7.1 Definición

Una base de datos (cuya abreviatura es *BD*) es una entidad en la cual se pueden almacenar datos de manera estructurada, con la menor redundancia posible. Diferentes programas y diferentes usuarios deben poder utilizar estos datos. Por lo tanto, el concepto de base de datos generalmente está relacionado con el de red ya que se debe poder compartir esta información. De allí el término **base**.

1.7.2 Sistema de gestor de Base de Datos

Un Sistema Gestor de Bases de Datos (SGBD) o DBMA (DataBase Management System) es una colección de programas cuyo objetivo es servir de interfaz entre la base de datos, el usuario y las aplicaciones. Se compone de un lenguaje de definición de datos, de un lenguaje de manipulación de datos y de un lenguaje de consulta. Un SGBD permite definir los datos a distintos niveles de abstracción y manipular dichos datos, garantizando la seguridad e integridad de los mismos (EZEQUIEL ROZIC, 2008).

Existen diferentes Gestores de Bases de Datos, cada uno se lo aplica de acuerdo a la grandeza de la Base de Datos que se vaya a realizar dentro de la Empresa, dependiendo

de la información requerida por esta; por ejemplo, Oracle, DB2, PostgreSQL, MySQL, MS SQL Server, etc.

1.7.2.1 Característica del Sistema de Gestor de Base de Datos

- **"Abstracción de la información:** Los SGBD ahorran a los usuarios detalles acerca del almacenamiento físico de los datos. Da lo mismo si una base de datos ocupa uno o cientos de archivos, este hecho se hace transparente al usuario. Así, se definen varios niveles de abstracción.

- **Independencia:** La independencia de los datos consiste en la capacidad de modificar el esquema (físico o lógico) de una base de datos sin tener que realizar cambios en las aplicaciones que se sirven de ella.

- **Redundancia mínima:** Un buen diseño de una base de datos logrará evitar la aparición de información repetida o redundante. De entrada, lo ideal es lograr una redundancia nula; no obstante, en algunos casos la complejidad de los cálculos hace necesaria la aparición de redundancias.

- **Consistencia:** En aquellos casos en los que no se ha logrado esta redundancia nula, será necesario vigilar que aquella información que aparece repetida se actualice de forma coherente, es decir, que todos los datos repetidos se actualicen de forma simultánea.

- **Seguridad:** La información almacenada en una base de datos puede llegar a tener un gran valor. Los SGBD deben garantizar que esta información se encuentra con seguridad frente a usuarios malintencionados, que intenten leer información privilegiada; frente a ataques que deseen manipular o destruir la información; o simplemente ante las torpezas de algún usuario autorizado pero despistado. Normalmente, los SGBD disponen de un complejo sistema de permisos a usuarios y grupos de usuarios, que permiten otorgar diversas categorías de permisos.

- **Integridad:** Se trata de adoptar las medidas necesarias para garantizar la validez de los datos almacenados. Es decir, se trata de proteger los datos ante fallos de hardware, datos introducidos por usuarios descuidados, o cualquier otra circunstancia capaz de corromper la información almacenada.

- **Respaldo y recuperación:** Los SGBD deben proporcionar una forma eficiente de realizar copias de respaldo de la información almacenada en ellos, y de restaurar a partir de estas copias los datos que se hayan podido perder.

- **Control de la concurrencia:** En la mayoría de entornos (excepto quizás el doméstico), lo más habitual es que sean muchas las personas que acceden a una base de datos, bien para recuperar información, bien para almacenarla. Y es también frecuente que dichos accesos se realicen de forma simultánea. Así pues, un SGBD debe controlar este acceso concurrente a la información, que podría derivar en inconsistencias".

1.8 SENSORES

1.8.1 Definición

Es un dispositivo diseñado para recibir información de una magnitud del exterior y transformarla en otra magnitud, normalmente eléctrica, que seamos capaces de cuantificar y manipular.

Normalmente estos dispositivos se encuentran realizados mediante la utilización de componentes pasivos (resistencias variables, PTC, NTC, LDR, etc... todos aquellos componentes que varían su magnitud en función de alguna variable), y la utilización de componentes activos (AGUILAR AGUILAR & LEMA LAGOS, 2011).

Un sensor se diferencia de un transductor en que el sensor está siempre en contacto con la variable de instrumentación con lo que puede decirse también que es un dispositivo que aprovecha una de sus propiedades con el fin de adaptar la señal que mide para que la pueda interpretar otro dispositivo. Como por ejemplo el termómetro de mercurio que

aprovecha la propiedad que posee el mercurio de dilatarse o contraerse por la acción de la temperatura (GARCIA RAMIREZ, 2014).

1.8.2 Redes de Sensores

Con sus siglas en Ingles (*sensor network*) es una red de ordenadores de pequeñísimos nodos, equipados con sensores, que colaboran en una tarea común. Las redes de sensores están formadas por un grupo de sensores con ciertas capacidades sensitivas y de comunicación inalámbrica los cuales permiten formar redes ad hoc sin infraestructura física preestablecida ni administración central (CORTI, D'AGOSTINO, MARTINEZ, & BELMONTE , 2011).

Las redes de sensores se determinan por su facilidad de despliegue y por ser auto configurables, pudiendo convertirse en todo momento en emisor, receptor, ofrecer servicios de encaminamiento entre nodos sin visión directa, así como explorar datos referentes a los sensores locales de cada nodo.

1.8.3 Diseño de una Red de Sensores

Una parte muy importante en las redes, es tener en cuenta que en base al tipo de aplicación, el diseño de la red puede variar. Las áreas a considerar para un diseño son:

- **Topología:** La topología es generalmente cambiante para las redes de Sensores Ad hoc. Es decir, los nodos se despliegan de manera aleatoria. Una vez desplegados no se requiere de la intervención humana, haciendo la configuración y el mantenimiento completamente autónomos. En la organización de la topología, cada nodo busca información completa de la red o parte de ella, con el fin de mantener las estructuras de información de la red actualizadas (RAMIREZ, 2012).

- **Ruteo:** La responsabilidad de un protocolo de ruteo es el intercambio de información, encontrando el camino más confiable para alcanzar el destino deseado teniendo en consideración la distancia, el requerimiento mínimo de energía y el tiempo de vida del enlace inalámbrico; búsqueda de la información

en el caso de que la conexión falle; reparación de los enlaces caídos gastando el mínimo de potencia de procesamiento y ancho de banda.

- **Energía:** Un cuello de botella que se tiene en la operación de los nodos sensores es la capacidad de energía. Los sensores tienen una vida intrínsecamente dependiente del tipo de batería que se utiliza. Así mismo, el hardware diseñado para los nodos deberá tener un consumo óptimo de energía como requerimiento primordial.

- **Sincronía:** Los nodos sensores deberán ser capaces de sincronizarse uno con otro de manera completamente distribuida, para que la calendarización del multiplexado en tiempo pueda ser impuesta y ordenada de forma temporal la detección de eventos sin ninguna ambigüedad. Dado que los nodos en una red inalámbrica de sensores operan de forma independiente, sus relojes podrán o no, estar sincronizados.

- **Calidad de Servicio:** La calidad del servicio puede interpretarse en las redes de Sensores por enlace, por flujo de información o por funcionamiento de nodo. En estas redes, tanto la red y como el host pueden tener situaciones que requieren de una buena coordinación. La falta de coordinación central y de un límite de recursos puede desencadenar un problema. El nivel de servicio y sus parámetros están asociados al tipo de aplicación [MAN03]. La comunicación en tiempo real sobre una red de Sensores deberá de ser garantizada a pesar de tener un máximo de retraso, un ancho de banda mínimo y otros parámetros involucrados en la calidad del servicio.

- **Tolerancia a Fallas:** La red debe ser capaz de modificar algún aspecto de ella donde se presente una falla. La falla deberá de ser identificada y resulta en un tiempo promedio. Este rubro es muy importante primordialmente para aplicaciones militares y para aplicaciones civiles donde existe un riesgo de pérdida de vida por falla de un equipo electrónico.

1.8.4 Sistema de monitoreo de sensores

1.8.4.1 Inalámbrico

Una red de sensores inalámbricos (WSN) es una red inalámbrica que consiste en dispositivos distribuidos espaciados autónomos utilizando sensores para monitorear condiciones físicas o ambientales. Un sistema WSN incorpora un Gateway que provee conectividad inalámbrica de regreso al mundo de cables y nodos distribuidos (NATIONAL INSTRUMENTS, 2009).

1.8.4.2 Aplicaciones

Ingenieros han creado aplicaciones WSN para diferentes áreas incluyendo cuidado de la salud, servicios básicos y monitoreo remoto. En el cuidado de la salud, los dispositivos inalámbricos vuelven menos invasivo el monitoreo a pacientes y posible el cuidado de la salud. Para servicios básicos como electricidad, alumbrado público y ayuntamientos de agua, los sensores inalámbricos ofrecen un método de bajo costo para un sistema de recolección de datos saludable que ayuden a reducir el uso de energía y mejor manejo de recursos. El monitoreo remoto cubre un amplio rango de aplicaciones donde los sistemas inalámbricos pueden complementar sistemas de cable reduciendo costos de cableado y permitiendo nuevos tipos de aplicaciones de medición. Aplicaciones de monitoreo remoto incluyen:

- Monitoreo ambiental de aire, agua y suelo
- Monitoreo estructural para edificios y puentes
- Monitoreo industrial de maquinas
- Monitoreo de procesos
- Seguimiento de activos

1.9 DISPOSITIVO USB

1.9.1 Definición

Es un dispositivo de almacenamiento que utiliza una memoria flash para guardar información. Se le conoce también con el nombre de **unidad flash USB**, **lápiz de memoria**, **lápiz USB**, **minidisco duro**, **unidad de memoria**, **llave de memoria**, entre otros. Los primeros modelos requerían de una batería, pero los actuales ya no. Estas memorias son resistentes a los rasguños (externos), al polvo, y algunos hasta al agua, factores que afectaban a las formas previas de almacenamiento portátil, como los disquetes, discos compactos y los DVD (ABAD RODRIGUEZ, RODRIGUEZ VERA, & VILLAVICENCIA , 2006).

1.9.2 Funcionamiento

Trabaja como interfaz para transmisión de datos y distribución de energía, que ha sido introducida en el mercado de PC´s y periféricos para mejorar las lentas interfaces serie (RS-232) y paralelo. Esta interfaz de 4 hilos, 12 Mbps y "plug and play", distribuye 5V para alimentación, transmite datos y está siendo adoptada rápidamente por la industria informática.

Emplea una topología de estrellas apiladas que permite el funcionamiento simultáneo de 127 dispositivos a la vez. En la raíz o vértice de las capas, está el controlador anfitrión o host que controla todo el tráfico que circula por el bus. Esta topología permite a muchos dispositivos conectarse a un único bus lógico sin que los dispositivos que se encuentran más abajo en la pirámide sufran retardo. A diferencia de otras arquitecturas, USB no es un bus de almacenamiento y envío, de forma que no se produce retardo en el envío de un paquete de datos hacia capas inferiores.

1.9.3 Clasificación

- **Baja Velocidad** (1.0): Tasa de transferencia de hasta 1,5Mbps (192 KB/s). Utilizado en mayor medida por los dispositivos de interfaz humana, como los teclados, ratones (mouse) y joysticks.

- **Velocidad completa** (1.1): Tasa de transferencia de hasta 12 Mbps (1'5 MB/s). Ésta fue la más rápida antes de la especificación USB 2.0, y muchos dispositivos fabricados en la actualidad trabajan a esta velocidad. Estos dispositivos dividen el ancho de banda de la conexión USB entre ellos, basados en un algoritmo de búferes FIFO.

- **Alta velocidad** (2.0): Tasa de transferencia de hasta 480 Mbps (60 MB/s). Lo usa por ejemplo la consola portátil de Sony PSP.

- **Súper alta velocidad** (3.0): Nuevo en el mercado (con chipsets que ya lo soportan comercialmente) y con tasa de transferencia de hasta 4.8 Gbps (600 MB/s). Esta especificación fue lanzada a fines de 2009 por Intel. La velocidad del bus es diez veces mayor que la del USB 2.0, debido a la que han incluido 5 conectores extra (conformando un total de 9 cables), desechando el conector de fibra óptica propuesto inicialmente. Es compatible con los estándares anteriores.

1.9.4 Modo de Transferencia

Tras su encendido, el dispositivo anfitrión -el PC- se comunica con todos los dispositivos conectados al bus USB, asignando una dirección única a cada uno de ellos (este proceso recibe el nombre de "enumeración").

Los modos de transferencia disponible en los USB son:

- **La transferencia por interrupciones:** la emplean los dispositivos más lentos, que envían información con poca frecuencia (por ejemplo teclados, ratones, etc.). Cuando se recibe alguna interrupción (es decir, se pulsa una tecla o se mueve el ratón de la PC), se envía esta información al anfitrión.

- **La transferencia por bloques:** se utiliza con dispositivos que mueven grandes paquetes de información en cada transferencia. Un ejemplo son las impresoras, pendrives o placas de red USB.

- **La transferencia asíncrona:** se emplea cuando se requiere un flujo de datos constante y en tiempo real, sin aplicar detección ni corrección de errores. Un ejemplo es el envío de sonido a altavoces USB, una placa digitalizadora o una sintonizadora de TV externa hace uso de este modo de transferencia. Como se puede intuir, el modo isócrono consume un ancho de banda significativo.

1.9.5 Cómo se realiza la transferencia de información

Estos modos de transferencia se llevan a cabo mediante un bus basado en el paso de un testigo (tokens), semejante a otros buses como los de las redes locales en anillo con paso de testigo y las redes FDDI. Para darse una idea, es como un "turno" que se le da a cada dispositivo para hacer su transferencia de información.

1.10 COMUNICACIÓN ENTRE DISPOSITIVOS

Los dispositivos de comunicación son periféricos de entrada y salida, medios necesarios para lograr que los nodos y demás elementos de una red tenga comunicación entre ellos.

1.10.1 Comunicación Serial

La comunicación serial radica en el envío de un bit de información de manera secuencial, esto es, un bit a la vez y a un ritmo acordado entre el emisor y el receptor.

La comunicación serial en computadores ha seguido los estándares definidos en 1969 por el RS - 232 (Recommended Standard 232) que establece niveles de voltaje, velocidad de transmisión de los datos, etc. Por ejemplo, este protocolo establece un nivel de -12v como un uno lógico y un nivel de voltaje de +12v como un cero lógico (por su parte, los Microcontroladores emplean por lo general 5v como un uno lógico y 0v como un cero lógico).

1.10.1.1 Tipos de comunicación en serie

- **Simplex:** En este caso el emisor y el receptor están perfectamente definidos y la comunicación es unidireccional. Este tipo de comunicaciones se emplean, usualmente, en redes de radiodifusión, donde los receptores no necesitan enviar ningún tipo de dato al transmisor (CHAVEZ, 2011).

- **Duplex, Halfduplex O Semi-Duplex:** En este caso ambos extremos del sistema de comunicación cumplen funciones de transmisor y receptor y los datos se desplazan en ambos sentidos pero no de manera simultánea. Este tipo de comunicación se utiliza habitualmente en la interacción entre terminales y una computadora central.

- **Full Duplex:** El sistema es similar al duplex, pero los datos se desplazan en ambos sentidos simultáneamente. Para que sea posible ambos emisores poseen diferentes frecuencias de transmisión o dos caminos de comunicación separados, mientras que la comunicación semi-duplex necesita normalmente uno solo. Para el intercambio de datos entre computadores este tipo de comunicaciones son más eficientes que las transmisiones semi-dúplex.

1.10.2 Comunicación por USB

Es de permitir o facilitar la interacción entre dos o más computadoras, o entre una computadora y otro periférico externo a la computadora. Existen algunos dispositivos de comunicación los cuales son:

- Fax-Módem
- Tarjeta de red
- Concentrador
- Conmutador
- Enrutador
- Tarjeta inalámbrica
- Tarjeta Bluetooth

A continuación se describirá dos de ellos

- **Tarjeta de Red.-** Es un periférico que permite la comunicación con aparatos conectados entre sí y también permite compartir recursos entre dos o más computadoras (discos duros, CD-ROM, impresoras, etc). A las tarjetas de red también se les llama **NIC** (por network interface card; en español "tarjeta de interfaz de red"). Hay diversos tipos de adaptadores en función del tipo de

cableado o arquitectura que se utilice en la red (coaxial fino, coaxial grueso, Token Ring, etc.), pero actualmente el más común es del tipo Ethernet utilizando una interfaz o conector RJ-45

- **Tarjeta Bluetooth.-** Bluetooth es la norma que define un estándar global de comunicación inalámbrica, que posibilita la transmisión de voz y datos entre diferentes equipos mediante un enlace por radiofrecuencia. Los principales objetivos que se pretende conseguir con esta norma son:
  - Facilitar las comunicaciones entre equipos móviles y fijos.
  - Eliminar cables y conectores entre éstos.
  - Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre nuestros equipos personales.

El alcance que logran tener estos dispositivos es de 10 metros. Usan ondas de radio.

1.10.3 Comunicación por Radiofrecuencia

1.10.3.1 Definición

El término radiofrecuencia, también denominado espectro de radiofrecuencia o RF, se aplica a la porción menos energética del espectro electromagnético, situada entre unos 3 kHz y unos 300 GHz. El hercio es la unidad de medida de la frecuencia de las ondas, y corresponde a un ciclo por segundo. Las ondas electromagnéticas de esta región del espectro, se pueden transmitir aplicando la corriente alterna originada en un generador a una antena (CABEZAS MIÑO, 2010).

1.10.3.2 Funcionamiento de la radiofrecuencia

Las ondas de radiofrecuencia (RF) se generan cuando una corriente alterna pasa a través de un conductor, se caracterizan por sus frecuencias y longitudes. La frecuencia se mide en hercios (o ciclos por segundo) y la longitud de onda se mide en metros (o centímetros). Las ondas de radio son ondas electromagnéticas y viajan a la velocidad de la luz en el espacio libre.

Las ondas electromagnéticas se componen de dos diferentes (pero relacionados campos) un campo eléctrico (conocido como el campo “E”), y un campo magnético (conocido como el campo “H”). El campo eléctrico se genera por las diferencias de voltaje. Dado que una señal de radiofrecuencia es una alternancia, el constante cambio de tensión crea un campo eléctrico que aumenta y las disminuye con la frecuencia de la señal de radiofrecuencia. El campo eléctrico irradia desde una zona de mayor tensión a una zona de menor voltaje.

El término «energía» se refiere a la fuerza de la señal de radiofrecuencia. Puede considerarse como la suma de RF que se transmite, o la fuerza de la señal en el receptor. La unidad básica de energía es el watt. Sin embargo, en el mundo de RF, hablamos de poder en términos de milivatios, abreviado como mW. Un mW = .001 Watt.

CAPITULO II

2 DIAGNÓSTICO

El diagnóstico hace referencia al análisis que se realiza para determinar cualquier situación y cuáles son las tendencias. Esta determinación se realiza sobre la base de datos y hechos recogidos y ordenados sistemáticamente mediante las encuestas, entrevistas y observación, basados en el conocimiento de cada técnico, según el área en que el asunto este presente y que permiten juzgar mejor qué es lo que está pasando, y lograr de manera eficiente resolver el problema.

2.1 ANTECEDENTES DIAGNÓSTICO

El diagnóstico se lo realizó en el mes diciembre del 2012 a Enero del 2013 en la ciudad de Esmeraldas, con la información obtenida en la Pontificia Universidad Católica del Ecuador Sede Esmeraldas, gracias al Jefe de Sistemas que con sus conocimientos teóricos y prácticos guio para que siga en marcha el proyecto.

La Encargada del Laboratorio de Computación que contribuyeron con ideas y presentaron sus inquietudes sobre la elaboración del proyecto, este personal es el encargado de solucionar anomalías que se presentan dentro del Laboratorio.

Se tuvo una conversación con el Director de la Escuela de Sistemas para analizar el punto de vista que tiene sobre el proyecto que se está realizando, se cuenta con el debido apoyo para la culminación exitosa de esta.

2.2 OBJETIVOS DIAGNÓSTICO

- Conocer los requerimientos del Jefe del Departamento de Sistemas de la PUCESE para la implementación del dispositivo de seguridad y protección de los equipos en el Laboratorio de Computación de la PUCESE.
- Identificarla ubicación correcta de los dispositivos de seguridad dentro del Laboratorio de Computación de la PUCESE.
- Evaluar el grado de agilidad del encargado del Laboratorio de Computación para el manejo del sistema y los dispositivos.
- Monitorear el funcionamiento del sistema, integrando todos los dispositivos instalados.
- Determinar la factibilidad de Implementar dispositivos de seguridad en el Laboratorio de Computación de la PUCESE.

2.3 VARIABLES DEL DIAGNÓSTICO

2.3.1. Jefe del departamento

Ayudará analizar cuáles serían las condiciones más optimas; Central de monitoreo, requerimientos, cantidad de equipos, fácil uso, dentro del Laboratorio como en el área de Sistemas para la instalación de los dispositivos.

2.3.2. Infraestructura

Ver las condiciones óptimas del Laboratorio y el lugar apropiado para la colocación de los dispositivos, de esto va a depender el buen funcionamiento del sistema y poder tener éxito con el proyecto.

2.3.3. Encargados del Laboratorio

Se necesitara de una capacitación para el manejo del sistema, ya que deberá mantenerse informado con la configuración de los dispositivos de lo que llegue a suceder dentro del laboratorio en caso de alguna anomalía.

2.3.4. Usuarios del Laboratorio

Para determinar la acogida que va a tener el dispositivo al momento de la implementación, con este indicador se notará que tan factible será dicha implementación.

2.3.5. Dispositivos y Central de Monitoreo

De acuerdo al número de máquinas será el número de dispositivos que se instalarán, la central de monitoreo es para ver cualquier anomalías que se presente dentro del laboratorio, esta central se instalará en la maquina principal de este.

2.4. INDICADORES O SUBASPECTOS

2.4.1. Número de equipos dentro del laboratorio de computación

Es importante detallar la cantidad de equipos que se encuentran dentro del laboratorio para así poder determinar a cuantos se les colocará el dispositivo. Como en el Laboratorio los equipos se encuentran en hilera habría posibilidad de colocar un dispositivo por cada hilera ya que por medio de la red se podrá detectar algún fallo.

2.4.2. Número de máquinas más frecuentes a utilizar

Es importante este indicador ya que permitirá saber exactamente cuáles son los equipos a los cuales se les pondrá el dispositivo, esto se lo hallará mediante una entrevista a la encargado del Laboratorio.

2.4.3. Fácil Manejo

El sistema tendrá una fácil interacción con el usuario, permitiendo llevar un control de todo lo sucedido dentro del Laboratorio,

2.5. MATRIZ DIAGNOSTICA

Es una estructura la cual contiene datos con el objetivo de proporcionar información necesaria de la empresa u organización, para determinar las técnicas de investigación que de acuerdo a cada indicador toque recolectar. Es importante recalcar que para algunos indicadores sea necesario utilizar varias técnicas de información.

Tabla 1. Matriz Diagnostica

Objetivos	Variables	Indicadores	Técnicas	Fuente de información
Conocer los requerimientos del Jefe del Departamento de Sistemas de la PUCESE para la implementación del dispositivo de seguridad y protección de los equipos en el Laboratorio de Computación de la PUCESE.	Jefe del Departamento	Grado de satisfacción. Disponibilidad en la manipulación de los equipos.	Entrevista	Jefe del Departamento de Sistemas

Identificar la ubicación correcta de los dispositivos de seguridad dentro del Laboratorio de Computación de la PUCESE.	Infraestructura	Número de equipos y ubicación dentro del laboratorio de computación. Equipos en donde se instalarán los dispositivos	Entrevista Observación Documental	Encargado del laboratorio y Jefe del Departamento de Sistemas
Evaluar el grado de agilidad del encargado del Laboratorio de Computación para el manejo del sistema y los dispositivos.	Encargados del Laboratorio	Fácil manejo. Dispositivos no invasivos. Operar el sistema correctamente.	Observación Entrevista	Encargado del laboratorio

Monitorear el funcionamiento del sistema, integrando todos los dispositivos instalados.	Dispositivos y central de monitoreo.	Estabilidad del sistema. Comunicación entre dispositivos. Configuración de los dispositivos.	Observación Documental	Encargado del laboratorio. Responsable del diseño del Sistema.
Determinar la factibilidad de Implementar dispositivos de seguridad en el Laboratorio de Computación de la PUCESE.	Usuarios del Laboratorio		Encuesta	Docentes de la Universidad

2.6. MECÁNICA OPERATIVA

2.6.1. Población o Universo

Para el desarrollo de esta investigación se ha estimado una población de 126 personas, que están conformadas por; 28 docentes que usan el laboratorio de computación para impartir sus clases, 95 administrativos los cuales son los que tienen un equipo a su disposición, los cuales laboran en la institución quienes son los actores directos para que la investigación pueda tener éxito, 2 Encargadas del Laboratorio de Computación, quienes son las que estarán al tanto del monitoreo del Sistema integrado en el

Laboratorio y el Jefe de Sistemas para dar la autorización que se ejecute el Software en la máquina principal del Laboratorio.

2.6.2. Muestra

La población estimada es de 123, se realizara muestro aleatorio simple sin reposición, para hallar la muestra se aplica la siguiente formula.

$$\boldsymbol{n} = \frac{Z^2 PQN}{Z^2 \mathrm{PQ} + \mathrm{Ne}^2}$$

En donde,

n =	Tamaño de la muestra	
Z=	Nivel de Confiabilidad	1.96
P=	Probabilidad de ocurrencia	0.50
Q=	Probabilidad de no ocurrencia	0.50
N =	Población	123
e =	Error de Muestreo	0,05

$$\boldsymbol{n} = \frac{(1.96)^2 * 0.50 * 0.50 * 123}{(1.96)^2 * 0.50 * 0.50 + 123 * (0.05)^2}$$

$$\boldsymbol{n} = \frac{118.12}{1.26}$$

$$\boldsymbol{n} = 93.74$$

$$\boldsymbol{n} = 93$$

Por lo tanto, la muestra representativa con la que se trabajará es de 93.

Nota: Se realizaron dos muestras debido a que la población que necesitamos son docentes y administrativos sin contar con las 2 encargadas del laboratorio y el Jefe de Sistemas, aplicando el muestreo de aleatorio simple para los Docentes con la población de 28 nos da un tamaño de muestra de 39.

Para los Administrativos con el muestreo de aleatorio simple la población equivalente a 95 nos da como resultado el tamaño de la muestra de 76. En general la muestra representativa entre Docentes y Administrativos es la que se menciona anteriormente.

2.6.3. Información Primaria

2.6.3.1. Observación

Esta técnica facilita apreciar el problema de manera directa y participante con la finalidad de obtener información real y objetiva, porque mediante de esta se detallará la frecuencia con la que los estudiantes acceden al laboratorio y cuáles son las computadoras que más son utilizadas.

2.6.3.2. Encuesta

Serán diseñadas encuestas para ser sometidas al pilotaje con la finalidad de rediseñarlas, para ser aplicada a los docentes que utilizan el laboratorio de computación y administrativos de la Universidad, la información obtenida será tabulada, graficada y analizada (VER ANEXO 1 Y ANEXO 2).

2.6.3.3. Entrevistas

En el desarrollo de la investigación permanente se aplicará entrevistas estructuradas y no estructuradas para recoger información del jefe de Sistema y de la Encargada del Laboratorio.

2.6.3.3.1. Encargada del Laboratorio de Computación

Se realiza la entrevista a la encargada del Laboratorio porque mediante de ella obtendré mejor información requerida para el desarrollo de la investigación. Indicará con exactitud las PC con las que más frecuentan los estudiantes y las anomalías que se presentan dentro del laboratorio (VER ANEXO 4).

2.6.3.3.2. Jefe de Sistemas

Él es el encargado de dar la aceptación para la instalación del software en la PC principal del Laboratorio, y así poder dar el monitoreo correspondiente en las PC q se encuentran los dispositivos (VER ANEXO 3).

2.6.4. Información Secundaria

A través del internet se ha navegado por varias páginas a nivel nacional, que hayan utilizado aplicaciones con Arduino y software libre para tomar ejemplo y acoplar en el sistema que se requiere implementar.
Además se ha revisado proyectos que han sido implementados con este sistema de control de equipos tecnológicos utilizando antenas AM.

2.7. TABULACIÓN Y ANÁLISIS DE LA INFORMACIÓN

2.7.1. Encuesta dirigida al personal docente que da clases en el laboratorio de computación de la PUCESE

Pregunta No.1: ¿Qué dispositivos utiliza para proteger los computadores contra variaciones de voltaje?

Tabla 2. Tabulación pregunta Nº1 para Docente

DISPOSITIVOS	FRECUENCIA	%
Supresor de picos	4	10%
Reguladores	35	90%
Fuentes de alimentación ininterrumpida (UPS)	0	0%
Otro:	0	0%
TOTAL	**39**	**100%**

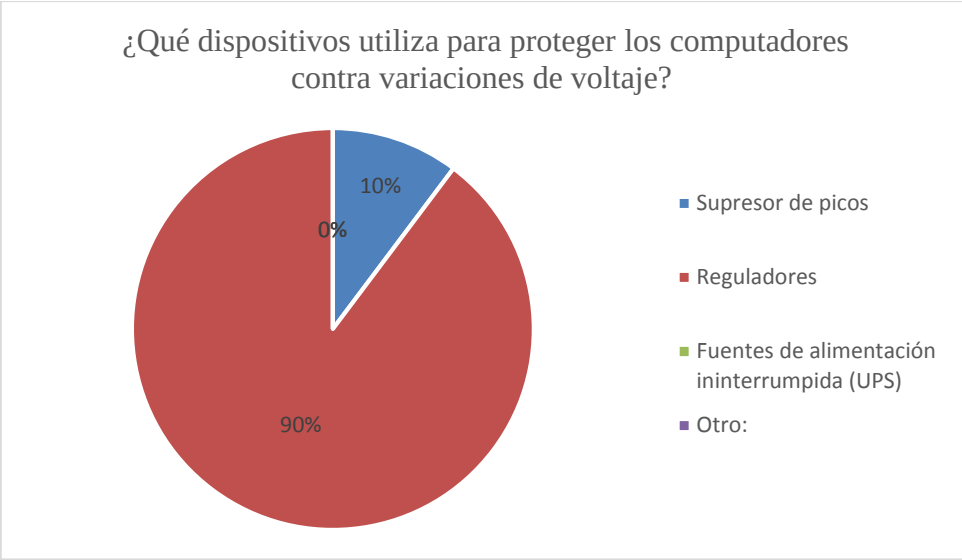


Gráfico 3. Relación pregunta Nº1

Elaborado por: Susana Estupiñán

ANÁLISIS

Como análisis de la información obtenida mediante la encuesta dirigida a los docentes, el 90% usa los reguladores para proteger sus equipos contra variaciones de voltaje y un 10% el supresor de picos, siendo que los UPS u otros no son utilizados.

Pregunta No.2: ¿Conoce usted qué tipos de dispositivos se utilizan para la protección contra robo de equipos informáticos?

Tabla 3. Tabulación pregunta Nº2 para Docente

DISPONIBILIDAD	FRECUENCIA	%
SI	14	36%
NO	25	64%
TOTAL	**39**	**100%**

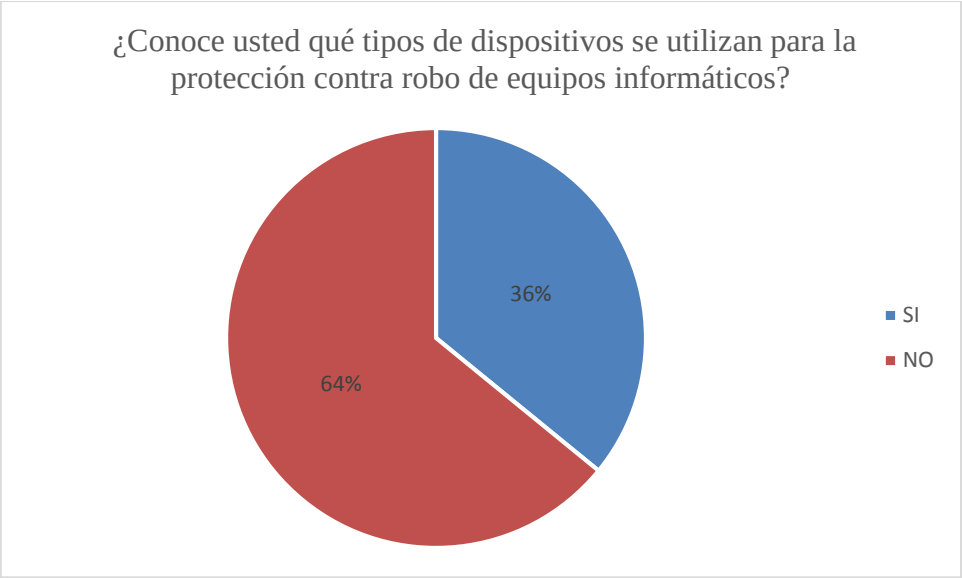


Gráfico 4. Relación pregunta Nº2

Elaborado por: Susana Estupiñán

ANÁLISIS

Existe el 64% los cuales no conocen los tipos de dispositivos para la protección contra robos de equipos informáticos siendo así la mayor necesidad de la instalación de uno de estos equipos. El 36% tienen un conocimiento sobre estos dispositivos, ya que lo han visto en centros comerciales.

Pregunta No.3: ¿Conoce usted si los equipos informáticos de la Universidad cuentan con dispositivos de protección contra robo?

Tabla 4. Tabulación pregunta Nº 3 para Docente

DISPONIBILIDAD	FRECUENCIA	%	
SI	14	36%	
NO	25	64%	
TOTAL	**39**	**100%**	

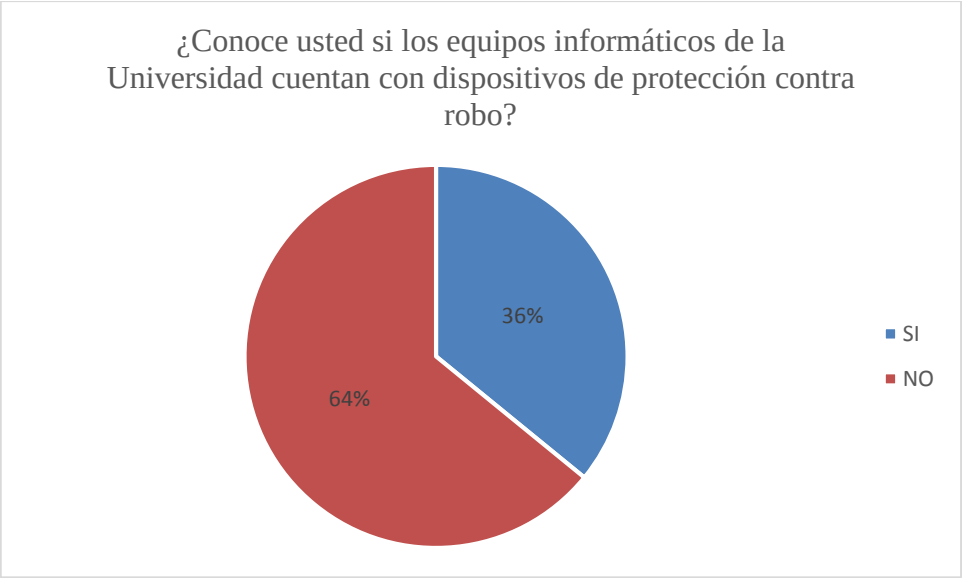


Gráfico 5. Relación pregunta Nº3

Elaborado por: Susana Estupiñán

ANÁLISIS

Los 25 de los 39 docentes respondieron que la Universidad no cuenta con ningún tipo de dispositivos contra robo de equipos informáticos que equivale al 64% manifestando que es de mucha importancia que exista un dispositivo de estos dentro de las instalaciones de la sede tanto en los laboratorio como en la biblioteca que son lugares los cuales cuentan con más influencia de estudiantes y equipos.

Pregunta No.4: ¿Le gustaría que exista un dispositivo que permita controlar la seguridad física de los equipos de computación de su oficina o laboratorio?

Tabla 5. Tabulación Pregunta Nº 4 para Docente

DISPONIBILIDAD	FRECUENCIA	%
SI	36	92%
NO	3	8%
TOTAL	**39**	**100%**

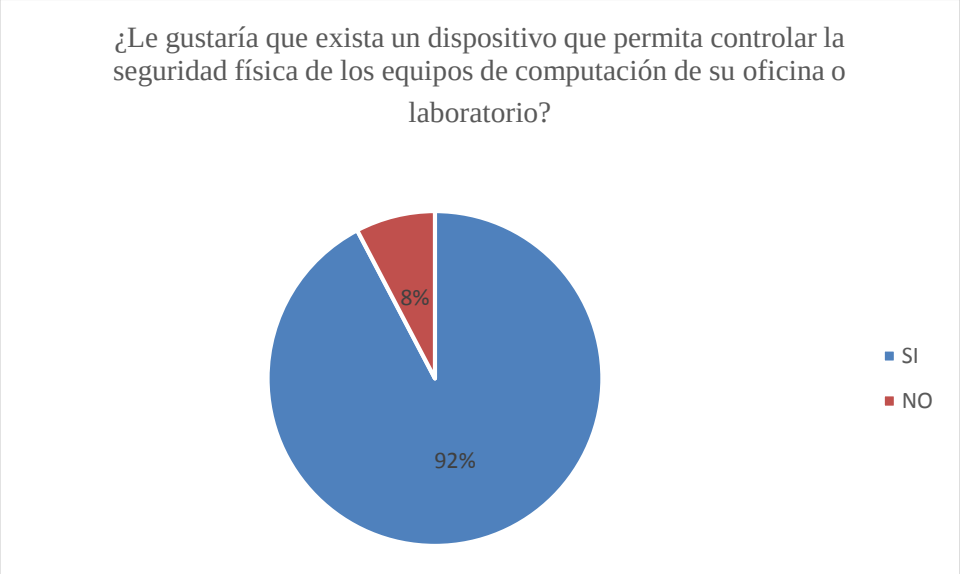


Gráfico 6. Relación pregunta Nº4

Elaborado por: Susana Estupiñán

ANÁLISIS

El grafico nos indica que 36 de los 39 encuestados que equivale al 92% de los docentes requieren de una seguridad física para los equipos informáticos, en su mayoría lo requieren en el laboratorio porque existe perdidas de los componentes que conforman el equipo informático.

Pregunta No.5: ¿Cree usted que la instalación de un moderno dispositivo de protección física de los equipos minimice los robos y pérdidas de los mismos?

Tabla 6. Tabulación pregunta Nº 5 para Docente

DISPONIBILIDAD	FRECUENCIA	%
SI	33	85%
NO	6	15%
TOTAL	**39**	**100%**

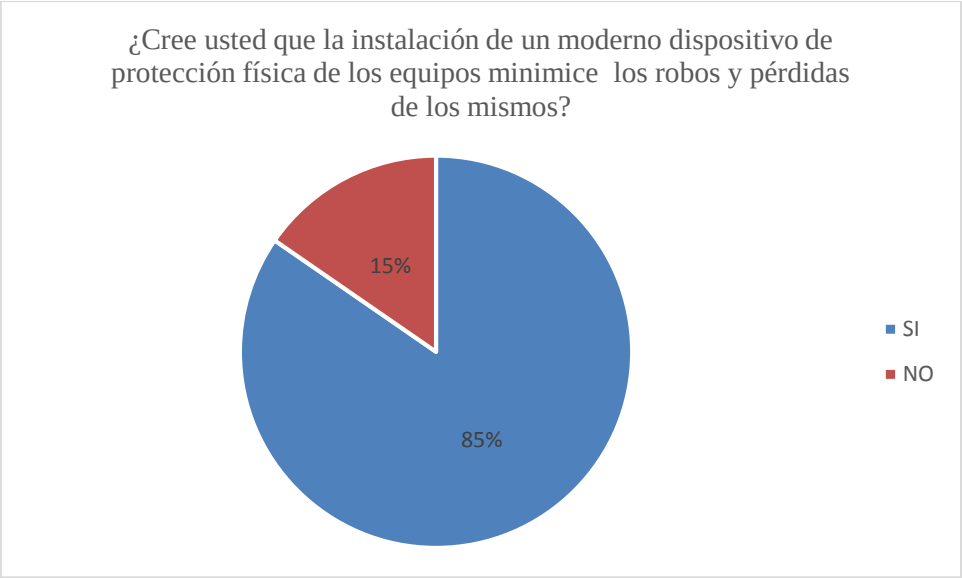


Gráfico 7. Relación pregunta Nº5

Elaborado por: Susana Estupiñán

ANÁLISIS

Como análisis de la pregunta, existe un 85% equivalente a 33 de los 39 docentes encuestados dando como respuesta SI, que es de mucha importancia que la Universidad cuente con unos de estos dispositivos, porque así minimizará la pérdida de los componentes de los equipos, los cuales son muy utilizados dentro del laboratorio, el 15% equivalente a 6 de los 39 docentes encuestados dijeron que NO.

Pregunta No.6: ¿De tener un costo el dispositivo cuanto estaría dispuesto a pagar por su computador?

Tabla 7. Tabulación pregunta Nº 6 para Docente

COSTO	FRECUENCIA	%
$25	22	56%
$50	8	21%
$100	5	13%
$150	2	5%
NINGUNO	2	5%
TOTAL	**39**	**100%**

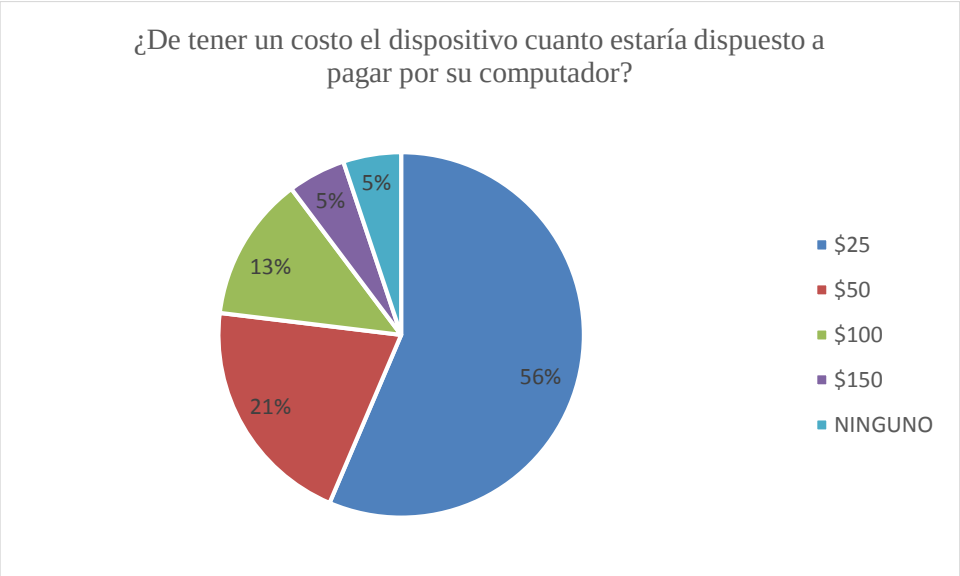


Gráfico 8. Relación pregunta Nº6

Elaborado por: Susana Estupiñán

ANÁLISIS

En esta pregunta solo se ha considerado el dispositivo como tal por computadora, se realizó esta pregunta en el caso de que el dispositivo sea comercializado y ya tener un presupuesto para aquello, dentro de las opciones que se puso, el 56% que equivale a 22 docentes de los 39 encuestados respondieron que está bien que el dispositivo sea vendido a $25 dólares, el 21% que sea vendido a $50 dólares, 13% a $100 dólares y el 5% respondieron que están de acuerdo entre $150 dólares y ningún valor.

2.7.2. Encuesta dirigida al personal administrativo de la PUCESE

Pregunta No.1: ¿Qué dispositivos utiliza para proteger los computadores contra variaciones de voltaje?

Tabla 8. Tabulación pregunta Nº 1 para Administrativo

DISPOSITIVOS	FRECUENCIA	%
Supresor de picos	13	17%
Reguladores	60	79%
Fuentes de alimentación ininterrumpida (UPS)	3	4%
Otro:	0	0%
TOTAL	76	100%

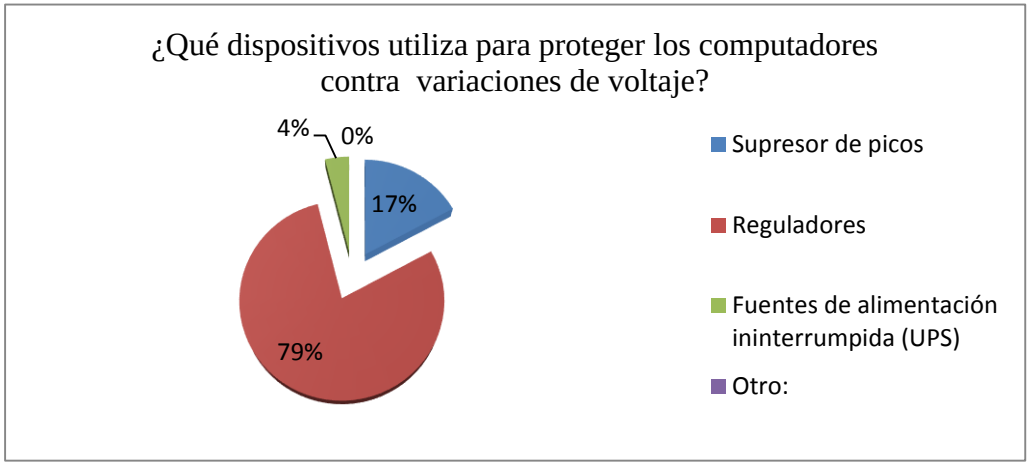


Gráfico 9. Relación pregunta Nº1 Administrativo

Elaborado por: Susana Estupiñán

ANÁLISIS

Como vemos el gráfico No.9 el 79% de los administrativos encuestados utilizan los reguladores como dispositivos para proteger los computadores contra las variaciones de voltaje, mientras que el 17% utiliza el supresor de picos, dando esto un análisis de que si existen personas las cuales tienen conocimiento de los dispositivos utilizan para la protección de sus equipos.

Pregunta No.2: ¿Conoce usted que tipos de dispositivos se utilizan para la protección contra robo de equipos informáticos?

Tabla 9. Tabulación pregunta Nº 2 para Administrativo

DISPONIBILIDAD	FRECUENCIA	%
SI	35	46%
NO	41	54%
TOTAL	76	100%

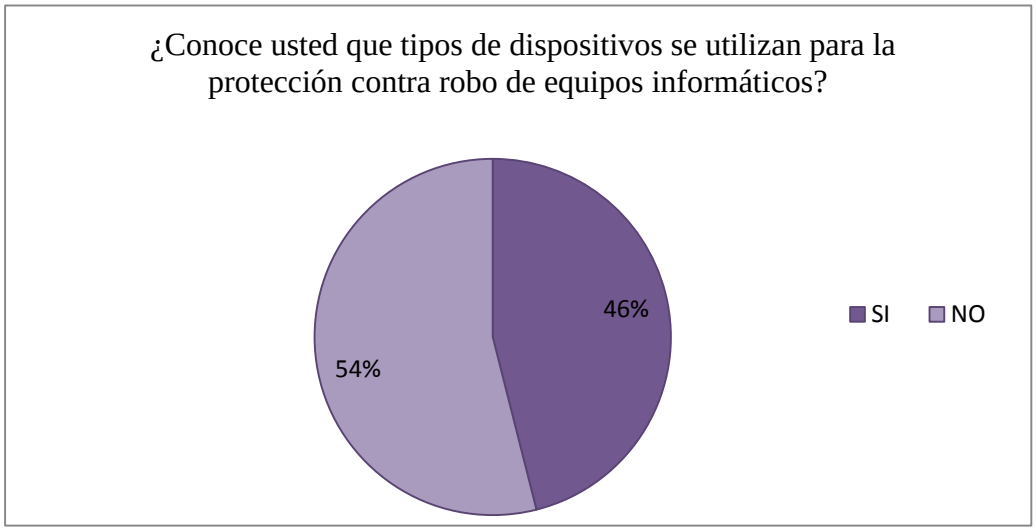


Gráfico 10. Relación pregunta Nº2 Administrativo
Elaborado por: Susana Estupiñán

ANÁLISIS

En el gráfico nos indica que 41 de los 76 encuestados de los administrativos que equivale al 54%, no conocen ningún dispositivo de protección contra robo, lo que conlleva a la implementación y la importancia que tienen estos ante cualquier eventualidad maliciosa.

Pregunta No.3: ¿Conoce usted si los equipos informáticos de la Universidad cuentan con dispositivos de protección contra robo?

Tabla 10. Tabulación pregunta Nº 3 para Administrativo

DISPONIBILIDAD	FRECUENCIA	%
SI	37	49%
NO	39	51%
TOTAL	76	100%

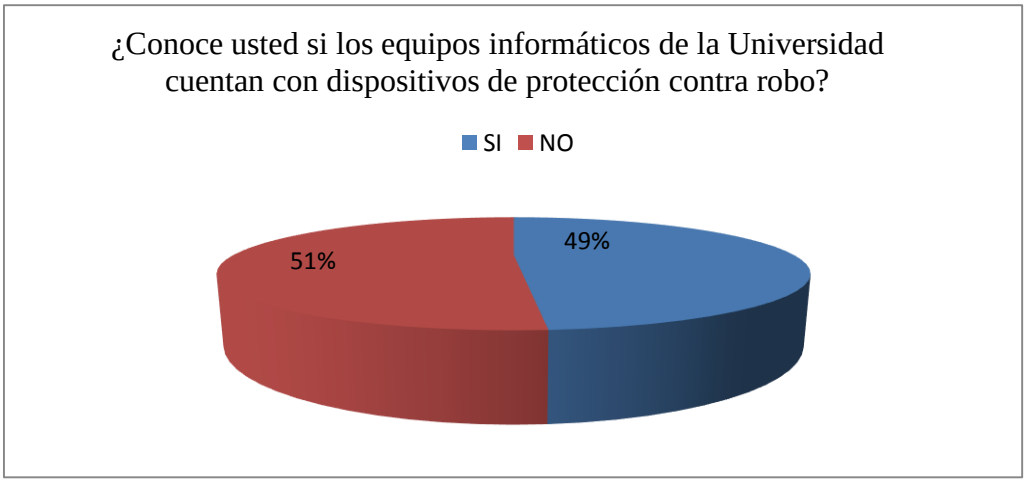


Gráfico 11. Relación pregunta Nº3 Administrativo
Elaborado por: Susana Estupiñán

ANÁLISIS

Como se puede observar en el gráfico No 3. Existe un porcentaje considerable de administrativos que no conocen sobre dispositivos de protección contra roba lo que hace muy necesario la implementación de uno de estos para que tomen conciencia de la importancia que tiene y así evitar pérdidas.

Pregunta No.4: ¿Le gustaría que exista un dispositivo que permita controlar la seguridad física de los equipos de computación de su oficina o laboratorio?

Tabla 11. Tabulación pregunta Nº 4 para Administrativo

PREDISPOSICIÓN	FRECUENCIA	%
SI	62	82%
NO	14	18%
TOTAL	76	100%

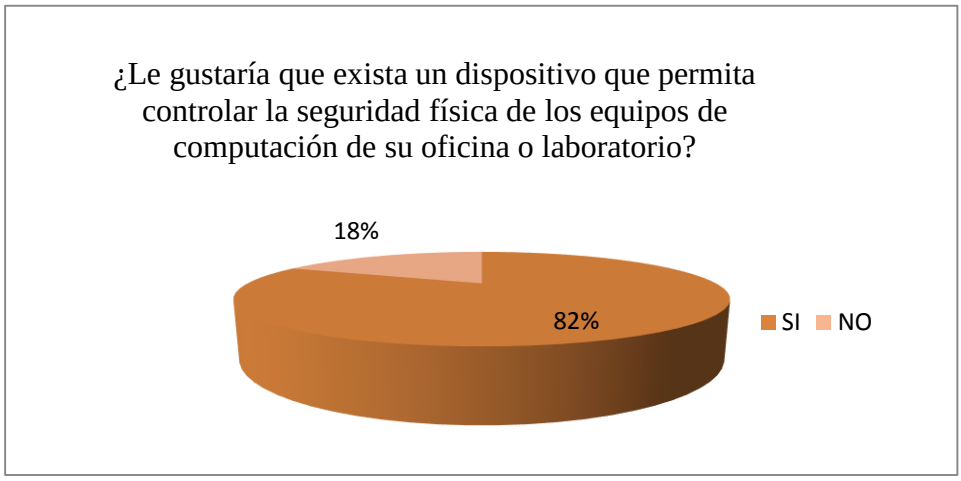


Gráfico 12. Relación pregunta Nº4 Administrativo

Elaborado por: Susana Estupiñán

ANÁLISIS

En el gráfico No 4. Podemos observar que a pesar de que los administrativos no conocen ningún tipo de dispositivos para la protección física de equipos informáticos, el 82% si tienen la predisposición para que esto exista dentro de su oficina o laboratorio y el 18% le dan un desinterés a algo importante dentro de la informática.

Pregunta No.5: ¿Cree usted que la instalación de un moderno dispositivo de protección física de los equipos minimice los robos y pérdidas de los mismos?

Tabla 12. Tabulación pregunta Nº 5 para Administrativo

DISPONIBILIDAD	FRECUENCIA	%
SI	57	75%
NO	19	25%
TOTAL	76	100%

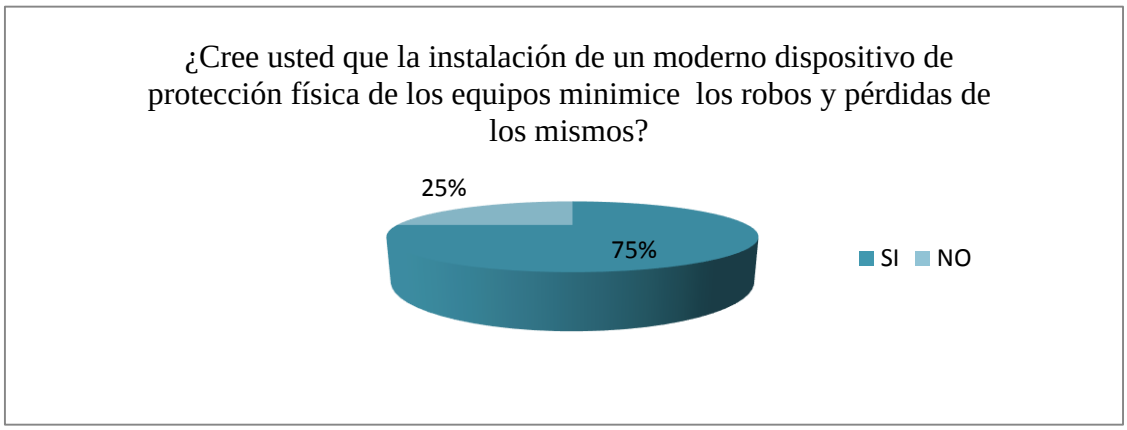


Gráfico 13. Relación pregunta Nº5 Administrativo
Elaborado por: Susana Estupiñán

ANÁLISIS

Como se observa en el grafico No 5. Casi en su totalidad de los administrativos que son el 57 de 76 encuestados con un porcentaje de 75%, están muy de acuerdo con la implementación del dispositivo ya que va a disminuir las incidencias de pérdidas de los equipos así dando seguridad al personal que está encargado de cada equipo.

Pregunta No.6: ¿De tener un costo el dispositivo cuanto estaría dispuesto a pagar por su computador?

Tabla 13. Tabulación pregunta Nº 6 para Administrativo

COSTO	FRECUENCIA	%
$25	31	41%
$50	14	18%
$100	22	29%
$150	5	7%
NINGUNO	4	5%
TOTAL	76	100%

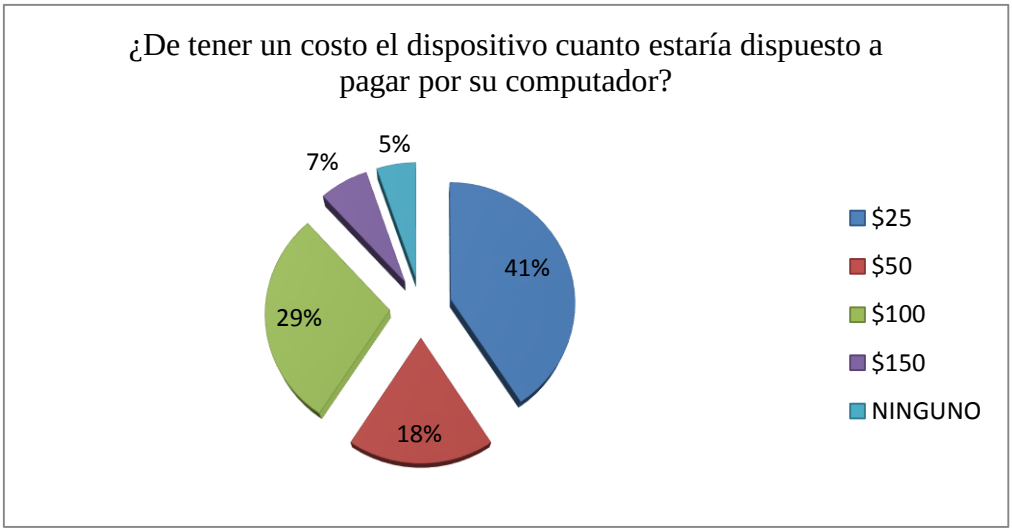


Gráfico 14. Relación pregunta Nº6 Administrativo

Elaborado por: Susana Estupiñán

ANÁLISIS

En el grafico No 6. Podemos observar que el 41% estaría dispuesto a pagar $25.00 por la instalación del dispositivo en el computador, el 29% pagar $100.00 y el 5% no cancelaría nada, esto nos indica que las personas si estarían dispuestas a cancelar entre

$25.00 y $100.00 por la instalación del dispositivo para la protección y seguridad física de los equipos se han estos dentro del lugar del trabajo o en sus hogares.

2.7.3. Análisis de la entrevista a la encargada del laboratorio de computación

Con respecto a la entrevista realizada a la Encargada del Laboratorio de Computación se observó que tiene conocimiento sobre los medios de seguridad física ya que estos son destinados a salvaguardar los laboratorios de cómputo generado por cualquier evento natural o humano que de forma intencional o por accidente puedan afectarlos, supo manifestar el interés en la importancia que tienen los dispositivos de seguridad física porque ayuda a la conservación de los equipos, prevenir daños y el rendimiento de los equipos sea más garantizado y de vida útil más prolongada.

Por otra parte manifestó que estaría de acuerdo con la implementación de algún dispositivo para la seguridad y protección de los equipos, un UPS para cuando no exista energía y entre en funcionamiento, de esta manera, no existirá inconveniente con los equipos, como protección y seguridad al momento de sustraer un equipo.

2.7.4. Análisis de la entrevista al jefe de sistemas

En la entrevista dirigida al Jefe de Sistemas Ing. Klever Posligua, se resume que está muy de acuerdo con implementar un dispositivo para la seguridad de los equipos tecnológicos que se encuentran dentro del laboratorio, ya que ahí solo existe un seguro de los equipos en caso de pérdidas ò en caso de alguna catastro que se presente dentro del laboratorio como incendio.

No cuentan con dispositivo de variaciones de energía, solo están conectados a los reguladores los cuales no son seguros ante alguna variación, esto depende de la vida útil que puedan tener los equipos. Con la implementación del dispositivo los equipos tendrán una vida útil más prolongada de lo establecido.

2.8. FODA

2.8.1. Fortalezas

F1. El uso de Tecnologías existentes en la Pontificia Universidad Católica del Ecuador para el desarrollo proyectos de investigación.

F2. Infraestructura y el equipamiento necesario del Laboratorio de Computación que permite controlar el flujo de personas que ingresan.

F3. El apoyo e interés por parte del jefe de Sistemas para la implementación del proyecto.

F4. Facilidad en el uso del sistema de control y monitoreo de los equipos instalados en las salas del laboratorio.

2.8.2. Debilidades

D1. Poco conocimiento sobre la seguridad física del equipo informático.

D2. La manipulación indebida del software a instalarse.

D3. Perdida de las partes de un computador o equipo.

D4. No existe una persona encargada de la seguridad de los equipos informáticos

2.8.3. Oportunidades

O1. Parámetros de acreditación por parte del SENECYT, con implementación de las TICS teniendo Laboratorios equipados.

O2. Instituciones que necesiten instalar el mismo sistema para la seguridad de sus equipos.

O3. Proyectos de innovación que financien la investigación y desarrollo.

O4. La posibilidad de brindar capacitaciones sobre el uso y manejo del dispositivo de seguridad.

2.8.4. Amenazas

A1. Equipos de similares características ofertados por una empresa, con costos de venta inferiores.

A2. Aparición de nuevos sistemas de seguridad más avanzados con otras mejoras.

A3. Otras Universidades locales que exita el sistema de seguridad de equipos tecnológicos.

A4. Constante variación de La ley Universitaria.

2.9. ESTRATEGIAS FA, FO, DO, DA

Estrategia de Sobrevivencia

- D3 Y A1.- Establecer el mantenimiento preventivo y correctivo en periodos no mayores a tres meses, asegurando de esa forma el óptimo funcionamiento de los equipos tecnológicos.

- D3 Y A2.- Mantener constantemente actualizadas las versiones del software, para que se complemente con el dispositivo y de esa manera garantizar un eficaz sistema de seguridad.

Estrategia Defensiva

- F1 Y A3.- Potencializar el uso de las herramientas tecnológicas implementadas en la Pontifica Universidad Católica del Ecuador para que permitan mediante la investigación desarrollar software que ayude a fortalecer el sistema de seguridad.

- F2 Y A3.- Registrar el acceso de los docentes para utilizar el laboratorio de computación a las horas establecidas, controlando a quien se le ha asignado la responsabilidad.

- F3 Y A2.- Conceder el apoyo incesante en la implementación del proyecto por parte del Departamento de Sistemas, permitiendo que la innovación se realice constantemente en beneficio de los bienes de cómputo de la Universidad.

- F4 y A2.- Administrar el sistema de seguridad mediante la interfaz amigable que ofrece, permite brindar comodidad a la hora de manipular el software.

Estrategia de Orientación

- D1 Y O4.- Celebrar capacitaciones acerca de las medidas de seguridad que se deben tomar para salvaguardar los equipos, dirigidas en especial a los responsables (Departamento de Sistemas) del control y monitoreo del laboratorio.

- D4 Y O3.- Fortalecer las ideas de innovación en el ámbito de desarrollo para atraer inversión que logre financiar los proyectos, de tal manera de incentivar personas a participar y así poder asignar responsabilidades.

Estrategia Ofensiva

- F3 Y O3.- Proporcionar las respectivas facilidades para la realización de mejoras de seguridad en el laboratorio, mediante la revisión de los proyectos propuestos.

- F4 Y O2.- Difundir las bondadosas prestaciones que ofrece la interfaz del sistema de seguridad y motivar a otras instituciones para que se sometan a utilizarlo de una manera segura y confiable.

	AMENAZA	OPORTUNIDADES
FORTALEZA	Diseñar un sistema confiable y sencillo que permita al usuario supervisar y controlar los equipos tecnológicos dentro del laboratorio utilizando la tecnología actual basada en el requerimiento del usuario.	Trabajar en conjunto con el departamento de sistemas para la instalación del software de control, seguridad y protección de las PC, llegando a solucionar algún tipo de problema que llegase a ocurrir, utilizando los recursos destinados a la innovación y desarrollo para su implementación dentro de la institución.
DEBILIDADES	Crear dispositivos de seguridad a bajo costo, instalando el sistema de seguridad en los equipos más vulnerables dentro del laboratorio de computación.	Realizar cursos de capacitación y entrenamiento en el uso de sistemas de seguridad de los equipos tecnológicos aplicando las TICS, para el logro de una Universidad competente llegando a ser reconocida en el País.

2.10. DETERMINACIÓN DEL PROBLEMA DIAGNOSTICO

Analizando cada una de las entrevistas y encuestas las cuales confirman que no se tiene conocimiento sobre el cuidado y seguridad de los equipos informáticos, se ha detectado algunos problemas diagnósticos, los que se producen por algunas causas.

La PUCESE cuenta con seguridad para el Laboratorio a través del monitoreo continuo de cámaras instaladas en ellos, no existe otro dispositivo para evitar la frecuencia de las pérdidas de los componentes que contiene la Computadora, a pesar de esto si requieren del dispositivo de seguridad ya que protege la información que contiene cada uno de esos equipos.

La mayor parte de los encuestados no saben lo que es un dispositivo de seguridad contra robo, han manifestado que en la institución si sería muy necesario ya que controlará la pérdida que se frecuenta dentro de las instalaciones y del laboratorio de computación, lo que conlleva a la implementación y la importancia que tienen estos ante cualquier eventualidad maliciosa.

Para la protección física que los usuarios tienen para el cuidado de sus equipos tecnológicos utilizan en la mayoría el regulador de voltaje, evitando así cualquier variación de voltaje ya que se puede dañar la computadora o perder alguna información que se esté realizando en ese momento, han manifestado que para una mejora ellos requerían de UPS ya que estos tienen un tiempo determinado para que se apaguen y llegar apagar la computadora.

También es de mucha importancia reconocer que no se tiene conocimiento para el cuidado y protección que se les debe dar a estos equipos, dejando a que en una Entidad no se desarrolle en su máximo potencial como se lo debe de hacer.

CAPITULO III:

PROPUESTA: IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA EN EL LABORATORIO DE COMPUTACIÓN DE LA PUCESE

3 ANTECEDENTES

En la actualidad vemos como la tecnología y la seguridad de equipos tecnológicos avanza para las mejoras tanto educativas como a nivel empresarial, por este motivo se propone la implementación de un dispositivo para la protección y seguridad de los equipos en el laboratorio de computación de la PUCESE, monitoreado por una aplicación informática, hoy en día a nivel mundial se encuentra esta tecnología implementada, evitando a que intrusos hurten los equipos tecnológicos dentro de empresas e instituciones.

Anteriormente la seguridad física de los equipos informáticos dentro del laboratorio no era suficiente, aun teniendo las cámaras de seguridad instaladas, han existido inconvenientes con los equipos tecnológicos y los componentes que estos los forman como los mouse que son los más vulnerable. Es importante dar seguridad física a este laboratorio ya que por medio de esta los usuarios que son los estudiantes se sentirán más conformes con la atención que se les brinda.

La falta de interés para proteger los equipos tecnológicos, es motivación principal del proyecto, para que exista una Universidad con infraestructura tecnológica de punta, el cuidar y proteger estos equipos tecnológicos es de mucha importancia.

En la ciudad de Esmeraldas no existe ninguna institución la cual tenga implementado este sistema, seria de mucha importancia y novedad antes otras instituciones locales el ver este sistema implementado en la PUCESE.

La Pontificia Universidad Católica del Ecuador Sede Esmeraldas (PUCESE), siendo una institución formadora de grandes profesionales con excelencia académica y

compromiso humano, lleno de valores cristianos, constantemente está implementando una gran cantidad de recurso que promuevan su misión con los estándares de calidad.
Es por ello, que la PUCESE ve la necesidad de implementar un sistema de seguridad y protección de equipos tecnológicos, con el fin de evitar perdida de estos equipos siendo un déficit para la universidad.

3.1 JUSTIFICACIÓN

La importancia que tiene al realizar este proyecto es que hoy en día la tecnología como la ciencia ha avanzado en toda sus aéreas para mejorar el ámbito educativo e institucional, por aquello, **la creación de un sistema de monitoreo para la protección y seguridad de los CPU en el laboratorio de computación de la PUCESE,** es importante su implementación llegando a cubrir las necesidades requeridas para la mejora del laboratorio.

La creación del sistema seguridad física llevará a los usuarios del laboratorio, al cuidado de los equipos tecnológicos, existen muchos factores que permiten implementar el sistema de monitoreo y protección física de los equipos, obteniendo un control automático en caso de una movilización no autorizada de los equipos informáticos.

El estudio realizado con las encuestas y entrevistas muestra los beneficiarios directos del proyecto, la institución obtendrá calidad en el de servicio de seguridad y la infraestructura tecnológica mejorará.

Es importante implementarlo, otras instituciones académicas y empresas podrán ver como una alternativa de seguridad este sistema. Teniendo así una ciudad con establecimientos educativos modernos e interactivos para una educación de calidad. Este proyecto tiene una importancia Local ya que se implementaría en el laboratorio de computación de la PUCESE.

3.2 OBJETIVOS DE LA PROPUESTA

3.2.1 OBJETIVOS GENERALES

Implementar un sistema de monitoreo que permita la seguridad física y protección de los equipos tecnológicos dentro del Laboratorio de Computación de la PUCESE.

3.2.2 OBJETIVOS ESPECIFICOS

- Determinar los problemas de seguridad física que se presentan en el laboratorio de computación de la PUCESE.

- Construir un dispositivo que permita monitorear y controlar los equipos informáticos dentro del laboratorio de computación.

- Analizar las variables del sistema de monitoreo para lograr la eficacia y eficiencia del dispositivo.

- Evaluar el funcionamiento del sistema de monitoreo, supervisión y accesibilidad de la aplicación.

3.3 SOLUCIÓN INFÓRMATICA

Este sistema de monitoreo de seguridad, contará con un dispositivo electrónico el cual estará colocado en los equipos tecnológicos que cuenta el laboratorio de computación, permitiendo que estos no sean vulnerables a daños o pérdidas.

Se colocará una antena en la puerta principal del laboratorio, esta recibirá la señal proveniente de los dispositivos, alertará a la encargada, en caso de hurto de un equipo tecnológico a parte se instalarán etiquetas magnéticas en todos los dispositivos, el software tendrá el registro de la hora y fecha de las alertas registradas; ya que las cámaras instaladas dentro del laboratorio servirán de apoyo para identificar alguna anomalía dentro del mismo.

En la máquina principal del laboratorio se mostrará un mensaje de alerta cuando sucedan imprevistos con los equipos dentro del área monitoreada por la antena, al momento de que la segunda puerta sea abierta también mandara una señal de alerta indicando lo sucedido.

3.3.1 Requerimientos del sistema

Para la implementación del sistema de monitoreo de seguridad, es importante especificar tanto las características del software y hardware en el cual se va a trabajar, así se detallaran las necesidades para el correcto funcionamiento del mismo, logrando los objetivos establecidos.

3.3.1.1 Software

Las características para el desarrollo del sistema, se centrará en un Sistema Operativo Windows 7 o Windows 8, para la flexibilidad, eficacia y mejor rendimiento de nuestro sistema.

Se determina este Sistema Operativo Windows 7, para el desarrollo del sistema, ya que las aplicaciones que se utilizarán son compatibles con este.

Para un desarrollo de software se debe tomar muy en cuenta todas las necesidades que el usuario requiere, analizar cada detalle para lograrlo. Un desarrollador se centra más en la solución dejando el problema a un lado.

3.3.1.2 Hardware

Como es un sistema pequeño ya que no se necesita de ningún servidor para la funcionalidad, ni es pesado en su capacidad, se ha determinado que las características en donde se lo va a implementar son básicas se requiere de:

- Sistema Operativo Windows 7 32 bit
- Memoria Ram 2 GB
- Procesador Dual Core de 2.00 GHZ

3.4 DESARROLLO

3.4.1 Diseño de Software

3.4.1.1 Java

Java es un lenguaje de programación, que se usa para el desarrollo de aplicaciones como dispositivos móviles, juegos y aparatos de televisión. La importancia que tiene es que su código se lo puede ejecutar en cualquier plataforma no necesita ser recompilado para que se ejecute.

3.4.1.2 Características

- **Lenguaje simple.-** se lo conoce como lenguaje simple porque viene de la misma estructura de C y C++, ya que C++ es un referente para la creación de java por eso utiliza determinadas características de C++ y se han eliminado otras.

- **Orientado a objeto.-** la programación en java en su mayoría está Orientado Objetos porque al estar agrupados en una estructura encapsulada es más fácil su manipulación.

- **Distribuido.-** java se ha diseñado para trabajar en ambiente de redes y contienen una gran biblioteca de clases para la utilización del protocolo TCP/IP, incluyendo HTTP y FTP. El código Java se puede manipular a través de recursos URL con la misma facilidad que C y C++ utilizan recursos locales.

- **Robusto.-** fiable en comparación con C, ya que se han eliminado muchas características con la aritméticas de punteros, proporciona numerosas comprobaciones en compilación y en tiempo real.

- **Portable**.- por ser indiferente a la arquitectura sobre la cual está trabajando, esto hace que su portabilidad sea muy eficiente y sus programas son compatible con todas las plataformas.

3.4.2 Sqlite

Es un sistema de gestión de base de datos relacional pequeña la cual es rápida y portable, a diferencia de los sistemas de gestión de base de datos **cliente – servidor**, el motor SQLITE es un proceso independiente con el programa principal, se comunica a través de llamadas o funciones, estas son guardadas como un solo fichero estándar en la máquina host.

3.4.2.1 Estructura de la base de datos

Se ilustra el modelo de la base de datos que es pequeña porque contiene dos tablas con sus respectivos atributos. La de Registro se necesita almacenar los sucesos ocurridos dentro del laboratorio de computación como se presenta en la (fig 15).

La tabla Usuario es requerida para la administración de la aplicación permitiendo crear nuevos usuarios para su respetivo acceso, como se muestra en la (fig 16).

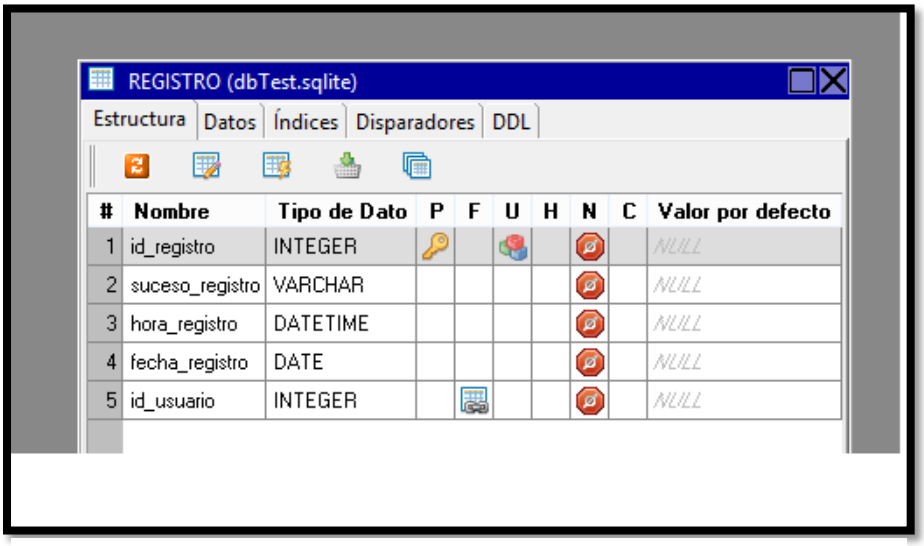


Gráfico 15. Tabla de Registro

Elaborado por: Susana Estupiñán

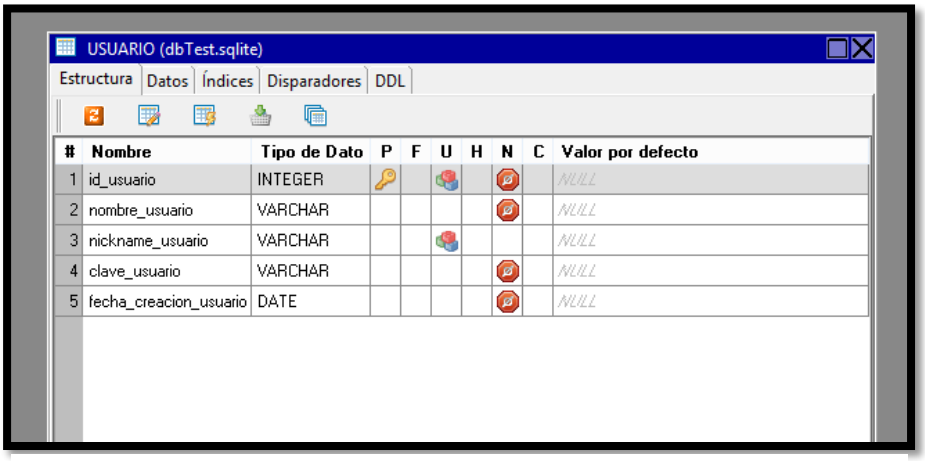


Gráfico 16. Tabla Usuario

Elaborado por: Susana Estupiñán

3.4.2.2 Código SQL

TABLA USUARIO

```
CREATE TABLE USUARIO (
   id_usuario            INTEGER PRIMARY KEY AUTOINCREMENT
                          NOT NULL
                          UNIQUE,
   nombre_usuario        VARCHAR NOT NULL,
   nickname_usuario      VARCHAR UNIQUE,
   clave_usuario         VARCHAR NOT NULL,
   fecha_creacion_usuario DATE    NOT NULL
);
```

TABLA REGISTRO

```
CREATE TABLE REGISTRO (
   id_registro     INTEGER  PRIMARY KEY AUTOINCREMENT
                    NOT NULL
```

```
                    UNIQUE,
  suceso_registro VARCHAR  NOT NULL,
  hora_registro   DATETIME NOT NULL,
  fecha_registro  DATE     NOT NULL,
  id_usuario      INTEGER  NOT NULL
                    REFERENCES USUARIO ( id_usuario )
);
```

3.4.3 Diseño de hardware

Una vez desarrollado cada una de las interfaces en la parte del Diseño de Software, esta etapa consta de la parte física, la cual es el complemento para que se dé el correcto funcionamiento del sistema. Existen algunos hardware que se utilizaron los cuales fueron programados.

Existen 3 tipos de Antenas Anti hurto, las cuales son; Tecnología AM 58 Khz. (Acustomagnético), Tecnología RF 8,2 MHz (Radiofrecuencia) y Tecnología EM (Electromagnético) cada una con sus características y usos para diferentes áreas.

La área de trabajo del proyecto es pequeña y no existen materiales metálicos es por aquello que se utiliza la tecnología AM 58 Khz. (Acustomagnético) la cual es la más apropiada para el sistema de control de los equipos tecnológicos que se encuentran en el laboratorio de computación.

3.4.3.1 Antena Acústica Magnética

Es un sistema de seguridad anti hurto la cual permite el control de los equipos tecnológicos que se encuentran dentro del laboratorio de computación, funciona con una tecnología más eficaz en la protección electrónica una de ellas es la AM 58 KHz (ACUSTICO MAGNETICO). Esta tecnología se caracteriza por dar un elevado rendimiento al sistema y gran capacidad de detección.

Son más requeridas en lugares los cuales no son muy grandes porque solo se maneja a una frecuencia de 58 KHz, La antena Transmisora genera ondas que son captadas por la antena Emisora al momento de que se detecte una etiqueta.
Como existen dos antenas solo se configura una que es la madre de la otra antena, el sistema que se usa para esta antena es el Sistema Dual, una antena es emisora y la otra es receptora, la distancia que llegan a cubrir es hasta 2 metros.

De acuerdo a las características del espacio a cubrir por las antenas se define el tipo de las etiquetas más apropiado a utilizarse.

3.4.3.2 Etiquetas Adhesivas DR Código de Barras

Se define el uso de esta etiqueta porque es la apropiada para la antena AM que se utiliza, trabaja con una frecuencia de 58 kHz, para la colocación de estas etiquetas en los equipos informáticos del laboratorio hay que tener mucho cuidado al momento de retirar el adhesivo, porque se puede dañar el campo magnético el cual tiene el código de barras y al momento que el equipo informático salga del laboratorio no se podrá activar la alarma de incidencia, por lo tanto en la base de registro no contará con aquello.

Para la seguridad y el buen funcionamiento de las etiquetas están deben de ser no visible, son más utilizadas en artículo de dimensiones pequeñas.



Gráfico 17. Etiquetas DR

3.4.3.3 Dispositivos adicionales

Para un mejor funcionamiento de la Antena se adquirieron dispositivos los cuales hace que la antena en si tenga un funcionamiento diferente al que se la adquirió, por ello es

muy importante en aplicaciones informáticas realizar innovación en productos nuevos, para un mejor desarrollo y éxito en el sistema a utilizarse.

La innovación tecnológica es dar un agregado al producto nuevo el cual sea vendible conformando productos, procesos y servicios, una vez que sea lanzado al mercado y este en producción se denomina Innovación.

3.4.3.3.1 Bluetooth

Es el que permite la comunicación entre el hardware y el software, cuando se ha realizado una llamada para hacer la acción que se especifica en el software desarrollado, este módulo de bluetooth es el JY-MCU específico para Arduino el cual está configurado en la antena emisora, que luego envía una señal al software para que este sea activado.

En el software recepta la cadena de trama que le han enviado para que este lo pueda procesar y por medio del Arduino Uno con la comunicación de Java puede ser mostrado en pantalla.

3.4.3.3.2 Modificación de las antenas

Para realizar el proceso de configuración de las Antenas, se realizaron varios pasos, al momento de abrir la antena hay que tener muy en cuenta donde se encuentra la fuente de energía y los pines para el encendido del LED, cuando ya se encuentra identificada las dos partes, en la que se encuentra el ping del Led, procedemos a conectar el protoboard que ya está configurado para comprobar si es el indicado de que nos dé señal de encendido del Led (VER ANEXO 5, FIG 1).

Al momento de realizar la conexión al interruptor la fuente de energía que trae la antena es de 220 V lo que es necesario conectar a un convertidor de energía para que la transforme a 110 V y su funcionamiento sea exitoso.

3.4.3.3.3 Modulo Emisor para Antena

La utilización del Arduino Uno es por la facilidad del código abierto y la portabilidad que usa, llegando a ser la última versión de la placa. Es el más utilizado en los proyectos por sus características que poseen.

El Arduino uno se encuentra programado que al momento que reciba una trama la cual este especificada, este la procese y la envié por el bluetooth hacía el Arduino uno que se encuentra como master receptando las señales en el software.

A parte del Arduino uno existe el Bluetooth JY-MCU que permite la comunicación con el Arduino uno para que sea enviado al Bluetooth receptor.

3.4.3.3.4 Modulo Receptor para PC

Se utilizó dos de estos Arduino Uno, porque sirve de entrada y salida al momento de realizar la llamada entre la antena y el computador donde se encuentra conectado el Arduino Uno que hace como receptor.

El proceso que realiza en este lado el Arduino uno es recibir la trama, lee lo enviado y si es correcto procesa la información y por medio del principal canal de comunicación que es el puerto serial lo muestra en pantalla.

3.4.3.3.5 Sensor magnético de puertas

Este sensor se lo colocará en la segunda puerta del laboratorio de computación, existen diversos tipo de sensores cada uno con características especiales y únicas de acuerdo a las necesidades del sistema, el sensor a utilizarse para esta aplicación es el magnético, para la apertura de la puerta mencionada sin previo aviso, se activará una alarma mandando un mensaje al sistema que dicha puerta está haciendo forzada o abierta.

Con este sensor se logrará una mayor seguridad del laboratorio de computación, puesto que la puerta se encuentra en un ambiente diferente a la puerta principal, el cual no es muy frecuente la entrada y salida de personal.

3.4.4 Instalación y Verificación del Sistema

Para realizar el proceso de la instalación de las antenas Acustomagnético se necesita inspeccionar el aérea en el cual van a ser instaladas con un mínimo espacio para colocarlas, si es posible se dejará un espacio entre 5 y 10 cm entre la pared o puerta de salida y el límite exterior de cada una de las antenas.

3.4.5 Instalación de las Antenas Modificadas

Es muy importante observar los alrededores en donde se instalará la antena, porque si existe focos con luces de neón que trabaja a una frecuencia entre 50 y 60 kHz pueden interferir en el funcionamiento del sistema, Una vez ya definido el lugar en la cual se colocará la antena procedemos a realizar los agujeros en el suelo de forma que cada antena quede fijada por los dos extremos.

La Antena TX se colocará más cerca de la fuente de alimentación, estas dos antenas siempre deben estar enfrentadas para que al momento de que exista una anomalía estas puedan activarse.

3.4.6 Instalación de las Etiquetas DR

Para realizar el proceso de etiquetar los equipos tecnológicos se debe tener presente que para un correcto funcionamiento deben estar no visible, y al momento de colocar la etiqueta en cada uno de los equipos hay que tener cuidado el no tocar el campo magnético de la barra de código porque al momento que esta sea pasada por las antenas no emanará ninguna señal de incidencia.

Hay que tener muy en cuenta no tener productos etiquetados a una distancia mínima de 1,5 metros de las antenas, porque se produce una activación innecesaria de alarma.

3.5 MANUAL DE USUARIO

Esta etapa consta del funcionamiento del dispositivo con cada una de sus interfaces amigables que el software tiene y de su estructura, se lo ha diseñado con el propósito de satisfacer las necesidades del cliente llevando un control como es la seguridad de los equipos informáticos del laboratorio de computación.

3.5.1 Interface de bienvenida

Al momento de ejecutar la aplicación saldrá una interfaz la cual se encuentra con tres botones los cuales son: Información, Iniciar y Salir cada uno de ellos con sus respectivas opciones.



Gráfico 18. Panta de Inicio

Información, Es la que consta los datos personales del desarrollador de la aplicación.



Gráfico 19. Información del Desarrollador

Iniciar, Es en esta interfaz es donde se verá cada movimiento que se realice dentro del laboratorio, que detallara al instante los sucesos mostrando mensajes de alerta, dentro de aquella existen tres menú, pues he aquí donde se encuentra el sistema de control de los equipos informáticos del laboratorio.



Gráfico 20. Detalle de los incidentes

3.5.2 Interfaz de configuración

Con esta interfaz sirve para que al momento de conectar el Arduino a la PC automáticamente le genera un puerto por el cual va a salir y recibir la información para mostrarlo en el sistema, siempre será el mismo puerto así sea conectado en otra pc, esto sucederá cuando la opción de inicio automático se encuentre activado. En caso de que no se encuentre activado buscara un puerto libre y lo asigna al Arduino.

Se recomienda que se encuentre activada la opción de inicio automático porque genera una mayor seguridad y así la persona encargada no tiene que estar haciendo la configuración respectiva.



Gráfico 21. Pantalla de Configuración

3.5.3 Interfaz de registro

Esta interfaz es la que genera los reportes de los incidentes que se ocasionan dentro del laboratorio, se realiza una búsqueda por fecha.

Se registra cada uno de los incidentes detallado indicando el número de puerta, la fecha y hora en que se está realizando el suceso.



Gráfico 22. Resumen de los sucesos

3.5.4 Interfaz Arduino

Se almacenan todos los puertos COM en donde se conecta el Arduino en la PC, la maquina automáticamente genere un IDE que es con el que se enlaza en el Arduino uno para que realice la operación correcta. Si al momento de haber realizado la configuración no se definió que se por defecto, entonces se tendría que colocar el puerto COM que la computadora en eso momento le asigno al dispositivo, para ver esto hay que dirigirse a la administración de dispositivos y seleccionar puertos COM ahí aparecerá el que se ha asignado.



Gráfico 23. Puertos COM

CAPITULO IV

Análisis de Impacto

4 ANTECEDENTES

Una vez que se ha desarrollado el sistema de seguridad de los equipos tecnológicos del laboratorio de computación de la PUCESE, se han establecidos varias aéreas de análisis y se han determinado impactos tanto positivo como negativos.

Se consideran varios ámbitos institucional, social, económico y tecnológico, los mismos que se detallaran con sus análisis respectivos para una mejor interpretación; en la siguiente matriz de impactos a continuación:

a) Los niveles de Impacto se clasifican numéricamente en la siguiente tabla:

IMPACTO NÙMERICO	DESCRIPCIÓN
-3	Impacto alto negativo
-2	Impacto medio negativo
-1	Impacto bajo negativo
0	No hay Impacto
1	Impacto bajo positivo
2	Impacto medio positivo
3	Impacto alto positivo

b) Para cada área o aspecto se determinaron indicadores de impactos en la respectiva matriz.
c) A cada indicador se le asigna un valor numérico de nivel del impacto en la respectiva matriz.

d) Se realizó una sumatoria de los niveles de impacto y se obtuvo el promedio de aéreas o ámbito.
e) Se detalla el análisis y argumento de las razones y circunstancias las cuales se les denomino el valor numérico a cada indicador.

4.1 Impacto Institucional

IMPACTO INSTITUCIONAL							
Nivel de impactos **Indicadores**	**-3**	**-2**	**-1**	**0**	**1**	**2**	**3**
Prevenir la pérdida de los equipos tecnológicos						x	
Control e inventario de los recursos disponibles dentro del laboratorio							x
Gestión de la seguridad del laboratorio							x
TOTAL						2	6

$\sum = 8$

Nivel de Impacto Institucional = $\sum$ / Numero de Indicadores

$$NI = 8/3$$

$$NI = 2{,}66$$

Nivel de Impacto Institucional = Alto positivo

- ***Medio positivo***, por medio del dispositivo puesto en cada equipo tecnológico las pérdidas de estos serán mínimas e incluso pueden ya no haber.

- Se tendrá un control de los equipos tecnológicos que se encuentran en el laboratorio y esto generará un impacto ***alto positivo*** permitiendo que se tenga el índice exacto de los recursos que se encuentran ahí.

- Por medio de la instalación del sistema de seguridad del laboratorio existirá la necesidad o requerimientos de que sean implementados en otras áreas dentro de la institución por lo cual considero un impacto ***alto positivo***.

4.2 Impacto Social

IMPACTO SOCIAL							
Nivel de impactos **Indicadores**	**-3**	**-2**	**-1**	**0**	**1**	**2**	**3**
El manejo adecuado de los recursos tecnológicos							X
Crear conciencia en uso y cuidado de los equipos tecnológicos						X	
Nivel de aceptación de la comunidad universitaria en proyectos innovadores							X
TOTAL						2	6

$\sum = 8$

Nivel de Impacto Económico = $\sum$ / Numero de Indicadores

$$NI = 8/3$$

$$NI = 2{,}66$$

Nivel de Impacto Económico = Alto Positivo

Análisis

- ***Alto positivo***, mediante la utilización de nuevas herramientas tecnológicas y de manejo sencillo, el sistema dependerá de una persona en específico para su correcto funcionamiento.

- Es de suma importancia dar un el cuidado correcto a los equipos destinados para la enseñanza y aprendizaje de calidad, dentro de la institución se debe tomar conciencia en el uso adecuado de estos dispositivos. Se consideró este indicador como ***medio positivo***.

- Dentro de la institución se han generado muchos proyectos innovadores, los cuales han fortalecido la excelencia universitaria a través de proyectos de investigación y desarrollo tecnológico, se lo considera como ***alto positivo***

4.3 Impacto Económico

IMPACTO ECONÓMICO							
Nivel de impactos **Indicadores**	**-3**	**-2**	**-1**	**0**	**1**	**2**	**3**
Utilización de software con licencia gratuita							X
El dispositivo se puede implementar a bajo costo dentro la institución				X			
Oportunidades para la implementación del sistema en otros establecimientos con similares requerimientos							X
TOTAL				0			6

$\sum = 6$

Nivel de Impacto Económico = $\sum$ / Numero de Indicadores

$$NI = 6/3$$

$$NI = 2$$

Nivel de Impacto Económico = Medio Positivo

Análisis

- Al utilizar software libre se tiene una reducción de los costos ya que el uso de este tipo de programas no implica la compras de licencias, se defino al indicador como ***alto positivo.***

- Este indicador no presenta impacto porque la PUCESE mediante sus proyectos que realizan los estudiantes no tendrá que adquirir software los cuales sean pagados con características similares.

- Alto positivo, mediante esta implementación se dará a conocer el dispositivo, por la utilidad y seguridad que brindará a los equipos tecnológicos, llevando a las instituciones locales a adquirirlo.

4.4 Impacto Tecnológico

IMPACTO TECNOLÓGICO							
Nivel de impactos **Indicadores**	**-3**	**-2**	**-1**	**0**	**1**	**2**	**3**
Uso de nuevas herramientas tecnológicas de hardware y software							X
Innovación de tecnología e integración de dispositivos							X
Desarrollo de aplicaciones en software libre							X
TOTAL							9

$\sum = 9$

Nivel de Impacto Tecnológico = $\sum$ / Numero de Indicadores

$$NI = 9/3$$

$$NI = 3$$

Nivel de Impacto Tecnológico = Alto positivo

- Las herramientas tecnológicas con el tiempo evolucionan permanentemente llegando a la aplicación de nuevas herramientas para el desarrollo del hardware y software, este indicador se ha considerado ***alto positivo***.

- En la actualidad se necesitan dispositivos creados para la solución de un problema específico en áreas determinadas, en este caso la seguridad y monitoreo, es por aquello que considero ***alto positivo***.

- Considero como ***alto positivo*** a este proyecto porque por medio de la implementación del desarrollo de software libre hará que se tenga una adecuada administración y control de los equipos tecnológicos a bajo costo.

4.5 Matriz General

IMPACTO GENERAL							
Nivel de impactos **Indicadores**	**-3**	**-2**	**-1**	**0**	**1**	**2**	**3**
Impacto Institucional							X
Impacto Social							X
Impacto Económico						X	
Impacto Tecnológico							X
TOTAL						2	9

$\sum = 11$

Nivel de Impacto Tecnológico = $\sum$ / Numero de Indicadores

$$NI = 11/4$$

$$NI = 2{,}75$$

Nivel de Impacto Tecnológico = Alto positivo

Análisis

- La implementación de este proyecto en todos sus impactos como lo son; Institucional, Social, Económico y Tecnológico presenta un ***Alto Positivo*** generando su ejecución y puesto en marcha del proyecto con importantes beneficios para la institución y el bienestar estudiantil.

- El proyecto genera pocos gastos económicos para su implementación, no será necesario realizar adquisición de equipos de computación, pago de licencias por el software a utilizar; ni contratar de forma permanente a una persona para que maneje el sistema, Por lo tanto *no genera impacto* pero si un ahorro significativo para la PUCESE en la implementación de este tipo de sistemas.

- En el Impacto Tecnológico del proyecto es Alto Positivo, se presentará una visión innovadora dentro del laboratorio de computación la cual permitirá un mejor control de los equipos tecnológicos que cuenta dicho laboratorio.

CAPITULO V

5 CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- El desarrollo de la Implementación de la seguridad electrónica que permite el control de los equipos tecnológicos es un gran aporte para la PUCESE ya que no cuentan con este tipo de tecnología que ayuden a la protección de estos equipos.

- La principal ventaja de este proyecto es su implementación no genera mucho gasto económico en lo referente al software debido a la plataforma en que fue desarrollada son de libre distribución.

- La aplicación es muy liviana y portable porque trabaja con software libre y se acopla a cualquier sistema operativo.

- Es un sistema innovador, empresas pueden adquirirlo porque controla los equipos, herramientas de trabajo y pequeños dispositivos, ante algún hurto dentro de una institución o negocio.

- Es una aplicación cuya interfaz es sencilla e intuitiva, que permite un fácil manejo al usuario y acceso al sistema.

- Los tiempos de respuestas son precisos ante algún hurto o salida de algún equipo sin previo aviso, los genera en momentos reales.

5.2 RECOMENDACIONES

En esta etapa es importante resaltar que se realizó un listado de especificaciones las cuales servirán para dar soluciones oportunas en caso de un mal manejo del sistema.

- El uso del software libre es importante dentro de cualquier aplicación, porque no tiene ningún costo de adquisición y tiene las mismas funcionalidades que otro comercial.

- Una vez implementado el sistema de seguridad electrónica en el laboratorio de la PUCESE, en caso mantenimiento, debe ser manipulado por personal con conocimiento de la plataforma en la cual se ha desarrollado, se adjunta manual de funcionamiento.

- En caso de un cambio de la encargada del laboratorio realizar la respectiva capacitación para que lleve un control de las incidencias presentadas durante el día o semana.

- Tener mucha conciencia del cuidado de estos equipos tecnológicos, porque contiene información importante y son parte de la comunidad universitaria para una mejor oferta académica.

- Instalar una nueva antena para controlar los equipos desde la puerta auxiliar del laboratorio de computación, el sistema tiene habilitado puertos adicionales para instalar dispositivos externos.

6 BIBLIOGRAFIA

ABAD RODRIGUEZ, W., RODRIGUEZ VERA, C., & VILLAVICENCIA , H. (15 de JULIO de 2006). *DISPOSITIVO USB.* CONTROL REMOTO VIA INTERNET DE UN PROCESO INDUSTRIAL, ESCUELA SUPERIOR POLITECNICA DEL LITORAL, GUAYAQUIL. Obtenido de USB: http://www.dspace.espol.edu.ec/bitstream/123456789/3264/1/5783.pdf

AGUILAR AGUILAR, J., & LEMA LAGOS, V. (11 de NOVIEMBRE de 2011). *ESCUELA POLITECNICA NACIONAL (EPN).* Obtenido de IMPLEMENTACION E INSTALACION DE UN SISTEMA DE SEGURIDAD EN LA NUEVA AERA DESIGNADA PARA EL LABORATORIO DE MICROCONTROLADORES: http://bibdigital.epn.edu.ec/bitstream/15000/7040/1/CD-5209.pdf

Alegsa, L. (1998). *DICCIONARIO DE DATOS.* Obtenido de SISTEMA: http://www.alegsa.com.ar/Dic/sistema.php

ALLAN, R. (2002). *ELECTRONICA.* SIMULADOR DE ELECTROCARDIOGRAMA, COLEGIO INDOAMERICANO. ESPAÑA: HALL, PRENTICE. Obtenido de http://132.248.38.3/SEV/pagina_congreso/congreso_estudiantil/memoria/area5/3.pdf

ATMEL. (2013). *ATMEL*. Obtenido de MICROCONTROLADOR ATMEL: http://www.atmel.com/products/microcontrollers/avr/default.aspx?tab=overview

BERMUDEZ, M., VARGAS IZQUIERDO, A., & SUAREZ RIVERA, K. (2010). *SISTEMA DE INFORMACION PARA EL ARCHIVO HISTORICO DEL DEPARTAMENTO NACIONAL DE PLANEACION*. CORPORACION UNIVERSITARIA MINUTO DE DIOS. Obtenido de CORPORACION UNIVERSITARIA MINUTO DE DIOS: http://repository.uniminuto.edu:8080/jspui/bitstream/10656/1733/1/TTI_VargasIzquierdoAngelaLuisa_2010.pdf

CABEZAS MIÑO, K. (2010). *RADIOFRECUENCIA.* CONTROL DOMOTICO INALAMBRICO CENTRALIZADO A TRAVES DE TOUCH SCREEN, ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO, CHIMBORAZO. Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/163/1/38T00155.pdf

CHAVEZ, R. (3 de NOVIEMBRE de 2011). *COMUNICACION SERIAL.* ESCUELA POLITECNICA NACIONAL, QUITO. Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/3903/1/CD-3625.pdf

CORTI, R., D'AGOSTINO, E., MARTINEZ, R., & BELMONTE , J. (2011). *SENSORES.* REDES INALAMBRICAS DE SENSORES INTELIGENTES, SEDICE, REPOSITORIO INSTITUCIONAL DE LA UNLP, ROSARIO. Obtenido de http://sedici.unlp.edu.ar/bitstream/handle/10915/19773/Documento_completo.pdf?sequence=1

E.J, B. (2003). *INGENIERIA DEL SOFTWARE, Una perspectiva orientada a objetos.* Obtenido de universidad de colombia: http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060024/Lecciones/Capitulo%20I/problemas.htm

ESPINOZA, J. C. (19 de febrero de 2007). *TUTORIAL MICROCONTROLADORES PIC.* SANTIAGO: PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE. Obtenido de http://web.ing.puc.cl/~mtorrest/downloads/pic/tutorial_pic.pdf

EZEQUIEL ROZIC, S. (2008). *BASE DE DATOS Y SU APLICACION.* DISEÑO E IMPLEMENTACION DE UN SISTEMA DE GESTIÒN DE GRADUADOS PARA LA UNIVERSIDAD TECNICA DE AMBATO, PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR SEDE AMBATO. Obtenido de http://repositorio.pucesa.edu.ec/jspui/bitstream/123456789/633/1/85002.PDF

GARCIA RAMIREZ, J. (JUNIO de 2014). *DESARROLLO DE ANALISIS DE FALLAS A TRAVES DE INTERFAZ TACTIL.* Obtenido de UNIVERSIDAD

TECNOLOGICA DE QUERETARO (UTEQ),: http://www.uteq.edu.mx/tesis/IMI/0390.pdf

JORQUERA, I. (24 de 10 de 2014). *XBee.CL*. Obtenido de TUTORIAL XBEE: http://xbee.cl/?p=27

NATIONAL INSTRUMENTS. (22 de ABRIL de 2009). Obtenido de RED DE SENSORES: http://www.ni.com/white-paper/7142/es/

NICHOLLS, J., & MAURICIO GOMEZ. (s.f.). *ALL ROBOTICS*. Obtenido de CLASIFICACION XBEE: http://all-robotics.com/

PADILLA, F. (2008). *DESARROLLO DEL SOFTWARE.* POTENCIANDO EL MODELADO CNCEPTUAL CON PATRONES, UNIVERSIDAD DE CASTILLA - LA MANCHA. Obtenido de http://www.dsi.uclm.es/personal/franciscomsimarro/pfc/pfc07/doc/feli08.pdf

PUCESE. (1990). *PUCESE*. Obtenido de RESEÑA HISTORICA: http://www.pucese.edu.ec/index.php/features/historia

PUCESE. (2013). *ORGANIGRAMA.* ESMERALDAS: PUCESE. Obtenido de http://www.pucese.edu.ec/images/organigrama%20estructural%20pucese.pdf

PUCESE. (2013). *VALORES, MISION Y VISION*. Obtenido de PUCESE: http://www.pucese.net/index.php/la-sede/valores

RAMIREZ, C. L. (MARZO de 2012). *UNIVERSIDAD POLITECNICA DE VALENCIA* . Obtenido de DISEÑO DE REDES DE SENSORES: https://riunet.upv.es/bitstream/handle/10251/15152/tesisUPV3764.pdf?sequence=1

ROLDAN VILORIA, J. (2010). *INSTALACIONES ELECTRICAS PARA LA VIVIENDA, CAJAS DE PROTECCION Y GRADOS DE PROTECCION* (8VA EDICION ed.). MADRID: MA. JOSE LOPEZ RASO. Obtenido de http://books.google.es/books?hl=es&lr=&id=BOhU0vqYhu8C&oi=fnd&pg=PR3&dq=La+caja+general+de+protecci%C3%B3n+el%C3%A9ctrica+conecta+a+l

os+clientes+a+la+red+de+la+empresa+distribuidora,+normalmente+en+baja+tensi%C3%B3n.+&ots=uv1p4GRrhO&sig=d6TDDwtcX6PdNhHG1P

SANCHEZ ROSERO, N., & NINACURI GUACHI, J. (2013). *MICROCONTROLADORES.* ESPOCH, ESTUDIO DEL CONTROL DOMOTICO , RIOBAMBA. Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/3078/1/25T00211.pdf

TORRITI, M. T. (26 de ABRIL de 2007). *TUTORIAL MICROCONTROLADORES PIC.* Obtenido de http://web.ing.puc.cl/~mtorrest/downloads/pic/tutorial_pic.pdf

TRUJILLO GRANADOS, H., & MERCHAN MILLAN, J. (2012). *PROCESO DEL DESAROLLO DEL SOFTWARE.* DESARROLLO E IMPLEMENTACION DE UN SISTEMA INTEGRADO DE GESTION EDUCATIVA, UNIVERSIDAD POLITECNICA SALESIANA, QUITO. Obtenido de http://www.dspace.ups.edu.ec/bitstream/123456789/3162/1/UPS-GT000318.pdf

ANEXOS

- **Anexo 1**

ENCUESTA DIRIGIDA AL PERSONAL DOCENTE QUE DA CLASES EN EL LABORATORIO DE COMPUTACIÓN DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE ESMERALDAS

1. **¿Qué dispositivos utiliza para proteger los computadores contra variaciones de voltaje?**

   Supresor de picos ☐

   Reguladores ☐

   Fuentes de alimentación ininterrumpida ☐

   Otro: _____

2. **¿Conoce usted que tipos de dispositivos se utilizan para la protección contra robo de equipos informáticos?**

   SI ☐ NO ☐

3. **¿Conoce usted si los equipos informáticos de la Universidad cuentan con dispositivos de protección contra robo?**

   SI ☐

   NO ☐

4. **¿Le gustaría que exista un dispositivo que permita controlar la seguridad física de los equipos de computación de su oficina o laboratorio?**

   ☐

   SI

   NO ☐

5. **¿Cree usted que la instalación de un moderno dispositivo de protección física de los equipos minimice los robos y pérdidas de los mismos?**

SI ☐

NO ☐

6. **¿De tener un costo el dispositivo cuanto estaría dispuesto a pagar por su computador?**

$25 ☐

$50 ☐

$100 ☐

$150 ☐

- **Anexo 2**

ENCUESTA DIRIGIDA AL PERSONAL ADMINISTRATIVO DE LA PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR SEDE ESMERALDAS

1. **¿Qué dispositivos utiliza para proteger los computadores contra variaciones de voltaje?**

   Supresor de picos ☐
   Reguladores ☐
   Fuentes de alimentación ininterrumpida ☐
   Otro: _____

2. **¿Con que frecuencia realiza mantenimiento al computador asignado a su estación de trabajo?**

   Diario ☐
   Una vez por semana ☐
   Una vez al mes ☐
   Nunca ☐

3. **¿Conoce usted que tipos de dispositivos se utilizan para la protección contra robo de equipos informáticos?**

   SI ☐ NO ☐

4. **¿Conoce usted si los equipos informáticos de la Universidad cuentan con dispositivos de protección contra robo?**

   SI ☐
   NO ☐

5. **¿Le gustaría que exista un dispositivo que permita controlar la seguridad física de los equipos de computación de su oficina o laboratorio?**

SI ☐

NO ☐

6. **¿Cree usted que la instalación de un moderno dispositivo de protección física de los equipos minimice los robos y pérdidas de los mismos?**

SI ☐

NO ☐

7. **¿De tener un costo el dispositivo cuanto estaría dispuesto a pagar por su computador?**

$25 ☐

$50 ☐

$100 ☐

$150 ☐

- **Anexo 3**

ENTREVISTA AL JEFE DE SISTEMAS

1. **¿Tiene Ud. conocimiento de cuál es el uso que dan los estudiantes a las computadoras?**

2. **¿Dentro del Laboratorio de Computación existe algún dispositivo físico que controle las variaciones de energía?**

3. **¿Se realiza un plan de seguridad física contra catástrofes como: inundaciones, incendios, cortes de energía?**

4. **¿Sabe Ud. la Importancia de la Seguridad física de los equipos del laboratorio de computación?**

5. **¿Ud. como Jefe de Sistemas, considera colocar algún dispositivo para la seguridad física de los equipos como: CPU, monitores, proyector, etc.?**

6. **¿Estaría Ud. de acuerdo con la implementación de un dispositivo para la seguridad y protección física de los equipos del Laboratorio de Computación?**

7. **¿Se presentan anomalías con respecto a la pérdida de equipos dentro del Laboratorio, en caso de producirse quién es el responsable?**

- **Anexo 4**

ENTREVISTA A LA ENCARGADA DEL LABORATORIO DE COMPUTACIÓN

1. **¿Tiene Ud. conocimiento sobre los medios de seguridad física en los equipos del laboratorio?**

2. **¿Qué piensa sobre los dispositivos de seguridad electrónica instalada dentro de las computadoras?**

3. **¿Cuál es la importancia de la seguridad física en los equipos del Laboratorio de Computación?**

4. **¿Ud. como encargada del laboratorio de computación, considera colocar algún dispositivo para la seguridad física de los equipos como: CPU, monitores, proyector, etc.?**

5. **¿Tiene Ud. conocimiento de cuál es el uso que dan los estudiantes a las computadoras?**

6. **¿Las personas que utilizan el laboratorio de computación, dan el uso correcto a los equipos, evitando averías o manipulación incorrecta?**

- **Anexo 5**

Verificacion del pin de encendido para la comunicación en modo alarma

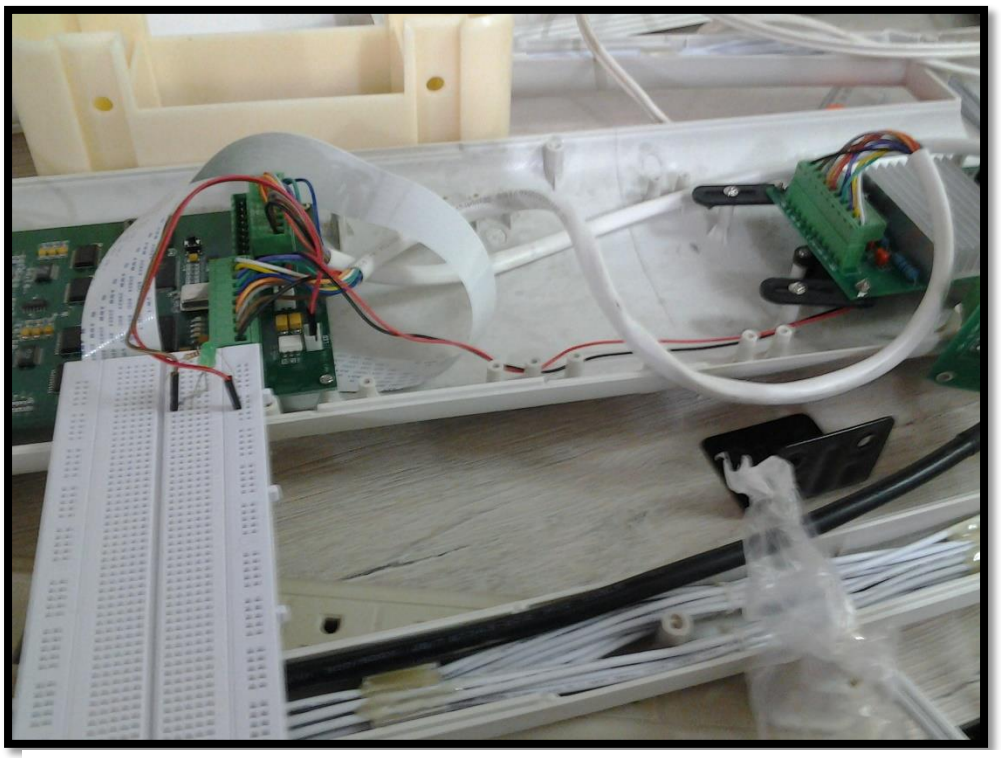


FIGURA 1. Verificación del Pin encendido

Conexión del protoboard, Arduino uno y el bluetooth para la comunicación de la antena con el computador.

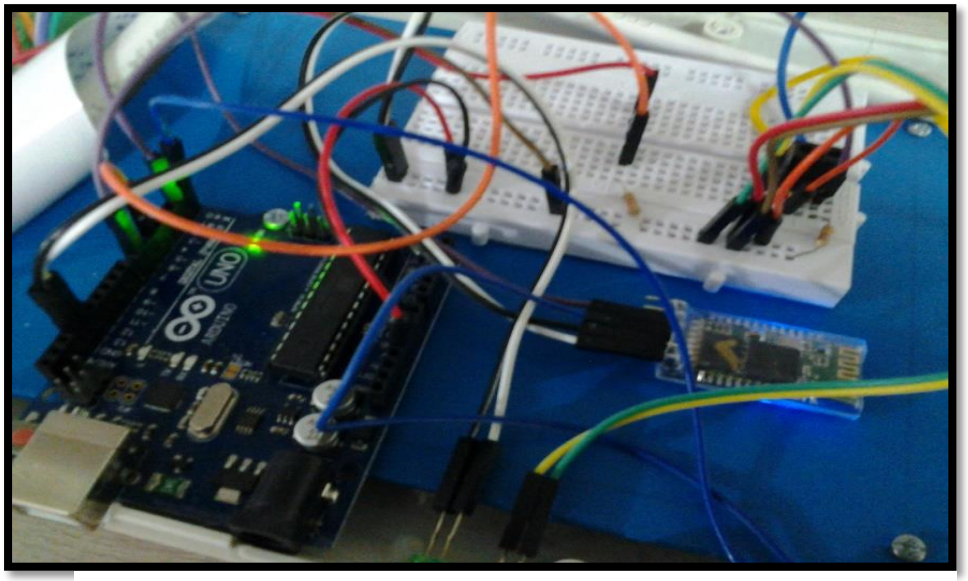


FIGURA 2. Conexión Arduino y bluetooth para comunicación

Se instaló un interruptor para que inhabilite la comunicación del bluetooth para la programación del Arduino uno mediante el cable USB.

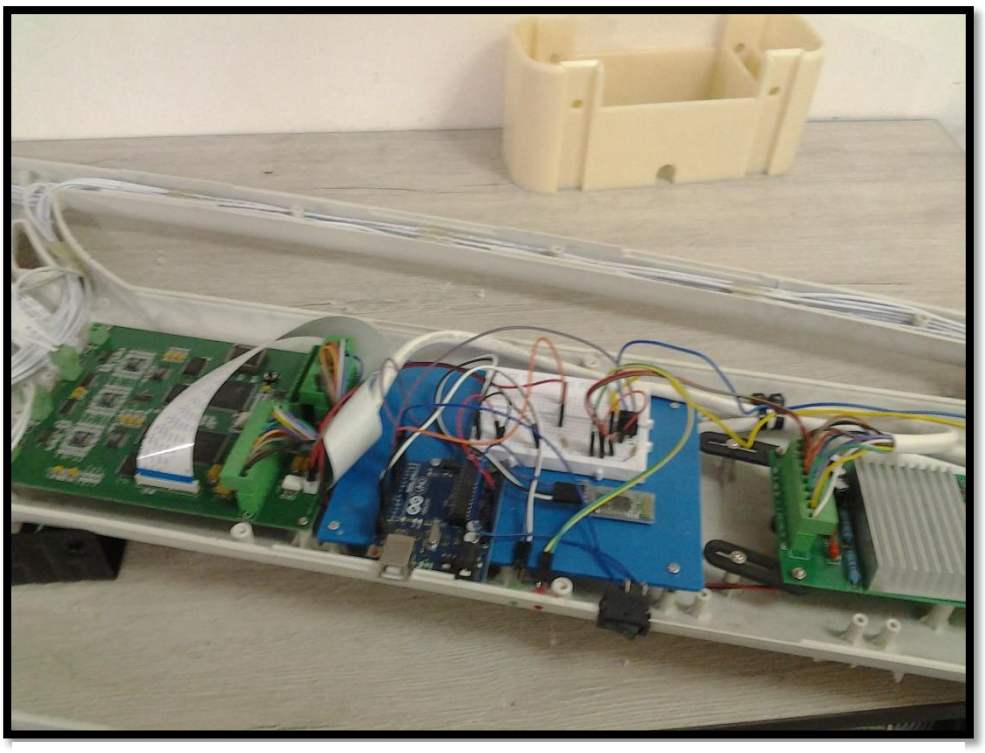


FIGURA 3. Interruptor para inhabilitar la comunicación del bluetooth

Sockert para repartir la energía a la antena y alimentar la tarjeta electrónica integrada a esta.

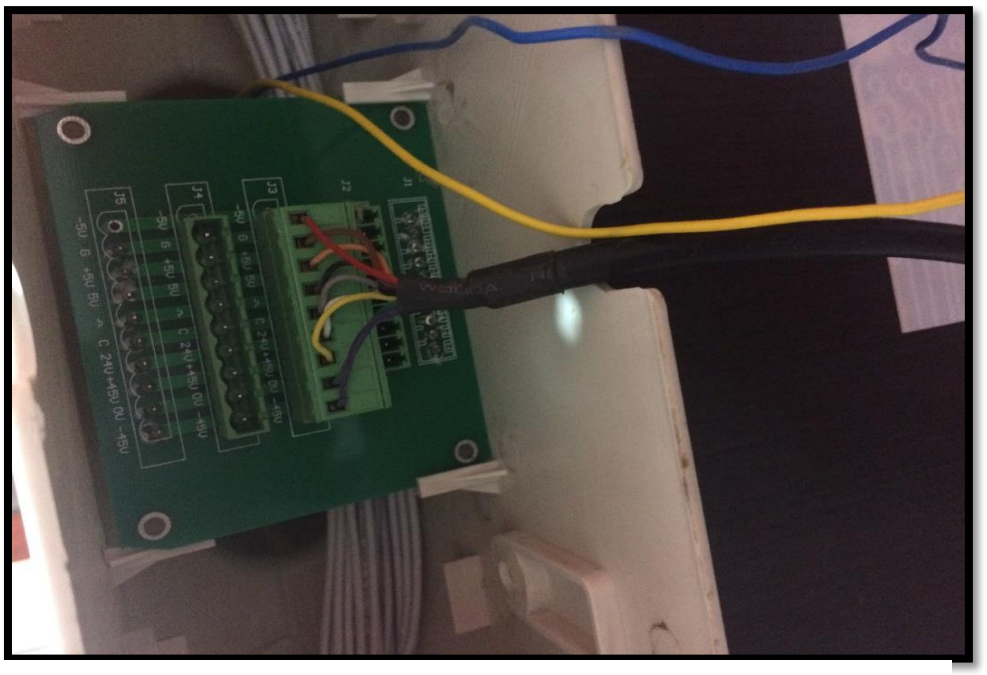


FIGURA 4. Fuente de Alimentación de la antena TX