# UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

## FACULTAD DE INGENIERÍA


# "SISTEMA DE MONITOREO DE SEGURIDAD FÍSICA EN PLATAFORMA LIBRE DE COMPONENTES ELECTRÓNICOS PARA ASEGURAR LA GESTIÓN DE LOS NIVELES DE CONTINUIDAD DE LOS SERVICIOS INFORMÁTICOS EN LA CENTRAL DE DATOS USAT"

**TESIS PARA OPTAR EL TÍTULO DE**
**INGENIERO DE SISTEMAS Y COMPUTACIÓN**

**AUTO: CESAR ARCEMIO CAMPOS BANCES**

**Chiclayo, Febrero del 2015**

# “SISTEMA DE MONITOREO DE SEGURIDAD FÍSICA EN PLATAFORMA LIBRE DE COMPONENTES ELECTRÓNICOS PARA ASEGURAR LA GESTIÓN DE LOS NIVELES DE CONTINUIDAD DE LOS SERVICIOS INFORMÁTICOS EN LA CENTRAL DE DATOS USAT”

**POR:**

**CESAR ARCEMIO CAMPOS BANCES**

**Presentada a la Facultad de Ingeniería de la Universidad Católica Santo Toribio de Mogrovejo para optar el título de INGENIERO DE SISTEMAS Y COMPUTACIÓN**

**APROBADA POR EL JURADO INTEGRADO POR**

**Ing. Ricardo David Imán Espinoza**
**PRESIDENTE**

**Ing. Huilder Juanito Mera Montenegro**
**SECRETARIO**

**Ing. Gregorio Manuel León Tenorio**
**ASESOR**

Esta dedicación surge como consecuencia de la admiración a la sabiduría y perseverancia de mi padre José y al amor y dedicación inacabable de mi madre Mary, a quienes les guardo un profundo amor y respeto por su gran ejemplo de vida y por formarme en valores desde mi infancia.

A mi esposa e hijos, quienes en todo momento me ofrecieron su apoyo invaluable, por el tiempo que dejé de estar con ellos por lograr este anhelo tan esperado, por su incondicional y recíproco amor.

A mi alma máter y en especial a todo el personal de TI de la USAT, a nuestro Director, Ing. Gregorio León, Lic. Lyndon Rodas, Ing. Jorge Olivos e Ing. Salvador Fernandez por su apoyo, aprecio y confianza depositada en mi persona.

**AGRADECIMIENTOS**

Al Todopoderoso, el que siempre está presente en nuestras vidas, nos guía e ilumina.

A mi Asesor. Ing. Gregorio León por sus valiosos aportes y por su incondicional apoyo a lo largo de todo este proyecto. Al Ing. Héctor Zelada, Ing. Roberto Ruidias y demás docentes que impartieron con profesionalismo todos sus amplios conocimientos en favor de nuestra formación académica.

Un agradecimiento especial también a mi asesora Ing. María Arangurí por impartirme el rigor académico en todas las asignaturas dictadas que me han servido de mucho para superar cualquier dificultad, por su paciencia, dedicación y apoyo.

# Índice

# RESUMEN

En el presente proyecto, tanto la justificación técnica, económica, social y científica han involucrado procedimientos, técnicas y metodologías que han sido aplicadas para un mejor desempeño de la Central de Datos dentro de la organización, en la cual, a través de la implementación de un sistema de monitoreo de seguridad física dentro del Centro de Datos de la USAT se ha conseguido centralizar en línea información relevante sobre indicadores correspondientes a seguridad física, teniendo la posibilidad de tomar acciones preventivas y no reactivas frente a los diferentes riesgos con los que convive actualmente esta área estratégica de la organización. El sistema de monitoreo de seguridad física ha sido implantado sobre una plataforma libre de software y hardware, garantizando el costo cero de licencias de software y permitiéndonos tener un hardware plenamente configurable a medida y escalable, asegurando como consecuencia la continuidad de los servicios informáticos que influyen directamente en la satisfacción tanto de los clientes internos como externos de la organización.

La hipótesis indica que "La implementación de un sistema de monitoreo de seguridad física mejora la gestión de los niveles de continuidad de los servicios informáticos de la Central de Datos USAT." en lo esencial, describe todos los procesos, ventajas y desventajas de la implementación de la propuesta, teniendo como objetivo principal asegurar la continuidad de los servicios informáticos que brinda la Central de Datos protegiendo desde una perspectiva holística de seguridad física el hardware instalado. El entorno donde se aplica esta investigación es un diseño cuasi experimental y nuestra población fue dividida en zonas específicas de la Central de Datos compuestas por equipos informáticos de acuerdo a los indicadores establecidos. Se utilizó una Metodología de Desarrollo de Proyectos de Hardware libre la cual ha garantizado en todos los hitos el correcto desarrollo de la solución propuesta.



PALABRAS CLAVE: Arduino, software libre, hardware libre, microcontrolador.



# ABSTRACT

In this project, technical, economic, social and scientific justification have involved procedures, techniques and methodologies that have been applied to improve the performance of the Central Data within the organization, which through the implementation of a monitoring security system within the Data Center has achieved USAT online centralize relevant information about indicators for physical security, with the possibility of taking preventive rather than reactive actions against the various risks that currently lives this strategic area of the organization. The monitoring security system has been implemented on a free software platform and hardware, ensuring zero-cost software licenses and allowing us to have a fully configurable and scalable as hardware, as a result ensuring the continuity of IT services directly influencing satisfaction of both internal and external customers of the organization.

The hypothesis "Implementing a monitoring system enhances security management levels continuity of computer services Data Central USAT." Essentially describes all the processes, advantages and disadvantages of implementing the proposal, with the main objective to ensure continuity of IT services provided by the Central data from a holistic perspective protecting physical security hardware installed. The environment in which this research applies a quasi-experimental design and our population was divided into specific areas of the Central Data consist of computer equipment according to established indicators. Methodology Development Project Free Hardware which has guaranteed all milestones in the proper development of the proposed solution was used.

KEYWORDS**:** Arduino, free software, free hardware, microcontroller

# I. INTRODUCCIÓN

Los Centros de Datos han dejado de ser simples centros de procesamientos para convertirse en verdaderas herramientas de negocios dentro las organizaciones, siendo todo un reto para TI asegurar su disponibilidad como principal objetivo. Las técnicas más comunes que habían sido utilizadas para monitorear el entorno de un centro de datos datan de los días de las computadoras centralizadas e incluían prácticas como caminar por las instalaciones del Centro de Datos con termómetros y confiar en que el personal del área informática "sienta" como está el ambiente, sin embargo, debido a que los centros de datos han evolucionado y el procesamiento distribuido y las tecnologías para servidores elevan la demanda de energía y enfriamiento, se debe analizar este entorno más cuidadosamente. Si analizamos desde una perspectiva internacional podemos apreciar que en la central de datos instalada en el edificio World Trade Center de Seatle (Estado de Washington, en el noroeste de los Estados Unidos de América) el área de Tecnologías de la información empezó a enfrentar una difícil situación debido al incremento de servidores como consecuencia de la ampliación significativa de sus sistemas de investigación y de producción. Como respuesta, se quería crear un nuevo centro de datos más grande que pueda albergar a todos los equipos informáticos, sin embargo se tenían que enfrentar a problemas como: carencia de carga adecuada de la subestación eléctrica, espacio físico para generadores y refrigeradores que un centro de datos convencional lo ameritan. Además, el área de tecnologías tenía que soportar problemas en su centro de datos como la mala distribución del aire que causaba que algunos de sus equipos informáticos lograran sobrecalentarse. Para contrarrestar esto, el área de TI optaba por bajar más la temperatura ambiente de la central consumiendo por ende más energía. A toda esta problemática, se propuso un diseño basado en mejores prácticas como la Power Usage Efficiency (PUE) que se basa en la optimización de eficiencia de energía, además de un monitoreo adecuado que sea capaz de prevenir posibles riesgos en lo que a seguridad física de centro de datos se refiere. Este diseño se logró implementar teniendo buenos resultados y superando estas dificultades.

Mediante ese contexto, en la presente tesis se analizó una realidad problemática similar en la Universidad Católica Santo Toribio de Mogrovejo quien a través de los años ha sufrido un incremento del 100% de sus servidores y del 50% en PC respecto a años anteriores con la finalidad de ampliar sus servicios informáticos para satisfacer la demanda por el aumento de su población estudiantil. Este incremento de servidores en la Central de Datos sumado a las demandas de enfriamiento que requieren las nuevas tecnologías de servidores incorporadas planteó deficiencias en lo que respecta a refrigeración y al monitoreo del entorno de esta Central, pues no existe redundancia de aire acondicionado y no se contaba con un monitoreo de seguridad física. En estas circunstancias, la organización se encuentra en riesgo de no poder prevenir estas amenazas a tiempo que afectarían directamente en la continuidad de sus servicios informáticos y por ende al desarrollo normal de sus actividades.

La formulación del problema se resuelve planteando que la implementación de un sistema de monitoreo de seguridad física en plataforma libre de componentes electrónicos asegura la gestión de los niveles de continuidad de los servicios informáticos de la Central de Datos USAT. En el logro de la hipótesis

se definen los siguientes objetivos; Disminuir los costos de inversión en adquisición de equipos informáticos en la Central de Datos por reposición, para optimizar el presupuesto reservado para adquisición de infraestructura de TI que tiene la organización; disminuir la cantidad de equipos que sufrieron daños por seguridad física; Incrementar el número de usuarios administrativos y estudiantiles satisfechos por la continuidad de los servicios informáticos proporcionada por la Central de Datos USAT; Aumentar el ciclo de vida útil de los equipos informáticos en la Central de Datos con el sistema de monitorización automatizado de seguridad en física implantado.
La presente investigación se sustenta desde el aspecto tecnológico porque se planeó mejorar la gestión de monitoreo de la seguridad física en la central de Datos de la USAT, a través de la implementación de un sistema de monitoreo automatizado en la cual se hizo uso de una innovadora plataforma libre de componentes electrónicos programables; aplicada para prevenir y reducir daños físicos de hardware de los equipos de cómputo. La plataforma de hardware y programación libre se basó en Arduino, una placa de componentes electrónicos que interactúa con un microcontrolador y un entorno de desarrollo. Esta plataforma fue diseñada para la elaboración de proyectos multidisciplinares.

El software utilizado consiste en un entorno de desarrollo que implementa el lenguaje de programación Processing/Wiring y un cargador de arranque boot loader (que se ejecuta en la placa). Al ser open-hardware, tanto su diseño como su distribución son libres, es decir, no necesita licencia alguna para poder utilizarse en cualquier tipo de proyecto. Existen innumerables tipos de interfaces que pueden ser conectados a esta plataforma, en este proyecto se utilizaron interfaces que cubrieron nuestras necesidades como: sensores de temperatura, sensores de humedad, interfaz Ethernet, actuadores (como relés), etc. Por otro lado, en el aspecto económico, el uso de este sistema de monitoreo de seguridad física no solo implicó la mejora en la gestión actual de seguridad física sino que redujo riesgos emergentes que se traducían en pérdidas de materiales costosos por la magnitud de inversión en infraestructura tecnológica que se tiene en esta Central de Datos. Actualmente se cuenta con una inversión que bordea los 300000 dólares solo en equipos informáticos instalados dentro del CPD. Este sistema ayuda a prevenir riesgos como incendios (por excesos de temperatura en el ambiente), corrosión de componentes electrónicos de los equipos informáticos (por una humedad inadecuada) y robos (por una inadecuada gestión de acceso de personas) etc. Y además toma acciones puntuales a los riesgos anteriormente descritos. En lo referente al aspecto social, el uso de esta tecnología para prevenir amenazas físicas en una zona crítica como una central de datos no solo salvaguarda la integridad física de personas y equipos informáticos sino que también ayuda a mejorar el adecuado consumo energético, representando esto una mejor disposición ecológica de la empresa.
Por otro lado, el impacto de tener equipos que funcionen ininterrumpidamente no solo colabora con la continuidad del negocio sino que los usuarios dentro de la organización como estudiantes, personal administrativo y fuera de la organización como padres de familia, empresas proveedoras, universidades con convenio, etc. se verán más satisfechos con el servicio que se proporciona. En el aspecto científico esta y otras tecnologías referentes no dejan de converger en un nuevo paradigma que para este estudio se aplicó y evaluó en el proceso de validación de nuestra hipótesis a través de un diseño de contrastación pre test y

post test, midiendo los indicadores que demuestran la mejora de la variable independiente.

# II. MARCO TEÓRICO

## 2.1 ANTECEDENTES DEL PROBLEMA:

### 2.1.1 INTERNACIONALES

Según Ricardo Napoleón Guangalango Vega y Patricio Esteban Moscoso Montalvo (2011), pertenecientes a la Escuela Politécnica del Ejercito del Ecuador en su tesis titulada "Diseño de Infraestructura de Telecomunicaciones para un Data Center", hacen un enfoque principalmente en el estudio y usabilidad de una norma y una metodología formal principalmente aplicable a este proyecto. La Norma ISO 27000 que especifica claramente los requerimientos necesarios para establecer, mantener y mejorar un Sistema de Gestión de Seguridad de la información y por otro lado la Metodología formal de Análisis y Gestión de Riesgos de los Sistemas de Información denominada MAGERIT, elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las tecnologías de la Información, enfocadas a las Administraciones públicas. Esta tesis concluye evidenciando mejoras a nivel de seguridad informática y reducción de riesgo de la situación actual de 65.4% a 29,3% según el análisis de sus indicadores, mitigando en gran porcentaje a las amenazas y vulnerabilidades encontradas en la investigación. La relación que existe con el presente proyecto de investigación es que ambas están fundamentadas en normas y metodologías formales para tratar problemas de seguridad física en un entorno informático. Si bien es cierto este proyecto se centra básicamente en la evaluación o auditoria de su Data Center para mejorar su gestión, gran parte de nuestro proyecto también evaluará el entorno del CPD actual, proponiendo la mejor alternativa y ofreciendo un producto acreditable. Se ha identificado en esta tesis algunos indicadores de seguridad física en un Anexo del ISO 27001 como controles de acceso a personal, protección contra amenazas externas y del entorno, perímetro de seguridad física, etc.

En la siguiente tesis cuyo título fue: Design and Evaluation of Physical Security in Data Centers (Diseño y Evaluación de Seguridad Física en Data Centers) (2013), cuyo autor Ilari Wager, estudiante de la University of Applied Sciencies de Laurea presenta como objetivo principal el desarrollo de un modelo para el diseño, implementación, evaluación y mejora de las medidas de seguridad física de las instalaciones del centro de datos. Además, con base en las teorías aplicables y el modelo de gestión de la seguridad física actuales, se elaboró un plan maestro de seguridad física del centro de datos que faciliten la toma de decisiones, ayude a justificar las inversiones en seguridad, así como mostrar el estado total de la protección específica del data center y las medidas de que se crearon. La relación que existe de esta tesis con nuestro proyecto de

investigación es que ambas están fundamentadas en normas y metodologías formales asimismo se sustenta en las mejores prácticas en los que a seguridad física de centro de datos se refiere. Nos enfocaremos en las Normas internacionales como la Norma TIA 941, ISO 27001 y el manual de buenas prácticas proporcionados por la ASHRAE donde especifica todos los lineamientos a considerar para evitar riesgos de seguridad física en Data Centers.

Según la Empresa CISCO, empresa líder en telecomunicaciones en su caso de estudio titulado: University Builds Physical Security Framework for Growth (Universidad Construye Marco de Seguridad Física para su crecimiento) (2010) describe un caso de estudio publicado electrónicamente aplicado en la Universidad Pública Channel Islands del estado de California en Estados Unidos. Como antecedentes se describe que esta prestigiosa universidad con el fin de poder incrementar el nivel tecnológico para un mejor aprendizaje de sus alumnos acorde a las nuevas tendencias decidió renovar la infraestructura tecnológica y arquitectónica de su Campus construido en 1930, esto significó también la renovación algo radical de su centro de datos para lo cual no estaban preparados en lo que respecta a amenazas físicas y lógicas. Esto a su vez representaba un riesgo explícito en la seguridad de este Data Center. Cisco explica como aplicando buenas prácticas de seguridad física electrónica logró minimizar riesgos al implementar desde un sistema de vigilancia por cámaras centralizado hasta un sistema de control de acceso físico, teniendo como resultados una reducción significativa de costos operativos (cerca de 50000 Dólares anuales) al mejorar la vigilancia por cámaras y al cambiar el acceso del personal por simples llaves y cerraduras a tarjetas magnéticas de identificación de usuarios. La relación que tiene este caso de estudio con nuestro proyecto es que ambos tienen la misma perspectiva de fondo, minimizar riesgos y reducir costos implementando mecanismos actuales de seguridad física en una central de datos para asegurar el crecimiento de la organización.

### 2.1.2 NACIONALES:

Según Liliana Raquel Castillo Devoto en su tesis titulada: "Diseño de Infraestructura de Telecomunicaciones para un Data Center" publicada en la Universidad Pontificia Universidad Católica del Perú en el año 2011 se enfoca en brindar una metodología de diseño de infraestructura de telecomunicaciones para la implementación de un Centro de Datos. Se enmarca en normas que establecen parámetros para la mejor ubicación y diseño de un Centro de Datos, soluciones de puesta a tierra, sus componentes y sus debidas rutas. Asimismo muestra un panorama de un estudio de las adecuadas distribuciones físicas de todos los componentes que componen una CPD. Según las conclusiones, este diseño planteó mejoras sustanciales en lo que respecta a normas de cableado estructurado, límite de espacios físicos establecidos para Data Center, ubicación de gabinetes de equipos de redes de comunicaciones y etiquetado de patch cord en la conectividad de los mismos. La relación que existe con el presente proyecto de investigación es que en nuestro proyecto analizaremos también este tipo de normas y buenas prácticas que se tienen en la actualidad sobre infraestructura de telecomunicaciones, pues tenemos que saber si la CPD de

estudio cumple con todas esas normas para poder aplicar de forma correcta nuestra propuesta de implementación de monitorización de seguridad física.

### 2.1.3 LOCALES

Según Víctor Carlos Quiñones Rado en su tesis titulada "Auditoría de los Sistemas Informáticos de la Escuela de Postgrado de la Universidad Nacional Pedro Ruiz Gallo" en el 2008 se pretendió determinar los problemas bajo la modalidad de auditoría de sistemas que se presentan en la unidad de Informática de la escuela de postgrado de esta universidad. El estudio realizado definió varias falencias en la gestión de seguridad física y lógica de esta unidad informática puntualizando en problemas como: pérdida de información confidencial por falta de control de acceso de usuarios, deterioros de los equipos de cómputo, por mala manipulación de personas no calificadas, ausencia de medidas de prevención de catástrofes como incendios. Según esta tesis, gracias a la auditoría se logró determinar qué aspectos estaban fallando mejorando la gestión de la seguridad física y lógica en la unidad de informática de la escuela de post-grado de esta Universidad. Según las conclusiones se logró mejorar al 100% las pérdidas de información incorporando un adecuado control de acceso del personal a las instalaciones de CPD.

La relación que existe con el presente proyecto de investigación es que en nuestro proyecto analizaremos también este tipo de falencias en cuanto a seguridad física de la central de datos de la USAT y además propondremos una solución implementada con tecnología libre de componentes electrónicos para monitorización con el fin de evitar los problemas encontrados en esta tesis de referencia. Esto significará una gran ventaja competitiva en la gestión de la seguridad física de la Central de Datos frente a las metodologías tradicionales de nuestro entorno.

## 2.2 BASES TEÓRICO – CIENTÍFICAS

En el presente estudio, nuestra variable dependiente: Gestión de los niveles de continuidad de los equipos informáticos influirá como punto de inicio para el desarrollo de este proyecto.

El concepto de Gestión, desde nuestra perspectiva, hace referencia a una especie de "acción y consecuencia" de administrar algo. A todo esto, se debe incidir en que gestionar involucra llevar a cabo diligencias que hacen posible la realización de un anhelo cualquiera. Sin embargo, gestionar engloba las ideas de gobernar, disponer, dirigir u organizar una determinada cosa o situación.

### 2.2.1 Seguridad Física en Centro de Datos

Empezaremos evaluando como es que se está gestionando la seguridad física en los Centros de Procesamiento de Datos en la actualidad.

En la actualidad, los Data Centers son actores claves de los negocios digitales, por este motivo, las empresas necesitan expandir su infraestructura para así optimizar y mejorar los rendimientos. Para dar respuesta a estas demandas, los departamentos de TI centran sus tareas de planificación en maximizar los diseños, despliegues, operaciones y gerenciamiento de la infraestructura de Centro de Datos. Según Gartner (2012), los Data Centers deben continuar con el crecimiento de datos, casi de manera exponencial para mantener la escalabilidad en todos sus sistemas para continuar con el crecimiento de los negocios. Para ello, la conectividad, la reducción de costos de energía, enfriamiento y el espacio son puntos esenciales.

En ese mismo contexto, [2] afirma Carlos Di Muccio (2012), los desafíos top relevantes desde hace pocos años van desde la disponibilidad, monitoreo y management, densidad de calor, eficiencia energética, densidad de la energía y restricción del espacio.
Según el libro "Holistic Management" (2007), se define a la seguridad al igual que una organización, que va desde un sistema viable hasta un sistema con posibilidades. Ver figura 1.

**FIGURA 1. La Seguridad Como una Organización**


**Fuente:** Jeimy J. cano. (2009). ISACA, Seguridad Lógica y Seguridad Física: Dos mundos Convergentes. 6 (1).

Como podemos apreciar la viabilidad se refiere a la capacidad que tiene toda organización de continuar existiendo en su entorno por sí mismo independiente del medio. La seguridad es viable en si misma gracias a la inseguridad que vive permanentemente en el entorno.

En este contexto, nuestro proyecto de seguridad física aportará a la viabilidad de la organización asegurando la continuidad de sus servicios informáticos y por ende mejorando la gestión de sus procesos intrínsecos.

### 2.2.2 Seguridad Física y Electrónica

De acuerdo con Contos, B., W. Crowell; C. DeRodeff; D. Dunkel; E. Cole; en su libro "Physical and Logical Security Convergence (2007), existen cuatro categorías de seguridad física (figura 2): las obstrucciones físicas, las técnicas de vigilancia, los sistemas de inteligencia y el personal de seguridad. Estas cuatro categorías representan la caracterización de la seguridad misma en el mundo real, que hoy en día existen y que cuentan todas ellas con su referente en el mundo lógico.

**FIGURA 2. Cuatro Categorías de la Seguridad Física**


**Fuente:** Jeimy J. cano. (2009). ISACA, Seguridad Lógica y Seguridad Física: Dos mundos Convergentes. 6 (3).

### 2.2.3 Disciplinas de Administración de riesgos

Según ASIS Internacional (Red mundial de profesionales en temas de Seguridad y Protección) para las Certificaciones Profesionales PSP (Physical Security Professional), existen profesionales especialistas en cuatro diferentes disciplinas de aplicación de la administración de riesgos: seguridad de la información, seguridad física, continuidad del negocio y valoración de riesgos.

En este contexto, se puede apreciar claramente que el concepto especializado de seguridad tiende a integrarse en uno solo, estas disciplinas con visiones diferentes convergen en lo que a administración de riesgos se refiere y es como sustentamos nuestro proyecto de seguridad física en uno de los activos más importantes de la organización como es su Centro de datos, previniendo los riesgos que se puedan generar y garantizar los niveles de continuidad de los servicios informáticos de los mismos.

### 2.2.4 Monitoreo de una Central de Datos:

Otros de los componentes de un CPD se encuentra en el monitoreo que se define concretamente como una forma de vigilar, componente que es de vital apoyo para mantener la seguridad física del CPD.

### 2.2.5 Sensores

Un sensor básicamente es un dispositivo diseñado o preparado para captar información de una magnitud del exterior y transformarla en otra que seamos capaces de interpretar, cuantificar o manipular.

Se pueden utilizar una gran variedad de sensores con el fin de recepcionar datos que pueden ser interpretados al convertirlos en información y que a su vez nos indiquen problemas causados por las amenazas descritas anteriormente. En nuestro proyecto utilizaremos sensores de temperatura, humedad y En la siguiente tabla podemos mostrar algunas pautas para los sensores básicos:

**TABLA Nº 1** – Pautas para los sensores básicos

| Tipo de sensor | Ubicación | Mejor práctica general | Comentarios | Pautas aplicables de la industria | Ejemplo |
|---|---|---|---|---|---|
| Sensores de temperatura | Rack | En la parte superior, central e inferior de la puerta frontal de cada rack informático, monitorear la temperatura de entrada de los dispositivos del rack | En las salas de cableado y otros entornos de rack abierto, el monitoreo de temperatura debe encontrarse lo más cerca posible de las entradas de los equipos | Pautas ASHRAE[3] |  |
| Sensores de humedad | Hilera | Uno por cada pasillo frío, en la parte frontal del rack en el medio de la hilera | Dado que las unidades CRAC brindan mediciones de humedad, quizá sea necesario modificar la ubicación de los sensores de humedad por hilera si éstos se encuentran demasiado cerca de la salida de la unidad CRAC | Pautas ASHRAE |  |
| Sensores de líquidos tipo cable<br>Sensores puntuales de líquidos | Sala | Ubicar los sensores de líquidos tipo cable alrededor de cada sistema CRAC, de las unidades de distribución de enfriamiento, bajo los pisos elevados y cualquier otra fuente de filtraciones (como cañerías) | Sensores puntuales de líquidos para monitorear el derrame de fluidos de la bandeja de condensado, para el monitoreo en salas más pequeñas y cualquier otro punto a baja altura | No existen estándares en la industria |  |
| Cámaras digitales de video | Sala e hilera | Ubicarlas estratégicamente según la disposición del centro de datos, para controlar puntos de entrada y salida y brindar una buena vista de todos los pasillos calientes y fríos; asegurarse de cubrir todo el campo visual requerido | Se debe monitorear y grabar el acceso normal además del acceso no autorizado o fuera de horario con software de vigilancia por video | No existen estándares en la industria |  |

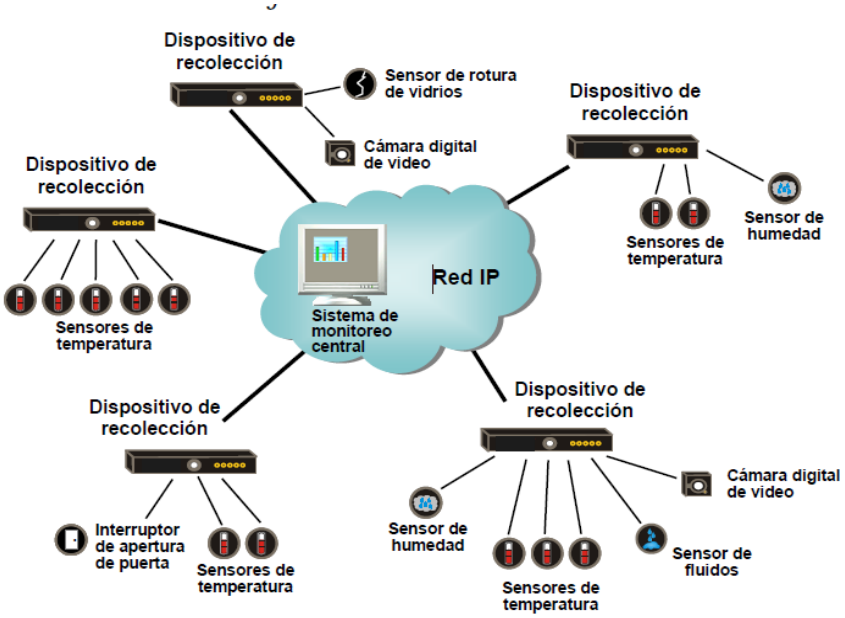
**Fuente**: Christian Cowan. (2009). APC, Amenazas Físicas en un Centro de datos. (7)

### 2.2.6 Sensores ambientales

Según Christian Cowan, gerente de productos ambientales y de seguridad de APC y Chris Gaskins, experto en la industria de alta tecnología, los sensores proporcionan datos en bruto, siendo de suma importancia interpretar adecuadamente estos datos para emitir alertas y notificaciones y realizar las correcciones necesarias. A medida que las estrategias de monitoreo se vuelven cada vez más sofisticadas, afirman estos expertos, es necesario contar con un procesamiento inteligente de la gran cantidad de datos que puedan surgir. En tal sentido, se debe de tener en consideración que una de las formas más efectivas y eficientes de recolectar y analizar los datos de los sensores para realizar acciones apropiadas, es el uso de dispositivos recolectores. En el proyecto utilizaremos sensores ambientales para realizar el monitoreo específicamente de temperatura y humedad. Estos sensores van a ser instalados

en lugares estratégicos por zonas dentro de la Central de Datos y enviarán información en bruto a nuestra plataforma electrónica Arduino quien procesará esos datos y enviará información relevante y alarmas mostradas en un único sistema.
En la siguiente figura tenemos un alcance de cómo pueden ser distribuidos los sensores ambientales para la recolección de datos en Una Central de Datos.

**FIGURA Nº 3: Recolección de Datos de los Sensores**




**Fuente**: Christian Cowan. (2009). APC, Amenazas Físicas en un Centro de Datos. (10)

### 2.2.7 Cámaras de seguridad en Centro de Datos

Las cámaras de seguridad han logrado constituirse en un instrumento imprescindible al momento de monitorear sistemas realmente críticos o sistemas especialmente atractivos para personas indeseadas o no autorizadas. En un Centro de Datos que almacena datos críticos para el funcionamiento de una organización, las cámaras de seguridad juegan un papel muy importante para monitorear el entorno de un CPD ante la posibilidad de intrusos o de actuaciones sospechosas del personal. Por lo expuesto, para controlar el acceso a personas no autorizadas a la Central de Datos de la USAT es imprescindible contar con cámaras de seguridad instaladas en puntos estratégicos las cuales puedan brindar imágenes de calidad aceptables para el monitoreo respectivo. En la actualidad vemos que las soluciones de seguridad basada en cámaras de vídeo han evolucionado vertiginosamente, tanto así que con cámaras IP que pueden emitir video por si mismas además de comprimir el video y enviarlo pueden tener una gran variedad de funciones como: envío de correo electrónico con imágenes, activación mediante movimiento de la imagen, activación a

través de otros sensores, control remoto, posibilidad de guardar y emitir los momentos anteriores a un evento, etc.

**FIGURA Nº 4. Cámara con conexión IP o analógica**


**Fuente:** Cámaras térmicas con conexión IP o analógica. [Imagen]. (accesada el 20 de agosto, 2013)

### 2.2.8 Amenazas físicas en Centro de Datos

De acuerdo con el enfoque de Christian Cowan y Chris Gaskins en un informe interno de APC (2011), entre las amenazas físicas a equipos informáticos se pueden localizar problemas de alimentación y enfriamiento, errores humanos, actividades maliciosas, incendios y la calidad de aire. Algunas de estas amenazas, incluyendo aquellas relacionadas con la alimentación y otras relacionadas con el enfriamiento y los incendios, se monitorean regularmente por medio de capacidades integradas en los dispositivos de alimentación, enfriamiento y extinción de los incendios. Sin embargo para cierta clase de amenazas físicas en un Centro de Datos, a veces el usuario no cuenta con soluciones de monitoreo prediseñadas e integradas. En este enfoque se deja muy claro las amenazas físicas que de no ser controladas debidamente pueden significar un riesgo en los equipos informáticos. Pues bien, la seguridad física se encarga de identificar, analizar y controlar estas variables que están presentes en escenarios donde existan equipos informáticos. En nuestra realidad ese escenario es la Central de Datos de la USAT donde se analizará primero las amenazas físicas tanto del ambiente físico como de los equipos informáticos existentes siguiendo siempre los lineamientos de las normas y buenas prácticas para seguridad física en Centro de Datos. A continuación se plasma en la siguiente figura los factores que representan amenazas tanto en infraestructuras físicas como digitales. Se puede apreciar que en este caso APC (Empresa dedicada a fabricar soluciones en protección de energía eléctrica a equipos informáticos) considera algunas amenazas físicas distribuidas que pueden ser monitoreadas con sensores específicos, caso similar al que aplicaremos en nuestro proyecto donde instalaremos sensores ambientales en puntos específicos y estratégicos distribuidos en zonas dentro de la Central de Datos.

**TABLA Nº 2. Amenazas a los Centros de Datos**

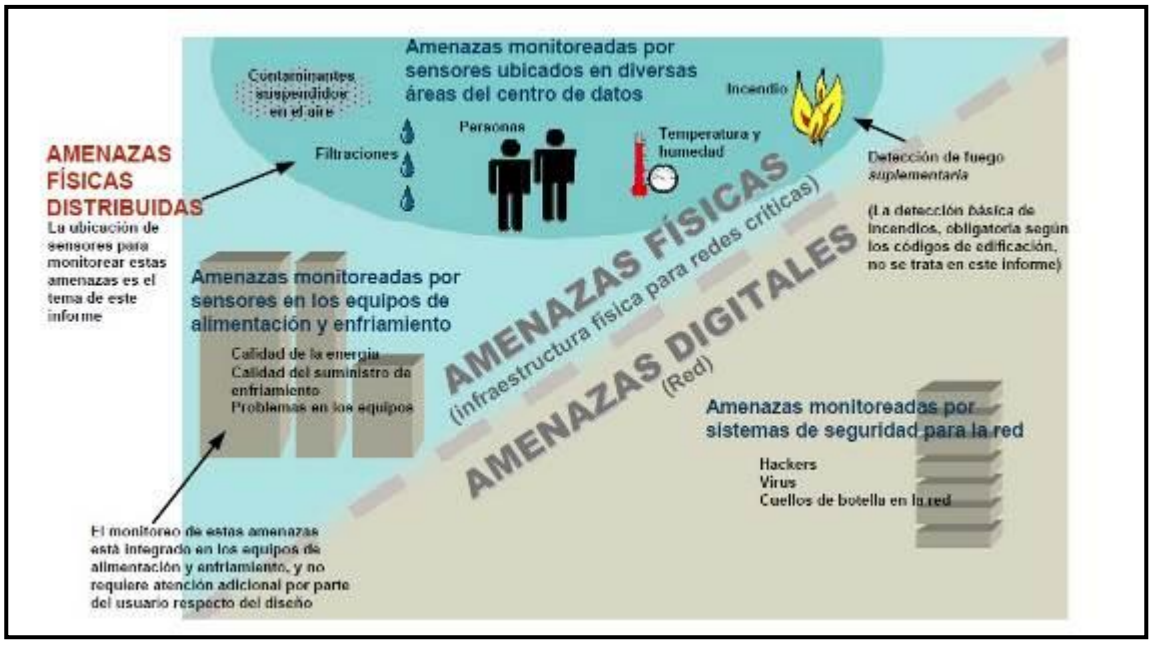
| Amenaza | Definición | Impacto en el Centro de Datos | Tipos de Sensores |
|---|---|---|---|
| **Temperatura del Aire** | Temperatura del aire en la sala, el rack y los equipos. | **Fallas** en los equipos y disminución de la vida útil de los equipos debido a temperaturas mayores de las especificadas y/o cambios drásticos de temperatura. | Sensores de Temperatura |
| **Humedad** | Humedad relativa de la sala y del rack a una temperatura determinada | Fallas en los equipos debido a la acumulación de electricidad estática en los puntos de baja humedad.<br>Formación de condensación en los puntos de humedad alta. | Sensores de Humedad |
| **Filtraciones de líquidos** | Filtraciones de agua o refrigerante | Daños en los pisos, el cableado y los equipos causados por líquidos. | Sensores de cable de filtraciones.<br>Sensores puntuales de filtraciones. |
| **Error humano y acceso del personal** | Daños involuntarios causados por el personal.<br>Ingreso no autorizado por la fuerza al centro de datos con intenciones maliciosas. | Daño a los equipos y pérdida de datos<br>Tiempos de inactividad de los equipos<br>Robo o sabotaje de equipos | Cámaras digitales de video.<br>Sensores de movimiento<br>Conmutadores de la sala.<br>Sensores de rotura de vidrios<br>Sensores de vibración |
| **Humo / Incendios** | Incendio de equipos eléctricos o materiales | Fallas en los equipos<br>Pérdida de bienes y datos | Detectores de humo suplementarios |
| **Contaminantes peligrosos suspendidos en el aire** | Químicos suspendidos en el aire, como hidrógeno de las baterías, y partículas, como polvo | Situaciones de riesgo para el personal y/o falta de confiabilidad en el sistema UPS, y fallas debidas a la emanación de hidrógeno.<br>Fallas en los equipos debidas al aumento de la electricidad estática y a la obstrucción de filtros/ventiladores por la acumulación de polvo | Sensores de químicos/hidrógeno<br>Sensores de polvo |

**Fuente:** Como monitorear amenazas físicas en Centro de Datos - Informe Técnico APC N° 102)

### 2.2.9 Amenazas Físicas Distribuidas:

En la actualidad, en lo referente a amenazas físicas en Centro de Datos se habla mucho de Amenazas Físicas Distribuidas que se encuentran presentes en varias ubicaciones y que requieren una evaluación, toma de decisiones y planificación con el fin de determinar el tipo, la ubicación y la cantidad de sensores en monitoreo. Para tal efecto, es necesario conocer qué tipo de amenazas físicas encuentran distribuidas en el Centro de Datos donde se va a instalar un sistema de monitoreo ya que si no se toma en cuenta esta evaluación se puede redundar en negligencias al combatir este tipo de amenazas.
Para tener un panorama claro de este tipo de amenazas, el impacto que puedan tener y los tipos de sensores recomendados que se tendrán en cuenta al momento de implementar la solución de monitoreo se muestra esta tabla descriptiva y explicativa que nos ayuda a aterrizar estos conceptos.

**FIGURA Nº 5: Amenazas Físicas Distribuidas**




**Fuente**: Informe Interno N° 43 de APC "Como monitorear las amenazas físicas en un Centro de Datos".

### 2.2.10 Umbrales sugeridos para los sensores de temperatura y humedad

La Sociedad Americana de Aire Acondicionado, Refrigeración y Calefacción (ASHRAE) en su nueva guía ambiental de buenas prácticas para Data Centers

hace referencia a los umbrales sugeridos para temperatura y humedad según la Norma ASHRAE TC9.9 recomendadas para Centro de Datos en varias de sus versiones. Ver tabla 03.

**TABLA Nº 3. Grados de temperatura y humedad recomendadas para Data Center**

| CONDICIONES DE TEMPERATURA Y HUMEDAD | **VERSIÓN 2004** | **VERSIÓN 2008** |
|---|---|---|
| LOW END TEMPERATURE | 20°C (68 °F) | 18°C (64.4 °F) |
| HIGH END TEMPERATURE | 25°C (77 °F) | 27°C (80.6 °F) |
| LOW END MOISTURE | 40% RH | 5.5°C DP (41.9 °F) |
| HIGH END MOISTURE | 55% RH | 60% RH & 15°C DP (59 °F DP) |

**Fuente:** Guía ambiental para Data Centers ASHRAE

Además de controlar estos parámetros sugeridos por la ASHRAE en lo que se refiere a temperatura y humedad, el sistema de monitoreo de seguridad física también será capaz de registrar el rango de cambio de la temperatura y humedad enviando alertas cuando encuentre variaciones considerables.

### 2.2.11 Alertas:

El sistema de monitoreo de seguridad física se basará en parámetros establecidos para las alarmas, es decir en qué valor o valores de un determinado sensor se debe activar una alarma y que además involucrará el método en cómo se va a enviar la alerta y por qué medio.

Para cada sensor, se determinará condiciones de funcionamiento aceptables debiéndose configurar umbrales para activar alarmas cuando las mediciones sobrepasen esas condiciones operativas. En condiciones normales, el sistema de monitoreo debería ser lo suficientemente flexible para configurar múltiples umbrales por sensor para alertar en los niveles de información, de advertencia, de alarma y de falla.

### 2.2.12 ASHRAE – Mejores Prácticas Eficiencia Energética

Según las recomendaciones de la ASHRAE en lo que respecta a eficiencia energética se deja atrás la filosofía de "más frio es mejor". Teniendo en cuenta estas mejores prácticas se puede conseguir un significativo ahorro de energía debido a una mejor eficiencia en el ciclo termodinámico de refrigeración. Nuestro proyecto que incluye sensores de temperatura y humedad distribuidos por zonas críticas dentro de la Central de Datos nos va a permitir saber qué zonas específicas necesitan más refrigeración que otras, lo que va permitir distribuir mejor el aire frio por esas zonas y por ende la temperatura de refrigeración. Esto implicará disminución de costos por consumo de energía.

### 2.2.13. "TIERS" En el diseño de un Centro de Datos. El ANSI/TIA-942

El estándar llamado ANSI/TIA-942 (Telecommunications Infrastructure Standard for Data Centers) que fue creado por miembros de la industria, consultores y usuarios, intenta estandarizar el proceso de diseño de los centros de datos. Este estándar está orientado a especialistas en la materia e ingenieros, anexando un sistema de clasificación de fiabilidad inventado por el Uptime Institute llamado: Los "Tiers".

El concepto de Tier nos indica el nivel de fiabilidad asociados a cuatro niveles específicos de disponibilidad, considerando que al mayor número de Tier, mayor disponibilidad y por ende mayor costo y tiempo asociado a la construcción. Hacemos referencia a este estándar para conocer en qué nivel actual de fiabilidad se encuentra la Central de Datos de la USAT según esta norma.

**Tabla Nº 4:** Tier 1 en Centro de Datos

| **Tier 1: Centro de Datos Básico: Disponibilidad del 99.671%** |
|---|
| • El servicio puede interrumpirse por actividades planeadas o no planeadas. |
| • No hay componentes redundantes en la distribución eléctrica y de refrigeración. |
| • Puede o no puede tener suelos elevados, generadores auxiliares o UPS. |
| • Tiempo medio de implementación, 3 meses. |
| • La infraestructura del Centro de Datos deberá estar fuera de servicio al menos una vez al año por razones de mantenimiento y/o reparaciones. |

**Fuente:** Norma ANSI-TIA 942

**Tabla Nº 5:** Tier 2 en Centro de Datos

| **TIER 2: Centro de Datos Redundante: Disponibilidad del 99.741%.** |
|---|
| • Menos susceptible a interrupciones por actividades planeadas o no planeadas. |
| • Componentes redundantes (N+1) |
| • Tiene suelos elevados, generadores auxiliares o UPS. |
| • Conectados a una única línea de distribución eléctrica y de refrigeración. |
| • De tres a seis meses para implementar. |
| • El mantenimiento de esta línea de distribución o de otras partes de la infraestructura requiere una interrupción de las servicio. |

**Fuente:** Norma ANSI-TIA 942

**Tabla Nº 6:** Tier 3 en Centro de Datos

| TIER 3: Centro de Datos Concurrentemente Mantenibles: Disponibilidad del 99.982% |
|---|
| • Permite planificar actividades de mantenimiento sin afectar al servicio de computación, pero eventos no planeados pueden causar paradas no planificadas. |
| • Componentes redundantes (N+1) |
| • Conectados múltiples líneas de distribución eléctrica y de refrigeración, pero únicamente con una activa. |
| • De 15 a 20 meses para implementar. |
| • Hay suficiente capacidad y distribución para poder llevar a cabo tareas de mantenimiento en una línea mientras se da servicio por otras. |

**Fuente:** Norma ANSI-TIA 942

**Tabla Nº 7:** Tiers en Centro de Datos

| **Tier 4: Centro de Datos Tolerante a fallos: Disponibilidad del 99.995%.** |
|---|
| • Permite planificar actividades de mantenimiento sin afectar al servicio de computación críticos, y es capaz de soportar por lo menos un evento no planificado del tipo 'peor escenario' sin impacto crítico en la carga. |
| • Conectados múltiples líneas de distribución eléctrica y de refrigeración con múltiples componentes redundantes (2 (N+1) significa 2 UPS con redundancia N+1). |
| • De 15 a 20 meses para implementar. |

**Fuente:** Norma ANSI-TIA 942

Gracias a estos parámetros podemos situar el nivel de fiabilidad del Centro de Datos de la USAT en el Nivel Básico, puesto que los servicios informáticos están propensos a interrumpirse por actividades no planeadas, como por ejemplo: por la falta de redundancia en el sistema de enfriamiento sumado a la ausencia de monitoreo eficaz y preventivo de seguridad física, el hardware puede sufrir daños al alcanzar temperaturas por encima de lo nominal.

### 2.2.14 Aplicación del Checklist de Evaluación al Centro de Datos

El Checklist es un conjunto de preguntas muy estudiadas que han de formularse de una manera flexible, empieza por un proceso interno de información a fin de obtener respuestas coherentes que a su vez permitan tener una correcta descripción de los puntos débiles y fuertes. Dicho esto, podemos utilizar el Checklist como una herramienta útil que pueda recolectar información relevante con el fin de poder evaluar la situación actual en lo referente a seguridad física de la Central de Datos de la USAT para en base a ello poder determinar si se encuentra en un marco en el que se cumpla con las normas, mejores prácticas o metodologías existentes en la actualidad.

Los checklist responden a dos tipos de calificación o evaluación:

**a) Checklist de rango.**

Contiene preguntas que se deben puntuar dentro de un rango preestablecido (por ejemplo del 1 al 5). El resultado es el promedio de las puntuaciones.

### b) Checklist Binario.

Está compuesto por preguntas con respuesta única y excluyente: Si o No. Aritméticamente hablando equivalen a 1 o 0, respectivamente.

Para nuestro caso utilizaremos los Checklist de rango por tener una mayor precisión en la evaluación que en los Checklist binarios.

### Obtención de Información para el análisis

Uno de los objetivos de este proyecto para tener un panorama de la realidad actual en seguridad física de la Central de datos es obtener información suficiente para corroborar si realmente se está trabajando de acuerdo a lo establecido, si se tiene coherencia en lo que se dice con lo que se hace y en base a eso poder realizar una evaluación y calificación efectiva de la seguridad física. Particularmente, es bueno saber que se tiene que tener mucho cuidado en la recopilación de evidencias, esto es fundamental para el proceso de análisis de la información.

A continuación podemos detallar algunos parámetros a considerar:

- ✓ Revisión de la estructura de Seguridad Física en el centro de datos.
- ✓ Revisión de documentos que referencien la seguridad física.
- ✓ Entrevista con el personal apropiado.
- ✓ Observación de operaciones y actuaciones de empleados

Es de suma importancia realizar una limpieza de datos, es decir seleccionar solo la información relevante para nuestro propósito relegando la información poco útil.

### Alcance de Pruebas:

Esta actividad tiene como objetivo definir el alcance que va a tener la prueba, esto con el fin de que dichas pruebas estén acordes a los controles de la entidad, decidiendo el grado de rigurosidad que van a tener nuestra pruebas realizadas.

Para determinar el alcance de nuestras pruebas debemos considerar el alcance mismo de la metodología el cual consiste en lo siguiente:

Revisión de dos perspectivas específicas y definidas de Seguridad Física a la Central de Datos, que consiste en los siguientes controles:

- ➢ Controles de Acceso.
- ➢ Controles Ambientales.

Una vez establecido el universo en el que se va a desarrollar la prueba, nos proporcionará uno de los puntos principales para llevar a cabo la revisión y evaluación del CPD: Entendimiento y/o actualización de las actividades de control y administración de riesgos existentes en la Central de Datos.

### Diseño de Pruebas para la Evaluación de las Actividades de Control realizadas.

El principal objetivo de este diseño de pruebas consiste en validar los controles que tiene implementado la organización para salvaguardar sus activos, aquí es donde vamos a comprobar si los controles actuales son eficaces y respaldan la continuidad del negocio de la posible materialización de un riesgo.
Todo esto se deriva de la consolidación de objetivos de COBIT e ISO realizada mediante un análisis previo que se detallan a continuación.

### CONTROL DE ACCESOS:

Se ha propuesto el siguiente objetivo de control de acceso al Centro de Datos:

**¿Se han aplicado e implementado diferentes restricciones de acceso físico para garantizar que solamente el personal autorizado pueda tener acceso a utilizar los recursos de la información?**

Para esto se pueden definir tres actividades de control:

### Actividad de Control N°1:

**Control de Accesos: Usuarios:** El acceso físico a las instalaciones del centro de datos esta monitoreado y está restringido para los usuarios que realizan labores cotidianas, requiriéndose autorización expresa del administrador de la red antes de que se otorgue el acceso.

En este aspecto, se pueden revisar los siguientes puntos:

- ✓ Existen definiciones de usuarios con privilegios de acceso al CPD
- ✓ Se cuenta con un registro de cada usuario que ingresa.
- ✓ Se realiza un registro de servicio y uso de los equipos informáticos del Centro de Datos.

### Control de Accesos N° 2:

**Control de Accesos: Personal Autorizado**: Un mecanismo de control de acceso físico se utiliza para restringir y registrar el acceso a las instalaciones del CPD.
En esta actividad los puntos a revisar son:

- ✓ El acceso es por previa autorización, siguiendo un proceso de reserva para accesar al CPD.
- ✓ Se cuenta con un mecanismo de identificación por medio de un dispositivo electrónico para autentificar la identidad de la persona.

- ✓ Se cuenta con un documento formal, expedido por el Director del área, con los nombres de cada personal autorizado para accesar al CPD.

**Controles Ambientales:**

Se considera el siguiente objetivo de control relacionado a los controles ambientales:

**¿Los recursos de información se encuentran protegidos contra riesgos ambientales y daños relacionados?**

**Actividad de Control N° 01:**

**Aire Acondicionado:** La gerencia o administración de TI monitorea periódicamente la eficacia de los mecanismos de control ambiental y evalúa el impacto comercial de las amenazas potenciales a los recursos físicos de la información (hardware).

Los puntos a revisar serían los siguientes:

- ✓ Se cuenta con un sistema de aire acondicionado separado que se dedica de forma exclusiva a enfriar el hardware del CPD.
- ✓ Se cuenta con un sistema redundante de aire acondicionado.
- ✓ La temperatura debe estar entre 15°C y 30°C, pero se recomienda que esté a 22 estables. (ASHRAE).

**Actividad de Control N° 02.**

**Sistema Contra Incendio:** La administración de TI ha implementado mecanismos adecuados de supresión y detección de incendios/humo.

Se revisaron los siguientes puntos:

- ✓ Se cuenta con un sistema de protección contra incendios automático.
- ✓ Se ha capacitado al personal del CPD para el manejo de extintores y se ha aprobado.
- ✓ Existen estrategias para la evacuación.

**Actividad de Control N° 03.**

**Ambiente General**: Las condiciones ambientales del centro de datos (temperatura y humedad) son vigiladas y reguladas.

Los puntos revisados fueron son los siguientes:

- ✓ La Monitorización del estado ambiental y del equipo de enfriamiento se hace de forma presencial o automática.
- ✓ Existe iluminación adecuada.

A todo esto se pudo estructurar un diseño de pruebas considerando como base cuatro objetivos de control de COBIT los cuales se adaptaron al plano de seguridad física. En este diseño se contemplaron las siguientes pruebas:

- ✓ El control implantado debe ser coherente de acuerdo al tipo de negocio.
- ✓ La organización realiza análisis para adquirir los controles de su seguridad física.
- ✓ Se concientizó al personal mediante capacitación de la importancia del control.
- ✓ ¿Se entienden y se administran los riesgos a los que se encuentran sometidos los activos dentro del CPD?
- ✓ ¿La seguridad física cubre las necesidades actuales del negocio?
- ✓ ¿Se cuenta con una planeación enfocada en la seguridad física?

- **Monitorear y Evaluar:**
  - ✓ ¿Se mide el desempeño de la seguridad para detectar los problemas antes de que sea tarde?
  - ✓ ¿Se puede garantizar que los controles internos son efectivos?
  - ✓ Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño.

- **Entregar y dar Soporte:**

  - ✓ ¿Está optimizada la seguridad física?

  - ✓ ¿La seguridad física hace que se trabaje de manera productiva y segura?

Después de tomar en cuenta y actividades de control se puede determinar que contamos con una prueba completa que nos brindará la suficiente información para la evaluación y calificación del CPD.

### 2.2.15 Análisis de Plataformas de Hardware Libre Existentes

A continuación se describe las principales plataformas de hardware libre que se encuentran en la actualidad, cada una con sus funcionalidades, ventajas y desventajas. Se sustenta tecnológicamente el uso de la plataforma Arduino para implementar nuestra propuesta de sistema de seguridad física adaptable para un entorno de Central de Datos.

Se puede mencionar que en la actualidad existen diversos proyectos que utilizan estas plataformas de hardware libre en diferentes ramas de la ciencia como en robótica, educación, etc. Nos permitimos sobresalir la idea de adaptar esta tecnología a un entorno crítico como es una Central de Datos, con metodologías y análisis de datos respaldadas por normas y buenas prácticas en lo referente a seguridad física, convergiendo con los conocimientos sólidos de electrónica y diseño de prototipos de este tipo de tecnologías.

Si bien es cierto que Arduino y Raspberry Pi evidentemente son unas de las plataformas de hardware libre más conocidas en la actualidad; podemos encontrar un abanico de iniciativas en entorno de hardware libre que vale la pena mencionar.

**FIGURA Nº 6.** Raspberry Pi

**Fuente:** Rasperry PI [imagen]. 2013. (accedido el 04 de marzo del 2014)

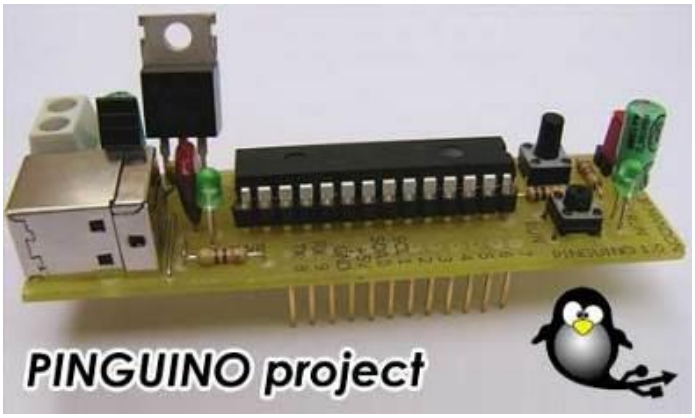
El Raspberry Pi es un micro ordenador de bajo costo desarrollado en el Reyno Unido por la Fundación Raspberry Pi, con el principal objetivo de impulsar e estimular la enseñanza de ciencias de la computación de las escuelas.
Dentro de sus características de hardware más relevantes se pueden mencionar: Un procesador de la prestigiosa firma Broadcom de cuyo modelo es el BCM2835. La velocidad de este procesador bordea los 700Mhz. También podemos destacar la presencia de un procesador gráfico VideoCore IV y 512MB de Memoria Ram. Posee un puerto USB, entradas de video y salidas de video RCA y HDMI. Como principal desventaja podemos describir que no cuenta con reloj en tiempo real.
En la siguiente tabla consideramos las especificaciones técnicas globales de esta plataforma.

**Tabla Nº 8:** Características de la Placa Raspberry Pi.

|  |
|---|
| **Características de las placas Raspberry Pi** |
| • Procesador Broadcom BCM2835 de 700MHz ARM1176JZFS con FPU y Videocore 4 GPU |
| • GPU que proporciona una tecnología Open GL ES 2.0, hardware acelerado de OpenVG, y admite imágenes de alta resolución 1080p30 H.264 |
| • La GPU tiene una capacidad de 1 Gpixel/s, 1.5 Gtexel/s o 24 GFLOPs con filtrado e infraestructura DMA |
| • 256 MB de memoria RAM (modelo A) y 512 MB para el modelo B |
| • Arranque a través de la tarjeta SD, ejecutando la versión de Linux |
| • 1 puerto USB 2.0 (modelo A), 2 puertos USB 2.0 (modelo B) |

**Fuente:** Rasperry PI [imagen]. 2013. (accedido el 04 de marzo del 2014)

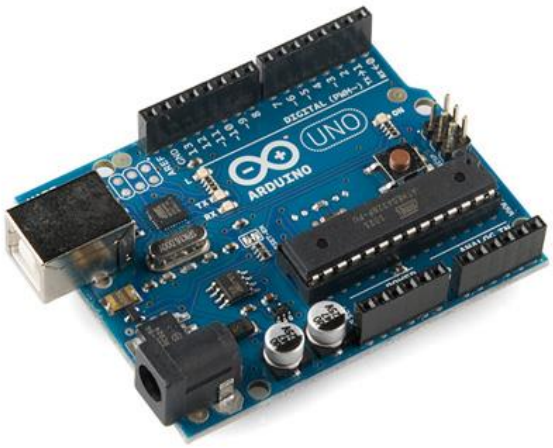
**FIGURA Nº 7:** Pingüino




**Fuente:** Pinguino [imagen]. 2010. (accedido el 05 de marzo del 2014)

La plataforma pingüino es una plataforma basada en Microcontrolador PIC similar en parte a Arduino.
Pinguino se basa en un microcontrolador 18F2550 presentado sobre una placa que permite insertarla directamente sobre una protoboard (tarjeta de pruebas). Sorprende un poco ver que se utiliza un PIC y no un AVR, aunque el PIC usado (18F2550) incorpora USB por hardware.

**FIGURA Nº 8**: Plataforma Electrónica Arduino

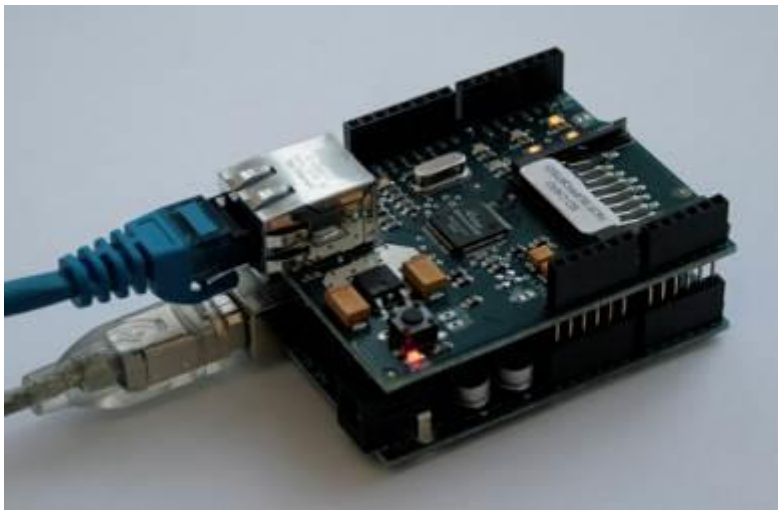



**Fuente:** Arduino UNO [imagen]. 2013. (accedido el 18 de febrero del 2014)

Arduino se basa en una plataforma denominada open hardware o hardware libre en la cual en una pequeña placa de circuito impreso (PCB) reúne los componentes necesarios para conectar con el mundo exterior y hacer funcionar un microcontrolador Atmega. En la actualidad existen varios modelos de sistemas Arduino que van variando de microcontrolador, siendo los primeros el Atmega8 y el Atmega168. Al ser hardware libre puede utilizarse sin inconvenientes para desarrollar cualquier tipo de proyecto sin tener que adquirir ningún tipo de licencia.

En lo que respecta a la comunicación del Arduino con el ordenador, se realiza por Puerto Serie (RS232), Puerto USB, o por el sistema ICSP (In Circuit Serial Program). Para el proyecto se conectará el Arduino vía USB para la programación respectiva desde su mismo entorno de programación. Asimismo, existe la posibilidad de interconectar diversos "shield" que son componentes que amplían de una manera significativa los usos que se le puede dar a esta plataforma. Una de las shield que vamos a utilizar es la Shield Ethernet que nos va a permitir conectarnos a internet. Esta Shield Está basada en el chip ethernet Wiznet W5100 (datasheet). El Wiznet W5100 provee de una pila de red IP capaz de TCP y UDP. Soporta hasta cuatro conexiones de sockets simultáneas. Usa la librería Ethernet para escribir programas que se conecten a internet usando la shield.

**FIGURA Nº 9**: Conexión de Arduino con la shield Ethernet



**Fuente:** Arduino UNO [imagen]. 2013. (accedido el 18 de febrero del 2014)

## Características del micro de la placa Arduino UNO

En la actualidad existen varios modelos de placas Arduino, cada una con diferentes características y cualidades las cuales tuvimos que conocer para decidir la que más se ajuste a nuestro proyecto. El modelo estándar utilizado en nuestro proyecto es el Arduino Uno Rev.3 que fue fabricada el año 2010 y que tiene el mayor número de compatibilidades en la interconexión de diversidad de hardware (shields) que integramos en nuestro proyecto.

### El encapsulado del Microcontrolador

Actualmente existen dos tipos de encapsulados para las placas Arduino con dos formatos distintos, uno de ellos es el llamado SMD ("Surface Mount Device") y el otro llamado DIP ("Dual In-line Package"). Estos dos difieren en que en el primero los componentes están soldados en la superficie de la placa utilizando una tecnología llamada de "Montaje Superficial", mientras que en el segundo formato, los componentes están soldados a la placa mediante una serie de patillas metálicas que se pueden desoldar (separar) fácilmente y que permiten, por ejemplo, la sustitución del microcontrolador por otro.

### Modelo del Microcontrolador:

La placa Arduino Uno utilizada en nuestro proyecto incorpora el microcontrolador ATmega 328P del fabricante Atmel. Es importante puntualizar que la letra P situada al final del modelo hace referencia a la incorporación de la tecnología "Picopower" (Propiedad también de Atmel), la cual permite un consumo eléctrico sensiblemente menor comparándolo con otro microcontrolador cuyo modelo no tenga incluida esta letra. Trabajar con un voltaje menor y consumir menos corriente hacen que esta tecnología Picopower sea relevante y ventajosa frente a otras tecnologías de microcontroladores. El microcontrolador ATmega 328P al igual que otra placas Arduino posee una arquitectura AVR, desarrollada por Atmel, que a su vez compite con otras arquitecturas como por ejemplo la PIC del fabricante Microchip.

### Las Memorias del Microcontrolador

Es relevante tener en cuenta el tipo y la cantidad de memoria presente en el interior de un Microcontrolador. En el caso del ATmega328P tiene una capacidad de 32KB.

En los tipos de memoria que podemos destacar son:

### Memoria Flash:

Esta memoria de tipo persistente tiene la función de almacenar de forma permanente el programa que ejecuta el microcontrolador.
En los microcontroladores que vienen incluidos en la placa Arduino no podemos utilizar toda la capacidad de la memoria flash porque existen 512 bytes ("llamado bootloader block") ocupados por un código pre-programado de fábrica llamado gestor de arranque o bootloader.

### Memoria SRAM:

Los datos que suelen tener un contenido variable a lo largo del tiempo son alojados en una memoria volátil llamada SRAM. Independientemente del tipo de dato, los valores siempre serán eliminados siempre y cuando se deje de alimentar eléctricamente el microcontrolador. En el caso del ATmega328 esta memoria tiene una capacidad de 2KB

### Memoria EPROM:

Los datos en los que se desea que permanezcan grabados una vez apagado el microcontrolador para ser utilizados en posteriores reinicios son almacenados en este tipo de memoria persistente. En el caso del ATmega 328P esta memoria tiene una capacidad de 1KB.

### Protocolos de Comunicación I2C / TWI y SPI:

La transmisión de un conjunto de datos desde un componente electrónico a otro se puede realizar de múltiples formas. Una de ellas es estableciendo una comunicación "serie" donde la información es transmitida bit a bit por un único canal, enviando por tanto un solo bit en cada momento. Por el contrario, otra manera de transferir datos es por la llamada comunicación paralela, en la cual se envían varios bits simultáneamente, cada uno por un canal separado y sincronizado con el resto.
El microcontrolador utiliza el sistema de comunicación serie, a través de sus pines de E/S, para transmitir y recibir órdenes y datos hacia o desde otros componentes electrónicos. Sin embargo no necesariamente se utilizan estos tipos de comunicación. Existen muchos protocolos y estándares diferentes basados todos ellos en la transferencia de información en serie, con una implementación distinta pero con detalles técnicos específicos (modo de sincronización, velocidad de transmisión, tamaño de los paquetes de datos, etc).
Los estándares más importantes en lo que el ATmega328P es capaz de comprender y por lo tanto, los que podría utilizar para contactar con una gran variedad de periféricos son:

**I2C:**
(Inter-Integrated Circuit), también conocido con el nombre de TWI (Two-wire), literalmente "dos cables" en inglés), es un sistema cuya principal característica es utilizar dos líneas para transmitir la información. Estas líneas son las llamadas "SDA" que sirven para transferir los datos y otra llamada "SCL" la cual se encarga de llevar la señal de reloj. En la práctica también se necesitan dos líneas más que son la de alimentación y la de tierra.

**SPI:**
(Serial peripheral Interface): Al igual que el sistema I2C, este sistema de comunicación es un estándar que permite controlar a cortas distancias casi cualquier dispositivo digital que acepte un flujo de bits serie sincronizado (regulado por un reloj). Un dispositivo conectado al bus SPI puede ser maestro o esclavo, donde el primero es el que inicia la transmisión de datos y además genera la señal de reloj.

# III. MATERIALES Y MÉTODOS

## 3.1. Diseño de Investigación:

### 3.1.1) Tipo de Estudio y diseño de Contrastación de hipótesis

Debido a que no se realizará operación de variables independientes, esta investigación se enmarca dentro de un diseño cuasi-experimental.
Los diseños cuasi-experimentales en su esencia, son esquemas de investigación no aleatorios. Esta no aleatorización las diferencia de los diseños experimentales ya que no es posible establecer de forma exacta la equivalencia inicial de los grupos. Sin embargo Cook y Campbell (1966) consideran los cuasi-experimentos como una alternativa válida a los experimentos de asignación aleatoria, en aquellas situaciones donde se carece de pleno control experimental. Por otro lado, con el solo propósito de consolidar nuestro tipo de estudio y diseño de contratación de hipótesis hacemos referencia a la definición que incluye las características más relevantes de la metodología cuasi-experimental ofrecida por Pedhazur y Schmelkin (1991) que consideran a esta metodología como una investigación que posee todos los elementos de un experimento, excepto que los sujetos no se asignan aleatoriamente a los grupos. Como consecuencia de la ausencia de aleatorización nosotros como investigadores nos enfrentamos con la tarea de identificar y separar los efectos de los tratamientos del resto de factores que afectan a la variable dependiente.

Específicamente, para el diseño de contrastación de la hipótesis utilizaremos uno de los métodos que consiste en un pretest-postest o lo equivalente a decir una medición antes y después con grupo de control. Este método sigue tres fases bien definidas:

Antes de la aplicación de la variable independiente se realiza una medición previa de la variable dependiente a ser utilizada. Luego se aplica un estímulo que viene a ser la variable dependiente y por último se realiza una nueva medición de la variable dependiente después de la aplicación de la variable independiente.

Se definirán los actores involucrados en las actividades actuales de seguridad física considerando los procesos actuales tal y como son, es decir, sin el sistema propuesto y luego se realizara una medición de los indicadores definidos. Posteriormente se determinaran los valores para los indicadores cuando el sistema propuesto se encuentre en marcha. Como último procedimiento se efectuará la contrastación de la situación antes y después y se evaluará si realmente ha mejorado el proceso y lo que involucra a seguridad física de la Central de Datos de la USAT.

### 3.1.2) Población, muestra de estudio y muestreo

La población está conformada por todos los equipos de cómputo instalados en la Central de Datos que brindan los servicios informáticos a la USAT compuestos por dos zonas. La zona de servidores y swicth conformada por 20 servidores y 10 switch administrables y la zona de Alimentación ininterrumpida compuesta por dos dispositivos de alimentación de energía eléctrica (UPS), siendo un total de 32 equipos

### 3.1.3) Muestra

Para un cálculo de muestras en poblaciones se utiliza la siguiente fórmula:

$$n = \frac{Z^2 * P * Q * N}{(N-1) * e^2 + (Z^2 * P * Q)}$$

Sin embargo, debido a que todos los equipos informáticos instalados dentro de la Central de Datos interactúan para ofrecer los servicios informáticos, se trabajó con toda la población.

### Muestreo

En este proyecto se trabajó con toda la población y se calculará en base a cada uno de los indicadores establecidos.

### 3.1.4) Métodos, técnicas e instrumentos de recolección de datos.

**Tabla 9.** Técnicas para la Recolección de Datos

| MÉTODOS | TÉCNICAS E INSTRUMENTO |
|---|---|
| **Entrevistas** | Comunicación abierta (con el Director de TI) |
| **Análisis** | Documentación técnica de los equipos informáticos. |
| **Observación** | Verificación in-situ de los equipos en la Central de Datos. |

### 3.1.5) Hipótesis

La implementación de un sistema de monitoreo de seguridad física en plataforma libre de componentes electrónicos mejora la gestión de los niveles de continuidad de los servicios informáticos de la Central de Datos USAT.

### 3.1.6) Variables e Indicadores

- **Variable Independiente:**

Sistema de Monitoreo de seguridad física en plataforma libre de componentes electrónicos.

- **Variable Dependiente:**

Gestión de los Niveles de continuidad de los equipos informáticos.

**- Indicadores:**

- Costos de inversión que implica la adquisición de equipos informáticos nuevos para la Central de Datos.

- Cantidad de equipos que sufrieron daños por problemas de seguridad física.

- Número de usuarios administrativos y estudiantil satisfechos por la continuidad de los servicios informáticos proporcionada por la Central de Datos según el enfoque de seguridad física.

- Ciclo de vida útil de los equipos informáticos en la Central de Datos con metodología tradicional en seguridad física vs sistema de monitorización automatizado de seguridad en física.

## Tabla Nº 10. Operacionalización de Variables

| OPERACIONALIZACIÓN DE VARIABLES | | | | |
|---|---|---|---|---|
| VARIABLE | DESCRIPCIÓN | INDICADOR | INSTRUMENTO | OPERACIONALIZACIÓN |
| Costos de Inversión | Costos de Inversión que implica la adquisición de equipos informáticos Nuevos por reposición | Costos anuales por la reposición de equipos informáticos | Pagos a Proveedores | ∑ de Pagos a proveedores según cronogramas |
| Seguridad física | Cantidad de equipos que sufrieron daños por problemas de seguridad física | Índice de equipos averiados por año | Encuestas y entrevistas | ∑ Número equipos informáticos en la actualidad ∑ Número de equipos informáticos en el pasado. |
| Nivel de Satisfacción | Número de usuarios administrativos y estudiantiles satisfechos por la continuidad de los servicios informáticos proporcionados por el CPD según el enfoque de seguridad física | Porcentaje de Usuarios satisfechos | Encuestas y entrevistas | Resultado de encuesta actual / Resultado de encuesta anterior |
| Aumentar Ciclo de vida útil de equipos informáticos | Ciclo de vida útil de los equipos informáticos en la Central de Datos con metodología tradicional en seguridad física vs sistema de monitorización automatizado de seguridad física. | Porcentaje diferencial del ciclo de vida útil de los equipos de cómputo | Encuestas y entrevistas | Resultado de encuesta actual / Resultado de encuesta anterior |

### 3.1.7 Plan de Procesamiento para el análisis de datos

Para el análisis de datos sobre el entorno de análisis y gestión de riesgos de los sistemas de información se utilizará Checklist sugeridos por COBIT y la Norma ANSI-TIA942. En lo que respecta al producto acreditable, los datos de los valores de temperatura, humedad relativa, movimiento, etc. se obtendrán y se procesarán sobre la plataforma LAMP instalada en una miniPC (Pcduino).

## 3.2. Metodología de desarrollo del producto acreditable.

El desarrollo de este proyecto se sustentó en la Metodología de Desarrollo de Hardware Libre elaborada por la Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL).

La metodología consta de tres procesos bien definidos y estructurados. En el proceso de conceptualización se busca delimitar los alcances que se quiere para el proyecto en estudio, luego en el proceso de administración lo que se busca es llevar a cabo la planificación para el diseño, fabricación y pruebas del dispositivo. Por último, en el proceso de desarrollo se especifican los pasos que en principio se deben cumplir, dependiendo de la naturaleza del dispositivo.

La Fundación CENDITEL cede permisos de utilización, modificación y distribución de la documentación que respalda la Metodología de Desarrollo de Hardware Libre bajo los términos establecidos en la licencia de documentación GFDL, Versión 1.2 de la Free Software Foundation.

**FIGURA 10: Plataforma de Desarrollo de Hardware Libre**


Fuente: Fundación Cenditel – Metodología de Desarrollo de Hardware Libre

# IV. RESULTADOS

Aquí abordaremos todas las fases desarrolladas para la obtención del producto acreditable del Proyecto de Tesis "Sistema de Monitoreo de Seguridad Física en Plataforma Libre de Componentes Electrónicos para asegurar la Gestión de los Niveles de Continuidad de los Servicios Informáticos de la Central de Datos USAT", sustentándose en la Metodología de Desarrollo de Hardware Libre elaborada por la Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL).

## METODOLOGIA DE DESARROLLO DE HARDWARE LIBRE

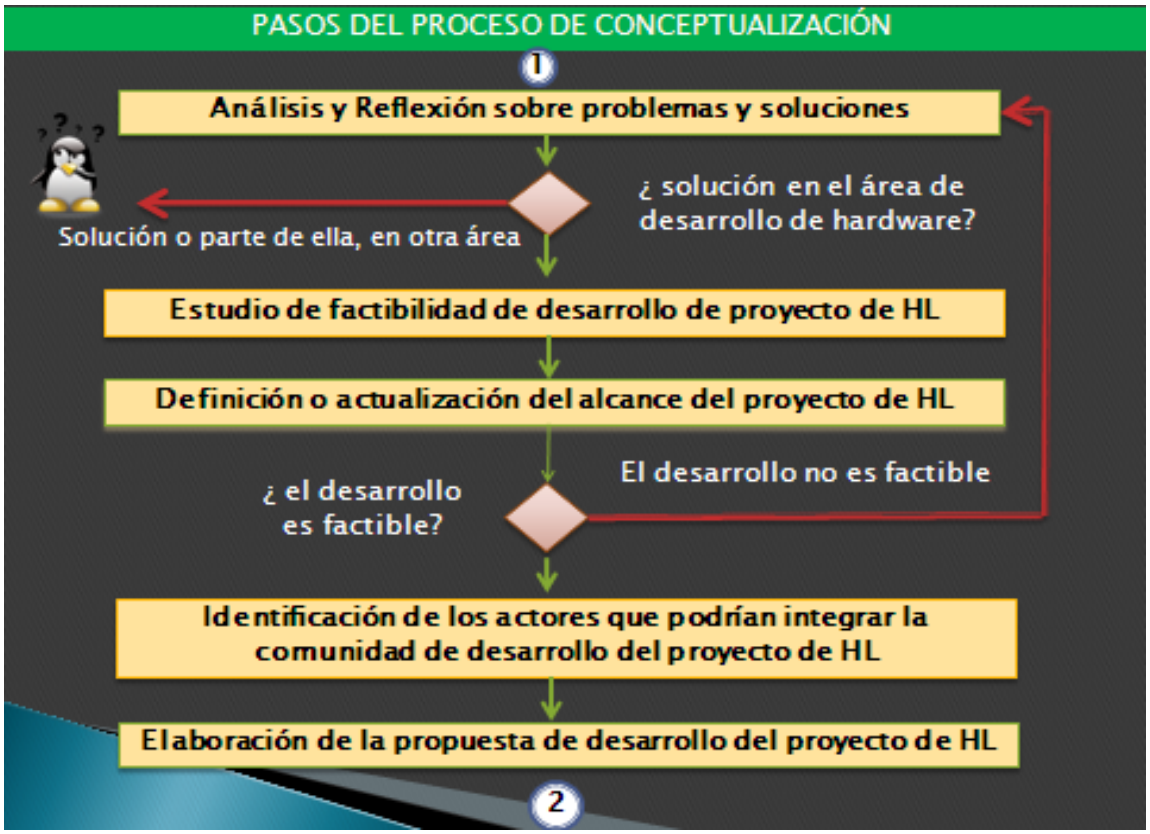
La metodología consta de tres procesos bien definidos y estructurados. En el proceso de conceptualización se busca delimitar los alcances que se quiere para el proyecto en estudio, luego en el proceso de administración lo que se busca es llevar a cabo la planificación para el diseño, fabricación y pruebas del dispositivo. Por último, en el proceso de desarrollo se especifican los pasos que en principio se deben cumplir, dependiendo de la naturaleza del dispositivo.

**FIGURA 11: Plataforma de Desarrollo de Hardware Libre**


Fuente: Cenditel. Metodología de Desarrollo de Hardware Libre.

## 4.1 Proceso de Conceptualización del proyecto

**FIGURA 12: Pasos del Proceso de Conceptualización**




Fuente: Cenditel. Metodología de Desarrollo de Hardware Libre

### 4.1.1. Análisis y Reflexión sobre Problemas y Soluciones:

En esta fase se han analizado los problemas y necesidades que tiene la organización en lo que respecta a asegurar la continuidad de sus servicios informáticos, asimismo sus posibles soluciones desde perspectivas tanto de hardware como de software, ambos libres.
Para esto se ha creído conveniente mostrar un diagrama causa efecto de la situación problemática actual:

FIGURA 13: Situación problemática


Tal como se puede apreciar, el incremento significativo de la población estudiantil en los últimos años ha repercutido en el crecimiento de servidores instalados en la Central de Datos con el fin de satisfacer la demanda de servicios informáticos dentro de la organización. Debido a este incremento de servidores que se traduce en nuevas tecnologías incorporadas, las demandas de enfriamiento también han aumentado, por lo que la forma actual de monitorear el entorno de la Central de Datos plantea deficiencias. Actualmente en la Central de Datos existen equipos informáticos tales como servidores, switch, routers, etc, instalados en racks distribuidos en todo el espacio del Data Center. Solo se controla valores ambientales como la temperatura y humedad con un solo equipo doméstico instalado en una zona determinada. No se cuenta con lecturas automáticas de estos valores en determinados ambientes del Centro de Datos, ni tampoco se cuenta con información sobre accesos físicos significando esto un riesgo potencial.

Es necesario automatizar estas lecturas de factores ambientales así como recibir información sobre posibles intrusiones de una forma eficaz, de forma continua y centralizada. El sistema propuesto tendrá que interactuar con sensores, almacenar el valor de estos a manera de históricos en una base de datos local y mostrar una interfaz gráfica, configurable y de fácil utilización para monitorear de una manera más fiable estos factores. Sin embargo, no solo es necesario

monitorear sino que el sistema debe tomar acción, activando algún mecanismo de defensa contra los riesgos de temperatura y humedad elevados y contra intrusos siguiendo las Normas, Estándares y Buenas Prácticas vigentes en la actualidad.

### 4.1.2 Estudio de Factibilidad de Desarrollo del proyecto de Hardware Libre.

Después de definir la problemática anteriormente descrita y establecer las causas que ameritan una solución automatizada, es pertinente realizar un estudio de factibilidad para determinar la infraestructura tecnológica y la capacidad técnica que implica la implantación del sistema en cuestión, así como los costos - beneficios y el grado de aceptación que la propuesta genera en la organización. Este análisis nos permitió determinar las posibilidades de diseñar el sistema propuesto y su puesta en marcha. Los aspectos tomados en cuenta para este estudio no solo abarcó aspectos como disponibilidad del equipo de trabajo, urgencia con la que se requiere el desarrollo del hardware, tal como sugiere esta metodología sino que además se consideraron aspectos como Factibilidad Técnica, Factibilidad Económica, Análisis Costo-Beneficios y Factibilidad Operativa.

### a) Factibilidad Técnica:

De acuerdo a la tecnología necesaria para la implementación de un sistema de seguridad física en plataforma libre de componentes electrónicos en el Data Center de la USAT, se evaluó dos enfoques: Hardware y Software.

### Hardware

Especificaciones y requerimientos del hardware utilizado que aseguran un óptimo desempeño del producto acreditable.

**TARJETA ARDUINO UNO**

FIGURA Nº 14. Plataforma de hardware libre Arduino

**Fuente:** Arduino UNO [imagen]. 2013. (accedido el 20 de febrero del 2014)

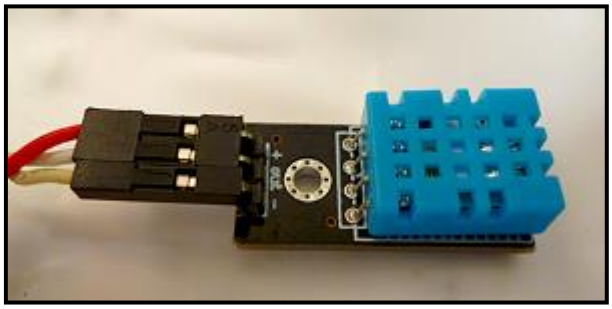
**TABLA Nº 11. Características técnicas de la placa Arduino UNO**

| **Microcontrolador** | **Atmega328** |
|---|---|
| Tensión de Funcionamiento | 5V |
| Voltaje de entrada (recomendado) | 7-12V |
| Voltaje de entrada (límites) | 6-20V |
| Digital I/O Pins | 14 |
| Pines de entrada analógica | 6 |
| EEPROM | 1kb |
| Velocidad de reloj | 16Mhz |

**Fuente:** Arduino UNO. 2014 (accedido el 20 de febrero del 2014)

## a.1) Sensor de Temperatura y Humedad

**FIGURA Nº 15.** Sensor de Temperatura y Humedad DHT11



Fuente: Foto tomada al sensor utilizado en el proyecto

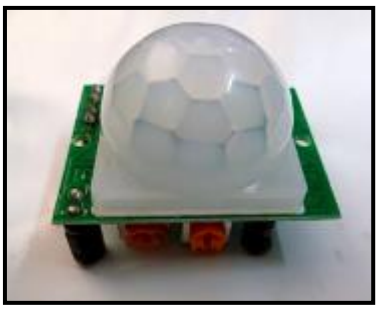
**TABLA 12. Características técnicas del sensor DHT11**

| **Parámetro** | **Sensor DHT11** |
|---|---|
| Alimentación | 3vdc – 5vdc |
| Señal de salida | Digital |
| Rango Medida Temperatura | De 0 a 50 °C |
| Precisión Temperatura | ±2 °C |
| Rango de Medida Humedad | De 20% a 90% RH |
| Precisión Humedad | 4% RH |
| Tiempo de sensado | 1s |

Fuente: D-Robotics UK. 2014 (accedido el 21 de febrero del 2014)

## a.2) Sensor de Movimiento

**FIGURA 16. Sensor de Movimiento PIR HC-SR501**



Fuente: Foto tomada al sensor utilizado en el proyecto

**TABLA 13. Características técnicas del Sensor PIC HC-SR501**

| **Procesador de señal** | Sanyo Genius BISS0001 |
|---|---|
| Voltaje | 5V-20V |
| Consumo | 65Ma |
| Salida TTL | 3.3V, 0V |
| Tiempo de respuesta | Ajustable 0.3sec – 10 min. |
| Tiempo de espera | 0.2 seg. |
| Radio de alcance | Menos de 120º |
| Temperatura | -15 - +70ºC |
| Dimensiones | 32*24mm |

**Fuente:** Sensor de Movimiento PIR [imagen]. 2013. (accedido el 18 de febrero del 2014)

## a.3) Actuador: Módulo Relé

**FIGURA Nº 17. Modulo Relé de 4 Canales**


Fuente: Foto tomada al módulo relé

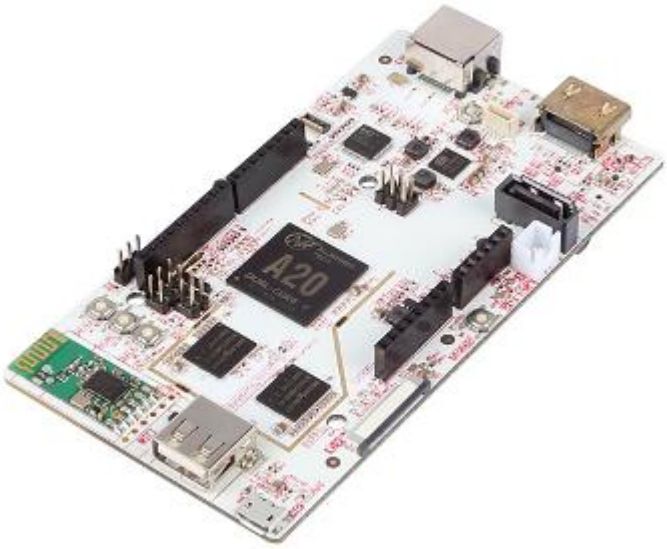
**TABLA 14. Características técnicas del Módulo Relé**

| | |
|---|---|
| Canales | 4 |
| Alimentación | 5Vcc |
| Consumo de dispositivos controlados | Hasta 10A / 250VAC |
| Protección | Por Optoaclopadores |
| Interfaz | Arduino, AVR, PIC |

Este módulo relé sirve de interface para la activación de extractores de aire que actúan o se activan cuando los valores de temperatura y humedad excedan los parámetros establecidos.

a.4)**PcDuino** (Mini Pc con interfaces compatibles con Arduino)

**FIGURA Nº 18. Mini PC PcDuino v2**




**Fuente:** PcDuino V2 [imagen]. 2013. (accedido el 01 de marzo del 2014)

**TABLA Nº 15. Características técnicas de PcDuino v2**

| | |
|---|---|
| CPU | Allwinner A10 / 1Ghz ARM Cortex 8 |
| GPU | OpenGL ES2.0, OpenVG 1.1 Mali 400 core |
| DRAM | 1GB |
| Storage | 2GB Flash (4GB after 2/1/2014), microSD card (TF) slot for up to 32GB |
| Video | HDMI |
| OS Support | Lbuntu 12.04 / Android |
| ExtensionInterface | Arduino (TM) Headers |
| NetworkInterface | 10/100Mbps RJ45<br>WiFi |
| Power | 5V, 2000Ma |

**Fuente:** PcDuino V2. 2013. (accedido el 01 de marzo del 2014)

**Software**

- ✓ Software IDE Arduino Versión 0018 (29/01/2010) – Software Libre.

  Idioma: Español

  Descarga Gratuita:
  http://arduino.googlecode.com/files/arduino-0019.zip

  Tamaño del archivo: 85MB

- ✓ Sistema Operativo Lubuntu

  Software Libre

  Versión: 12.04

  Idioma: Español

  Descarga Gratuita:
  https://s3.amazonaws.com/pcduino/Images/2013-11-26/pcduino_ubuntu_20131126.7z

  Tamaño del archivo: 289MB

- ✓ Apache HTTP Server

  Versión: 2.4.9 (released 2014-03-17)

  Software Libre.

- ✓ MySQL

  Versión 5.6

  Software Libre.

- ✓ PHP

  Versión: 5.4.30

  Software Libre.

### b) Factibilidad Económica

**TABLA Nº 16. Costos del total de hardware utilizado en el proyecto**

| HARDWARE | PRECIO EN S/ | CANTIDAD | TOTAL EN S/. |
|---|---|---|---|
| **Tarjeta Arduino UNO** | 85.00 | 01 | 85.00 |
| **Tarjeta Shield Ethernet** | 85.00 | 01 | 85.00 |
| **Sensor de Temperatura y Humedad DHT11** | 25.00 | 04 | 100.00 |
| **Sensor de Movimiento PIR** | 25.00 | 01 | 25.00 |
| **Módulo Relé de 4 canales** | 30.00 | 01 | 30.00 |
| **Pcduino** | 265.00 | 01 | 265.00 |
| **Case para Arduino** | 50 | 01 | 50 |
| **Case para PcDuino** | 50 | 01 | 50 |
| **Equipo UPS 500va /250w** | 130 | 01 | 130 |
| **Cables, accesorios y otros** | 70 | 01 | 70 |
| **TOTAL en S/.** | | | **890.00** |

### c) Factibilidad Operativa

#### c.1) Plan de implantación del sistema de monitoreo de seguridad física en el Centro de datos de la USAT.

**1. Autorización para implantación del proyecto.**

- Se cuenta con autorización del Director de Tecnologías de la Información de la USAT.

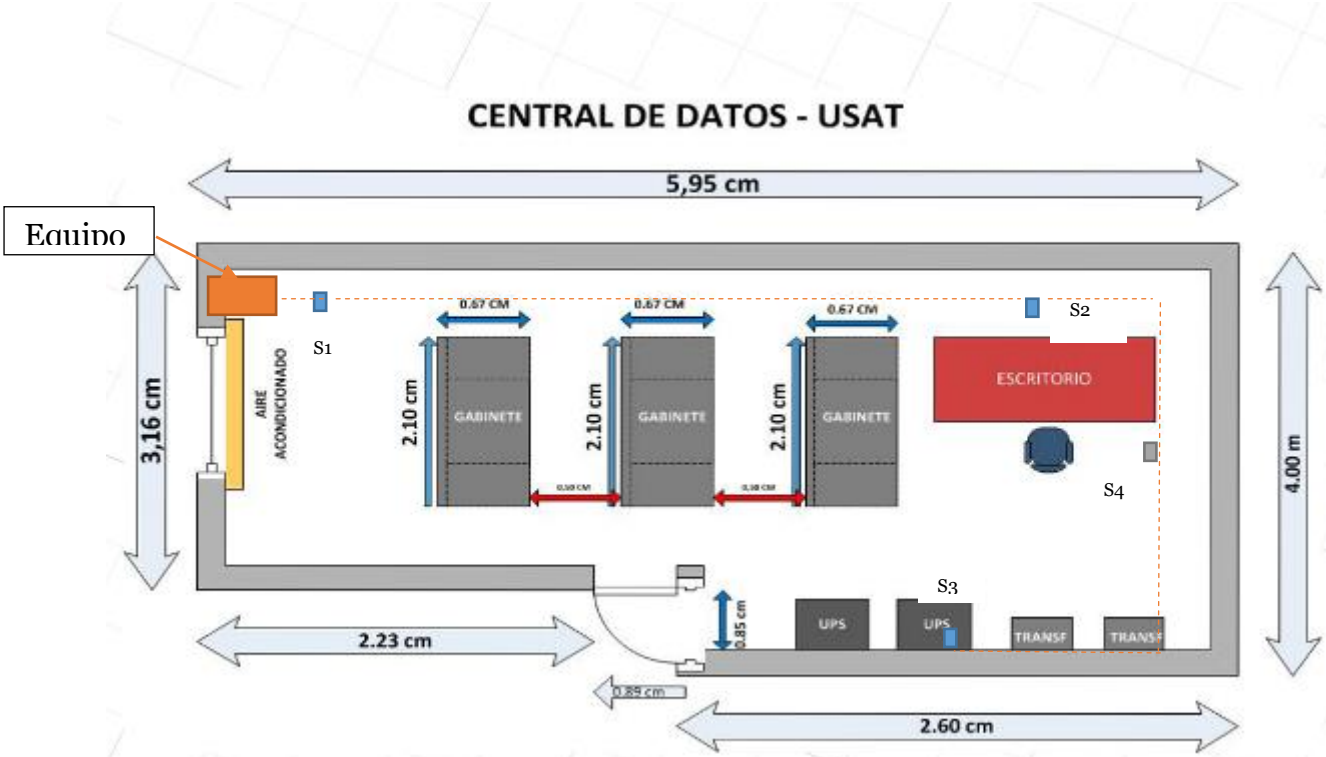
## 2. Adecuación de las instalaciones:

- Se cumple con las siguientes condiciones de adecuación:
  - Acceso a las instalaciones del Centro de Datos
  - Suministro eléctrico adecuado
  - Instalación eléctrica adecuada
  - Suministro de corriente interrumpida
  - Puntos de red operativos

## 3. Instalación y configuración del equipo

El sistema será instalado dentro del Centro de Datos, los sensores de temperatura y humedad serán instalados por zonas, el sensor de temperatura será instalado en una zona estratégica dentro del Data Center. Tanto el servidor (pcduino), como la tarjeta Shield Ethernet serán configurados con sus respectivas IP´s dentro de una misma Vlan.

**FIGURA Nº 19: Ubicación de la Instalación del Sistema de**




**Monitoreo**

-

**Leyenda:**

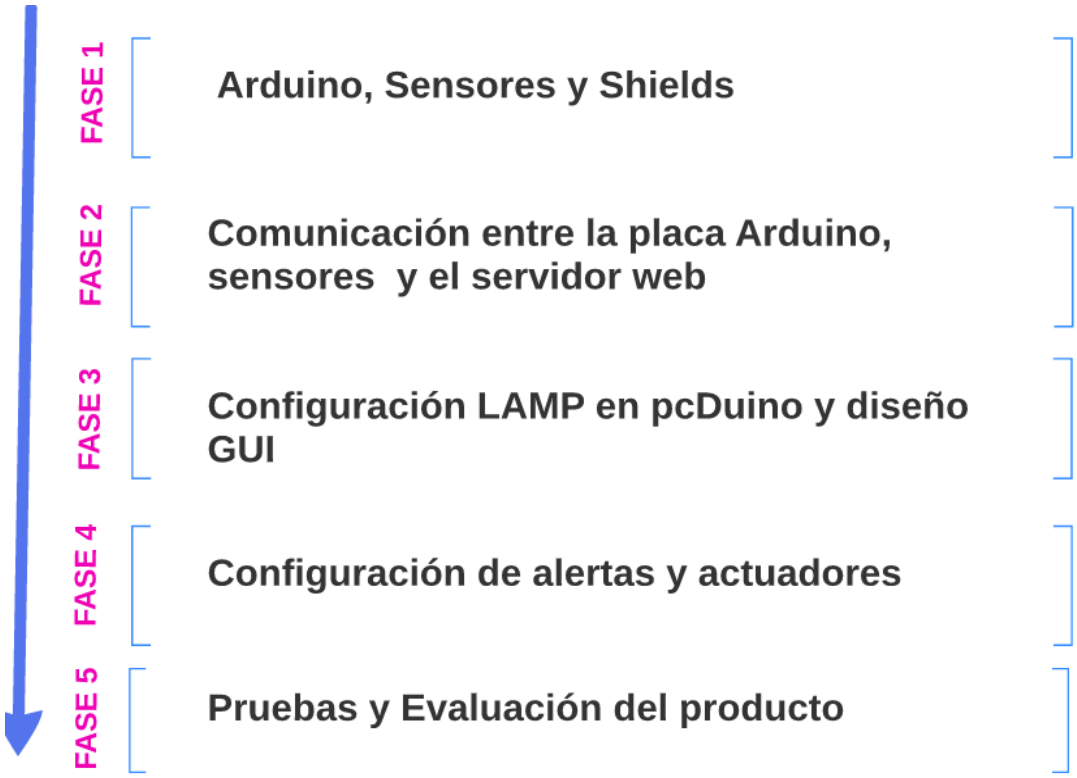
**Equipos (Plataforma Arduino + Pcduino)**
**S1: Sensor de Temperatura y Humedad 1**
**S2: Sensor de Temperatura y Humedad 2**
**S3: Sensor de Temperatura y Humedad 3**
**S4: Sensor de Movimiento**

## 4. Pruebas de Funcionalidad:

Se realizaron pruebas de funcionalidad en ambientes cuyas temperaturas oscilaban entre 18 y 24ºC y humedades entre 40 y 50% donde se registraron datos ininterrumpidos por 02 días consecutivos. El hardware no presentó problemas de funcionamiento en el tiempo que se tuvo a prueba.

### 4.1.3. Definición o Actualización del Alcance del proyecto de HL

**FIGURA Nº 20: Definición del Alcance del proyecto de Hardware Libre**



### 4.1.4. Identificación de los Actores que integran el proyecto de desarrollo de Hardware Libre.

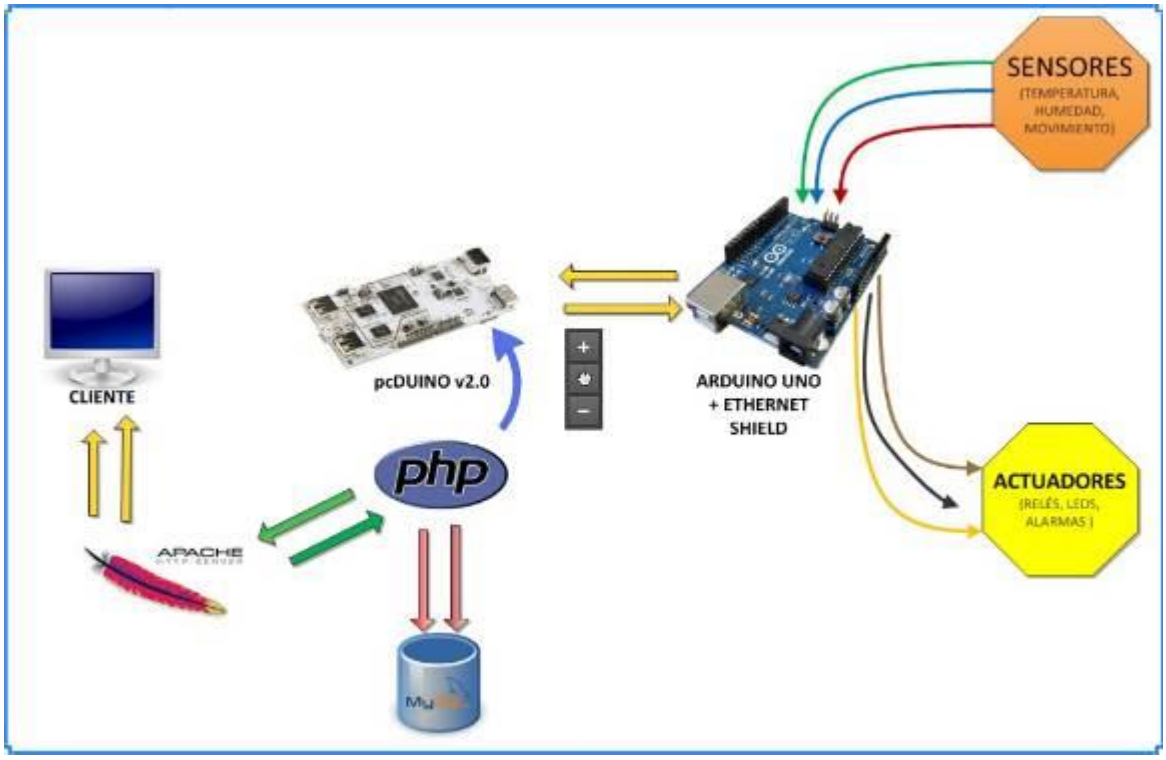
Los siguientes actores integran el proyecto:

- Director de Tecnologías de la Información. (El que ha facilitado toda la información requerida para el análisis, diseño e implementación del proyecto)

- Tesista: El responsable del Proyecto.

### 4.1.5. Elaboración de la Propuesta de Desarrollo del Proyecto de Hardware Libre.

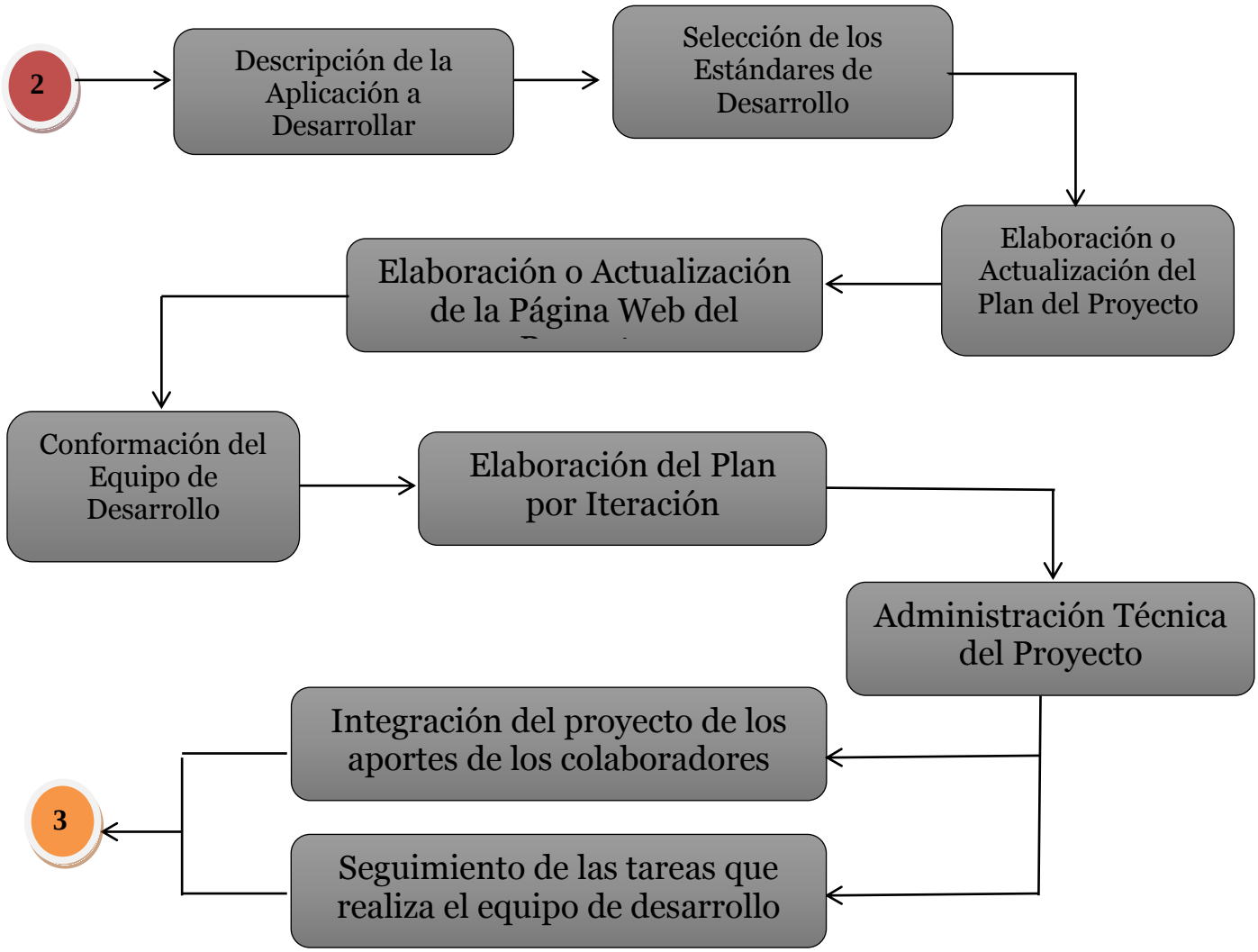
**FIGURA Nº 21: Arquitectura del Sistema de Monitoreo**



La tarjeta de desarrollo Arduino será programada para que interactúe con los sensores de temperatura, humedad y movimiento, estos valores serán enviados para ser almacenados y procesados por una mini pc (pcduino) que a su vez mostrará estos valores cada cierto tiempo en una página web en modo de gráficos. El sistema actuará ante cualquier evento programado activando o desactivando por ejemplo: extractores de aire, enviando emails o accionando alarmas sonoras.

### 4.2. Proceso de Administración de Proyectos de HL

FIGURA **Nº 22**: Actividades del proceso de administración de procesos de desarrollo de hardware libre



### 4.2.1 Descripción de la Aplicación a Desarrollar:

La aplicación a desarrollar es un sistema de seguridad física que será instalado en la Central de Datos de la USAT utilizando una plataforma de hardware libre, capaz de interactuar con sensores analógicos y digitales para obtener y procesar datos tanto de factores ambientales como de presencia física y además brindar la posibilidad de actuar ante un determinado evento según las necesidades y estándares considerados para seguridad física en Centro de Datos.

## 2.2 Selección de normas y estándares de Desarrollo del Proyecto

Las siguientes normas y estándares aplicadas a Centro de datos respaldan el desarrollo de nuestro proyecto:

### Normas ISO y BS:

### BS 25999

Esta norma hace referencia a la continuidad de la actividad comercial. La gestión de continuidad de la actividad comercial (BCM) se concibe como una ayuda para las organizaciones con el fin de minimizar el riesgo de interrupciones en sus servicios informáticos.

### ISO/IEC 20000

Esta norma hace referencia a todo lo relacionado con Gestión de servicios de TI y prestación de servicios de TI de gran calidad.

### ISO /IEC 27001

La Seguridad de la información en lo referente a protección de la información, el activo más valioso, es el aporte fundamental de esta norma.

### EN 16001

Factores como la eficiencia energética y el compromiso que deben asumir las organizaciones con el uso eficiente de esta energía son tratados en esta norma.

**TIER (Uptime) y TIA-942**

- **Tier Uptime**

✓ Según el estudio realizado, la central de Datos se encuentra ubicada en el nivel TIER 1 (Infraestructura básica)

- **TIA -942**

**TABLA Nº 17:** Rangos de Temperatura sugeridos para Data Center con Infraestructura básica según TIA-942

| NORMA TIA 942 | PARÁMETROS |
|---|---|
| Temperatura Mínima | 18ºC |
| Temperatura Máxima | 27ºC |
| Humedad Mínima | 40% |
| Humedad Máxima | 50% |

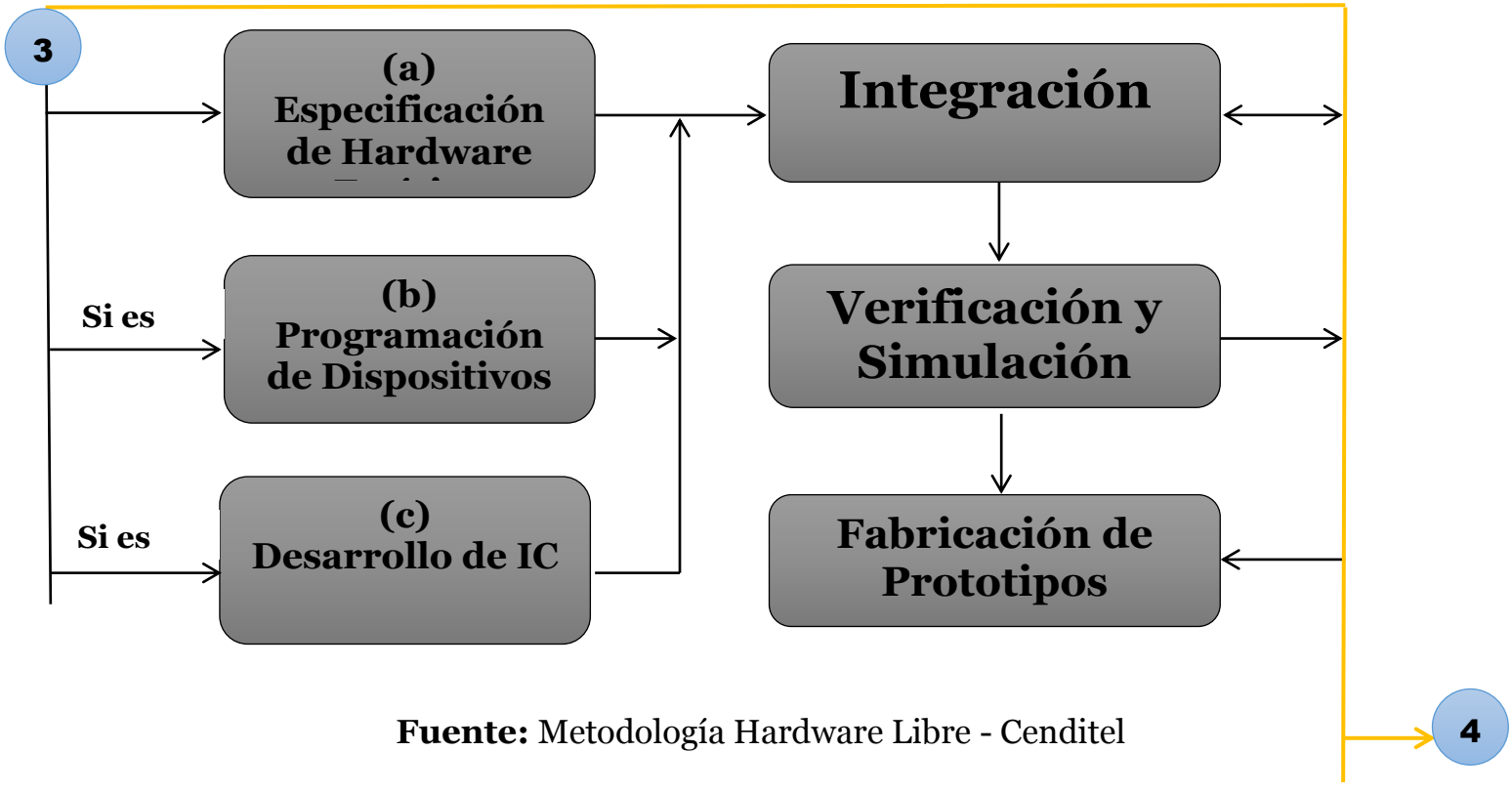
**Fuente:** Norma TIA942

**TABLA 18:** Rangos de Temperatura a considerar según estudio en el Centro de Datos de la USAT

| Rangos de Temperatura | PARÁMETROS |
|---|---|
| Temperatura Mínima | 17°C |
| Temperatura Máxima | 22°C |
| Humedad Mínima | 40% |
| Humedad Máxima | 50% |

### 4.3. Proceso de Desarrollo de Proyectos de Hardware Libre

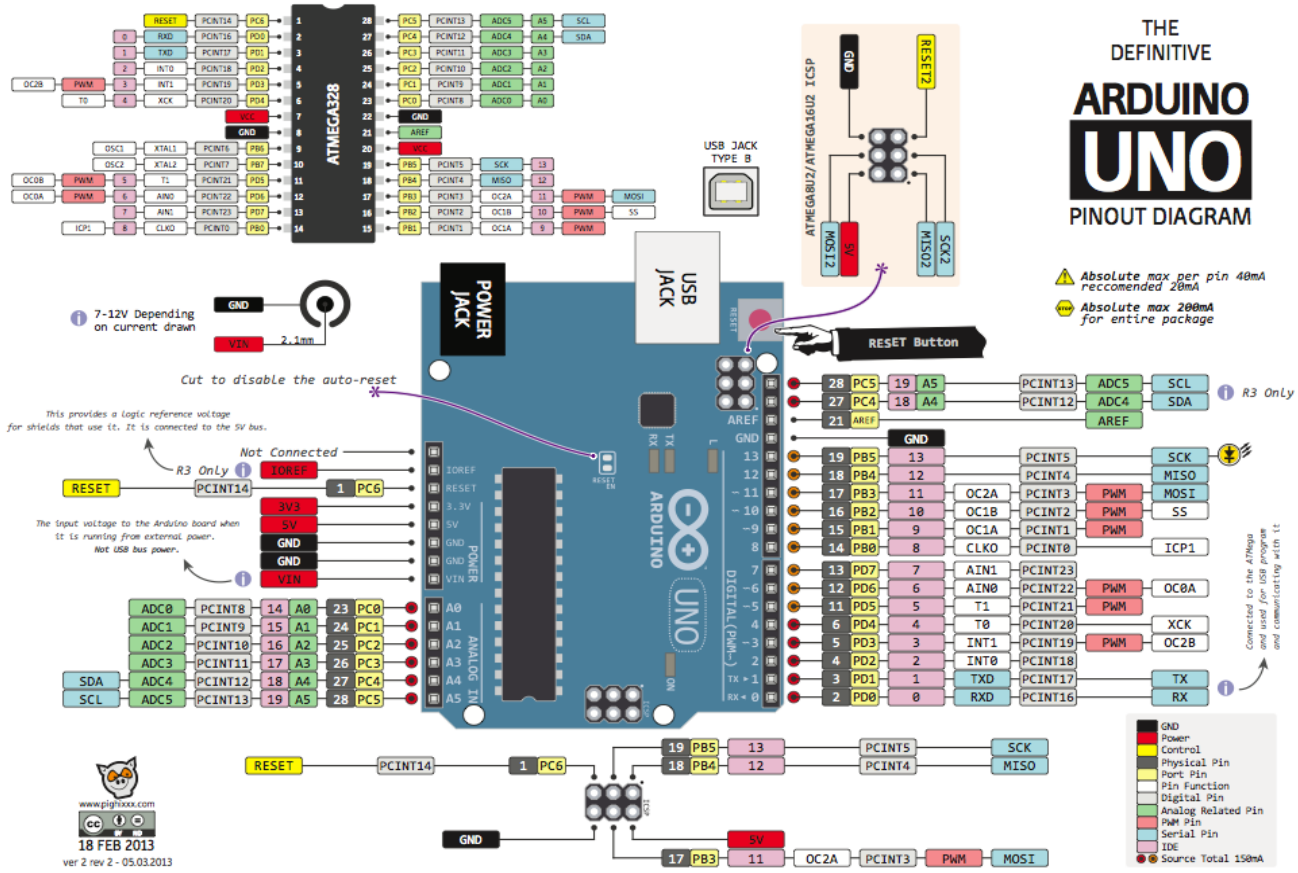
**FIGURA 23**: Proceso de Desarrollo de Proyectos de HL




**Fuente:** Metodología Hardware Libre - Cenditel

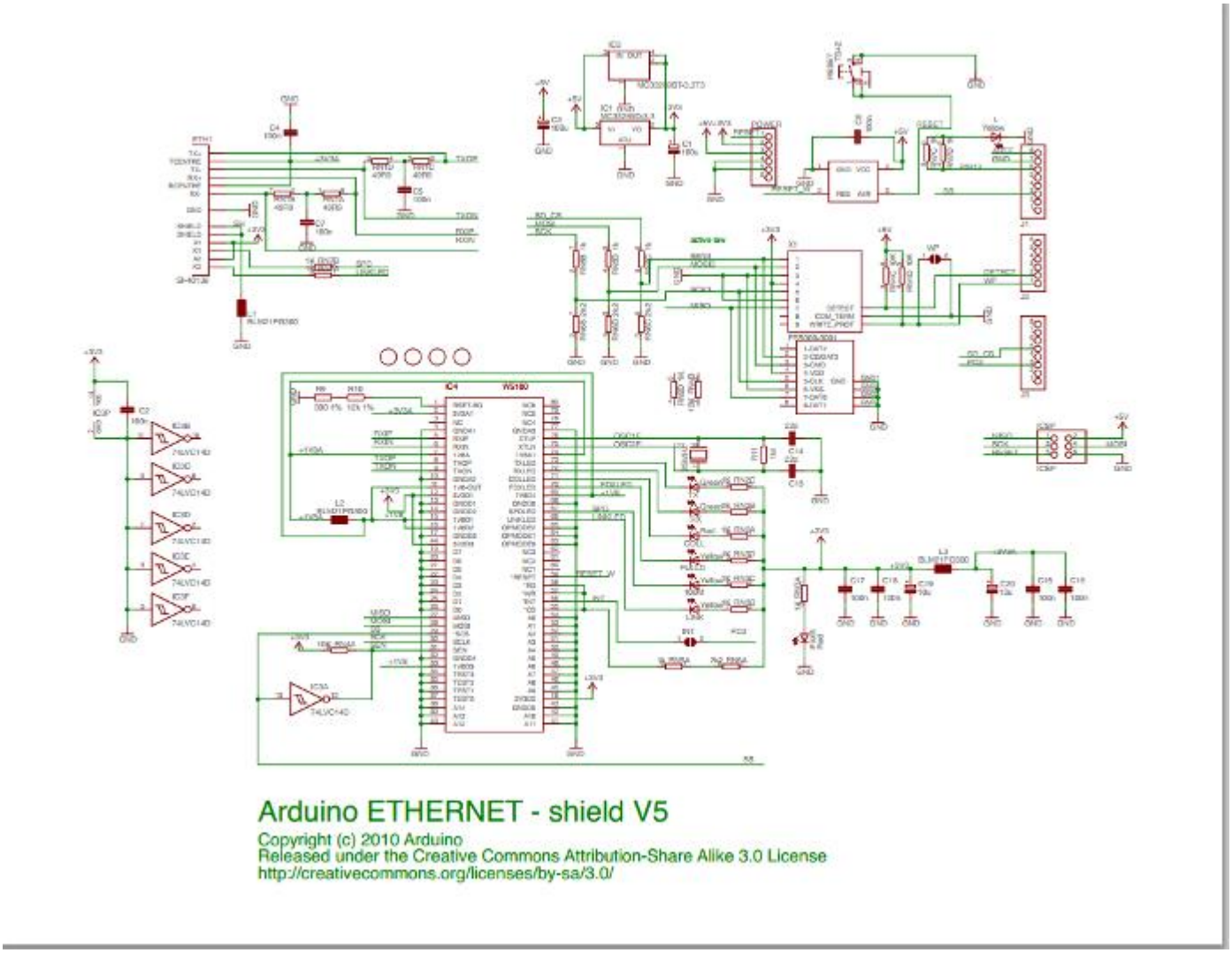
## a) **Especificación del Hardware Estático**

**FIGURA 24:** Diagrama Esquemático de la placa Arduino UNO




**Fuente:** Diagrama Esquemático Arduino UNO [imagen]. 2013. (accedido el 01 de marzo del 2014)

**FIGURA 25:** Diagrama Esquemático de la Tarjeta Shield Ethernet




**Fuente:** Diagrama Esquemático Tarjeta Shield Ethernet [imagen]. 2013. (accedido el 02 de marzo del 2014)

## A1) Integración de dispositivos

**FIGURA 26:** Integración de Dispositivos utilizados en el proyecto

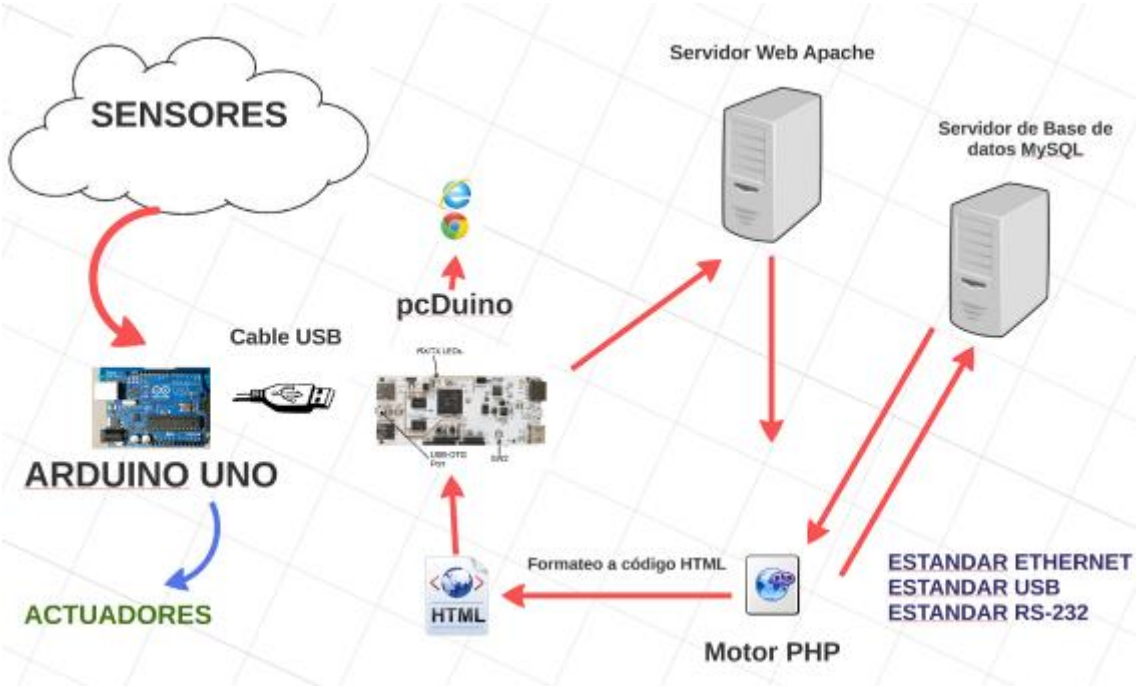
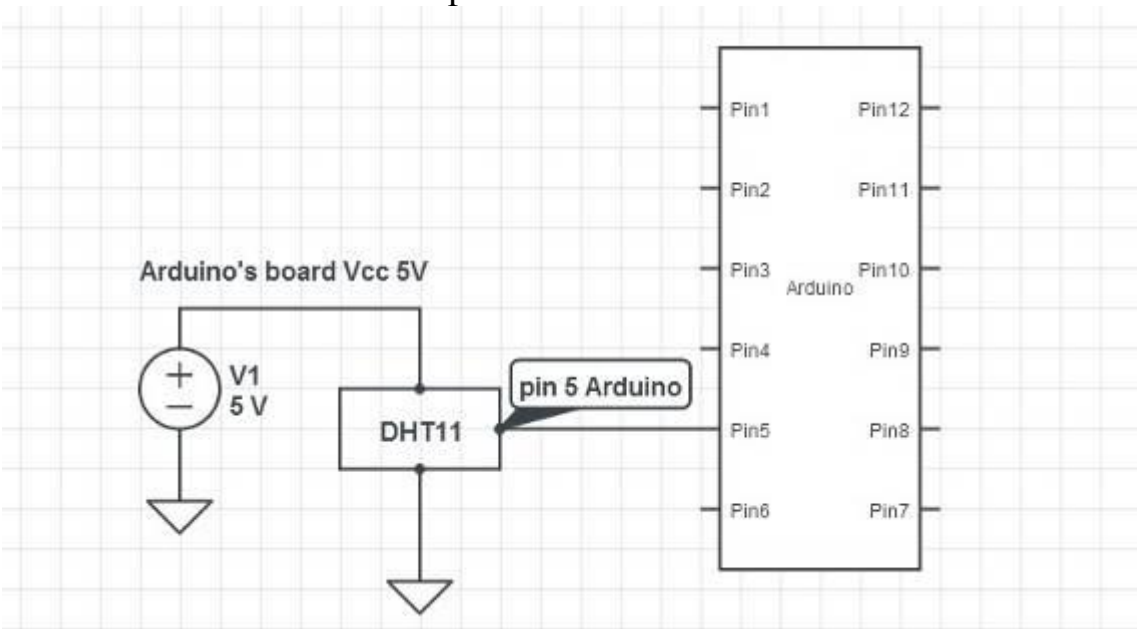
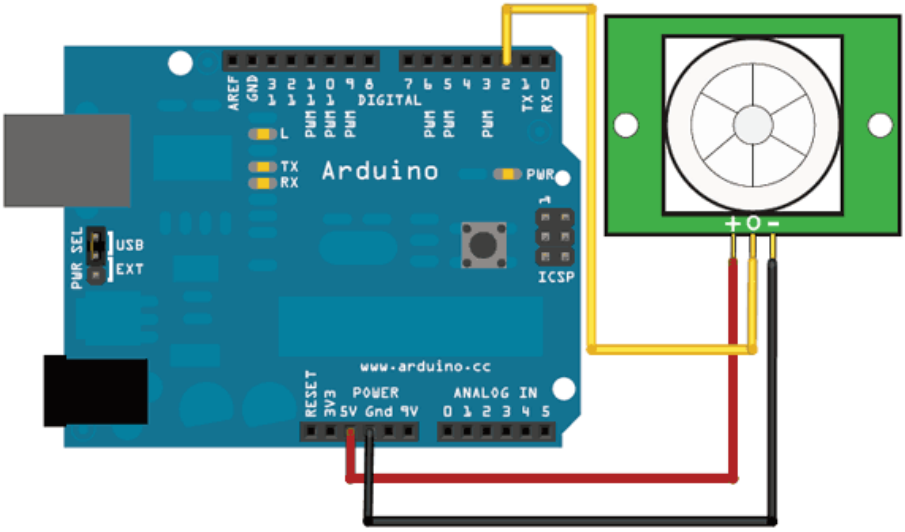



**FIGURA 27:** Integración del Sensor de Temperatura y Humedad DHT11 a la placa Arduino UNO



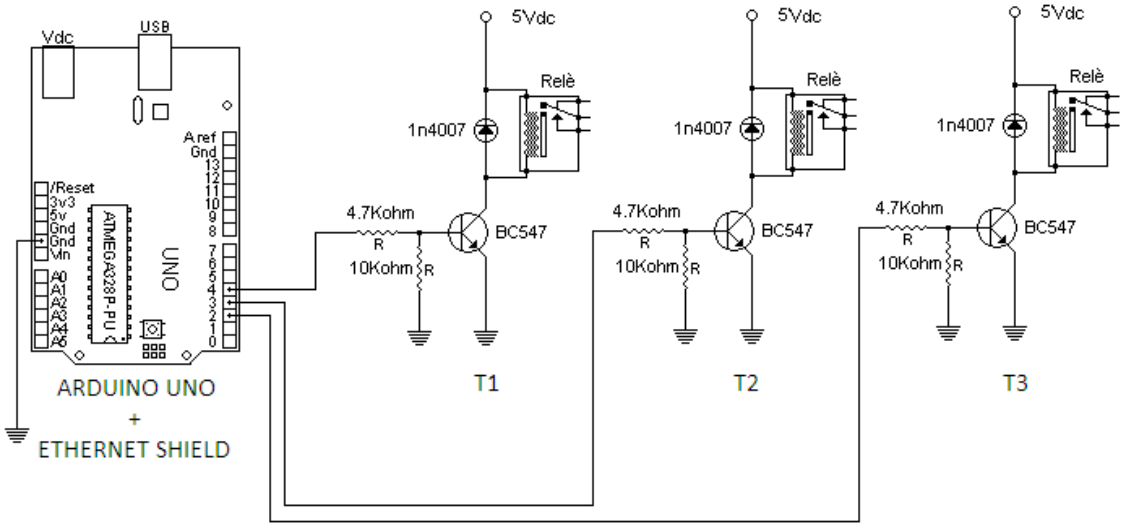

**Fuente:** Sensor de Temperatura y Humedad DHT11 [imagen]. 2013. (accedido el 01 de marzo del 2014)

**FIGURA 28:** Integración del Sensor de Movimiento PIR a la placa Arduino UNO




**Fuente:** Integración del sensor PIR a la placa Arduino Uno [imagen]. 2013. (accedido el 06 de marzo del 2014)

**FIGURA 29:** Integración de los relés a la placa Arduino UNO




**Fuente:** Integración de relés a la placa Arduino Uno [imagen]. 2013. (accedido el 06 de marzo del 2014)

**FIGURA 30:** Integración de Arduino Uno y pcDuino mediante interfaz USB


**Fuente:** Foto tomada a los dispositivos del proyecto

## b) Programación de Dispositivos:
### b1) Código en la Interfaz de Arduino:

```
/*
  Proyecto de Tesis II:
« Sistema de Monitoreo de Seguridad Física en plataforma libre de componentes electrónicos
  para asegurar la gestión de los niveles de continuidad
  de los servicios informáticos de la Central de Datos USAT. »

  Autor: Cesar Campos Bances
  IV PPIS&C - USAT

*/

// Importación de Librerías

#include "DHT.h" //libreria del Sensor de Humedad y Temperatura (DHT)
#include <SPI.h>
#include <Ethernet.h> // Libreria de la Shield Ethernet de Arduino

byte mac[] = {  0x90, 0xA2, 0xDA, 0x0D, 0x4E, 0xD7 }; // MAC de la tarjeta ethernet shield
byte ip[] = { 10,10,43,150}; // Direccion ip local (de la shield ethernet)
byte server[] = {10,10,43,30 }; // Direccion ip del servidor


EthernetClient client;

// declaración de variables
float humidity;
float temperature;
int rele = 9;
int analogPin = 3; //terminal del sensor de movimiento conectado al pin analógico 3
                   //Sensor de Movimiento Pir HC-SR501 polarizado con 5VCC
int val = 0; // Variable para almacenar el valor leído del sensor
// Definición de Pin donde va a estar conectado el sensor DHT
#define DHTPIN 8
#define DHTTYPE DHT11

// DHT Instancia
DHT dht(DHTPIN, DHTTYPE);

void setup()
{
  dht.begin(); //inicializa el sensor
  pinMode(rele,OUTPUT);
  Serial.begin(9600); // inicializa el puerto serial
  Ethernet.begin(mac, ip); // inicializa ethernet shield
  delay(1000); // espera 1 segundo despues de inicializar
}
```

```
void loop()
{
   float humidity = dht.readHumidity();
   float temperature = dht.readTemperature();
   val = analogRead (analogPin); // lee el pin de entrada
   if (temperature > 27){
     digitalWrite(rele,LOW);
    }
    else
  {
   digitalWrite(rele,HIGH);
  }
   if (val > 0){
     Serial.println("ALERTA: Se ha Detectado Movimiento: ");
    }
    else
  {
    Serial.println("NO se ha Detectado Movimiento ");
  }
    Serial.print("Temperatura: ");
    Serial.println(temperature);
    Serial.print("Humedad Relativa: ");
    Serial.println(humidity);
    Serial.println("Conectando..");
    Serial.println(val);


     if (client.connect(server,80)) {  // Se conecta al servidor
    client.print("GET /arduino.php?v1="); // Envia los datos utilizando GET
    client.print(temperature);
    client.print("&v2=");
    client.print(humidity);
    client.print("&v3=");
    client.print(val);
    client.println(" HTTP/1.0");
    client.println("User-Agent: Arduino 1.0");
    client.println();
    Serial.println("Conexion exitosa");


  }
  else
  {
    Serial.println("Falla en la conexion");
```

```
  }
  if (client.connected()) {}
  else {
    Serial.println("Desconectado");
  }
  client.stop();
  client.flush();
  delay(1000); // espera 1 segundos antes de volver a sensar la temperatura
}
```

Código elaborado por el autor de la tesis.

## B2) Código PHP (arduino.php) programado en el servidor (pcDuino)

```php
<?php
/*
  Proyecto de Tesis II:
« Sistema de Monitoreo de Seguridad Física en plataforma libre de componentes electrónicos
  para asegurar la gestión de los niveles de continuidad
  de los servicios informáticos de la Central de Datos USAT. »

  Autor: Cesar Campos Bances
  IV PPIS&C - USAT

*/

// Parametros de base de datos
$mysql_servidor = "127.0.0.1";
$mysql_base = "arduino";
$mysql_usuario = "admin";
$mysql_clave = "123";

$temperature = $_GET["v1"];
$humedad = $_GET["v2"];
$movimiento = $_GET["v3"];

//echo $temperature . " - " . $humedad;

// Valida que esten presente todos los parametros
if (($temperature!="") and ($humedad!="")) {
    mysql_connect($mysql_servidor,$mysql_usuario,$mysql_clave) or die("Imposible conectarse al servidor.");
    mysql_select_db($mysql_base) or die("Imposible abrir Base de datos");
    $sql = "insert into variables (fecha, temperatura, humedad, movimiento) values (NOW(),$temperature,$humedad,$movimiento)";
    mysql_query($sql);
}
?>
```

Código elaborado por el autor de la tesis.

B3) Código PHP (Página web ControlAmbientalv3) programado en el servidor (pcDuino)

```php
<?php

date_default_timezone_set('America/Peru'); //Se define la zona horaria
require_once('class.phpmailer.php'); //Incluimos la clase phpmailer
/*
  Proyecto de Tesis II:
« Sistema de Monitoreo de Seguridad Física en plataforma libre de componentes electrónicos
  para asegurar la gestión de los niveles de continuidad
  de los servicios informáticos de la Central de Datos USAT. »

  Autor: Cesar Campos Bances
  IV PPIS&C - USAT

*/

// Parametros de base de datos
$mysql_servidor = "127.0.0.1";
$mysql_base = "arduino";
$mysql_usuario = "admin";
$mysql_clave = "123";

    mysql_connect($mysql_servidor,$mysql_usuario,$mysql_clave) or die("Imposible conectarse al servidor.");
    mysql_select_db($mysql_base) or die("Imposible abrir Base de datos");

    $sql = "select * from variables order by fecha desc limit 1";
    $resultado_consulta_mysql=mysql_query($sql);

while($registro=mysql_fetch_array($resultado_consulta_mysql)){
 $tem=$registro['temperatura'];
 $hum=$registro['humedad'];
 $mov=$registro['movimiento'];
 $fec=$registro['fecha'];
}
```

```php
$sql1 = "select * from configuracion limit 1";
$resultado_consulta_mysql1=mysql_query($sql1);

while($registro1=mysql_fetch_array($resultado_consulta_mysql1)){
 $tmin=$registro1['tmin'];
 $tmax=$registro1['tmax'];
 $hmin=$registro1['hmin'];
 $hmax=$registro1['hmax'];
$actcorreo=$registro1['actcorreo'];
 $actmov=$registro1['actmov'];
}
```

(Código para la tabla de configuración de Temperatura máxima y mínima, Humedad máxima y mínima, activación de envío de correos, activación del sensor de movimiento).

```php

if($tem<=$tmin || $tem>=$tmax &&  $actcorreo==1){



$mail = new PHPMailer(true); // Declaramos un nuevo correo, el parametro true significa que mostrara excepciones y errores.

$mail->IsSMTP(); // Se especifica a la clase que se utilizará SMTP

try {
//---------------------------------------------------
  $correo_emisor="arduino.usat@gmail.com";     //Correo a utilizar para autenticarse
  //con Gmail o en caso de GoogleApps utilizar con @tudominio.com
  $nombre_emisor="USAT - ALERTA DE TEMPERATURA - ARDUINO";              //Nombre de quien envia el correo
  $contrasena="usat2014";          //contraseña de tu cuenta en Gmail
  $correo_destino="reset1976@gmail.com";      //Correo de quien recibe
  $nombre_destino="Cesar Campos";               //Nombre de quien recibe
//---------------------------------------------------
 //$mail->SMTPDebug  = 2;                     // Habilita información SMTP (opcional para pruebas)
                                              // 1 = errores y mensajes
                                              // 2 = solo mensajes
  $mail->SMTPAuth   = true;                   // Habilita la autenticación SMTP
  $mail->SMTPSecure = "ssl";                  // Establece el tipo de seguridad SMTP
  $mail->Host       = "smtp.gmail.com";       // Establece Gmail como el servidor SMTP
  $mail->Port       = 465;                    // Establece el puerto del servidor SMTP de Gmail
  $mail->Username   = $correo_emisor;         // Usuario Gmail
  $mail->Password   = $contrasena;            // Contraseña Gmail
  //A que dirección se puede responder el correo
  $mail->AddReplyTo($correo_emisor, $nombre_emisor);
  //La direccion a donde mandamos el correo
  $mail->AddAddress($correo_destino, $nombre_destino);
  //De parte de quien es el correo
  $mail->SetFrom($correo_emisor, $nombre_emisor);
  //Asunto del correo
  $mail->Subject = 'Prueba Arduino';
  //Mensaje alternativo en caso que el destinatario no pueda abrir correos HTML
  $mail->AltBody = 'Para ver el mensaje necesita un cliente de correo compatible con HTML.';
  //El cuerpo del mensaje, puede ser con etiquetas HTML
  $mail->MsgHTML("<strong>La temperatura ha excedido los 27 grados</strong>");
  //Archivos adjuntos
  //$mail->AddAttachment('img/logo.jpg');      // Archivos Adjuntos
  //Enviamos el correo
  $mail->Send();
  //echo "Mensaje enviado...";
 } catch (phpmailerException $e) {
  //echo $e->errorMessage(); //Errores de PhpMailer
 } catch (Exception $e) {
  //echo $e->getMessage(); //Errores de cualquier otra cosa.
}
```

(Código para el envío de correos de acuerdo a parámetros de temperatura establecidos)

```
<html>
  <head>

    <script src="gauge.js"></script>
    <style>body{padding:0;margin:0;background:#cd853f}</style>

  </head>
  <body>




<table align="center" border="1">


<tr>

<td bgcolor="#000" height="35">
<center><a  href="ControlAmbientalv3.php" style="color:#fff">PANEL</a> |
<a  href="config.php" style="color:#fff">CONFIGURACION</a></center>
</td>

</tr>


<tr>
<td>

<div style="float:left">
<canvas id="gauge"></canvas>
<div id="console"></div>

```

Código de configuración de los indicadores de temperatura y humedad

```
<script>
    var gauge = new Gauge({
        renderTo    : 'gauge',
        width       : 400,
        height      : 400,
        glow        : true,
        units       : 'ºC',
        title       : 'Temperatura',
        minValue    : 0,
        maxValue    : 50,
        majorTicks  : ['0','5','10','15','20','25','30','35','40','45','50'],
        minorTicks  : 5,
        strokeTicks : false,
        highlights  : [
            { from : 0,   to : <?echo $tmin;?>, color : 'rgba(255,   255, 0, .15)' },
            { from : <?echo $tmin;?>, to : <?echo $tmax;?>, color : 'rgba(0, 255, 0, .15)' },
            { from : <?echo $tmax;?>, to : 50, color : 'rgba(255, 30,  0, .25)' }
        ],
        colors      : {
            plate      : '#222',
            majorTicks : '#f5f5f5',
            minorTicks : '#ddd',
            title      : '#fff',
            units      : '#ccc',
            numbers    : '#eee',
            needle     : { start : 'rgba(240, 128, 128, 1)', end : 'rgba(255, 160, 122, .9)' }
        }
    });


    gauge.onready = function() {

gauge.setValue(<?php echo $tem; ?>);
    };
    gauge.draw();
</script>
</div>

```

**FIGURA 31.** Diseño de página web del Sistema de Monitoreo de Seguridad Física para el Centro de Datos USAT


**FIGURA 32.** Interfaz de configuración de parámetros.


**FIGURA 33.** Interfaz de Configuración de parámetros (botón actualizar)

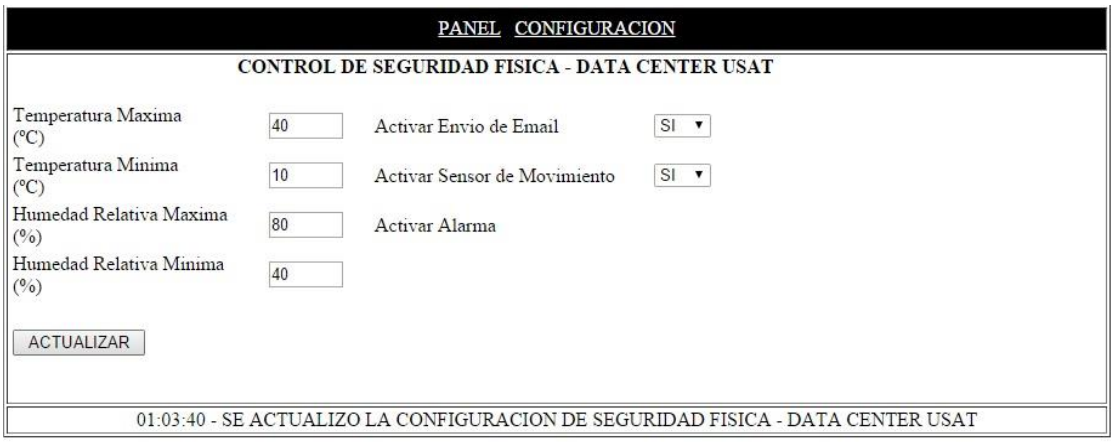


**FIGURA 34.** Pruebas en Pc-Duino


**FIGURA 35.** Ejecución de Sketch Arduino en Pc-duino

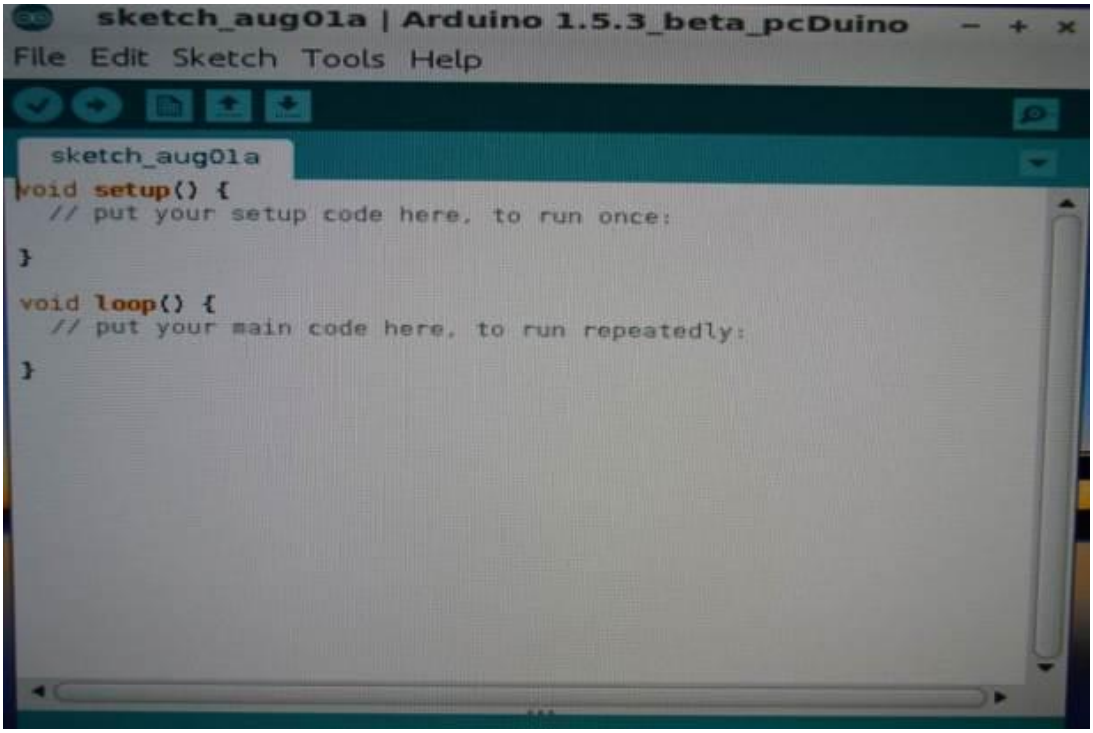



**FIGURA 36.** Ejecución del código en lenguaje Arduino del Proyecto de Monitoreo de Seguridad Física

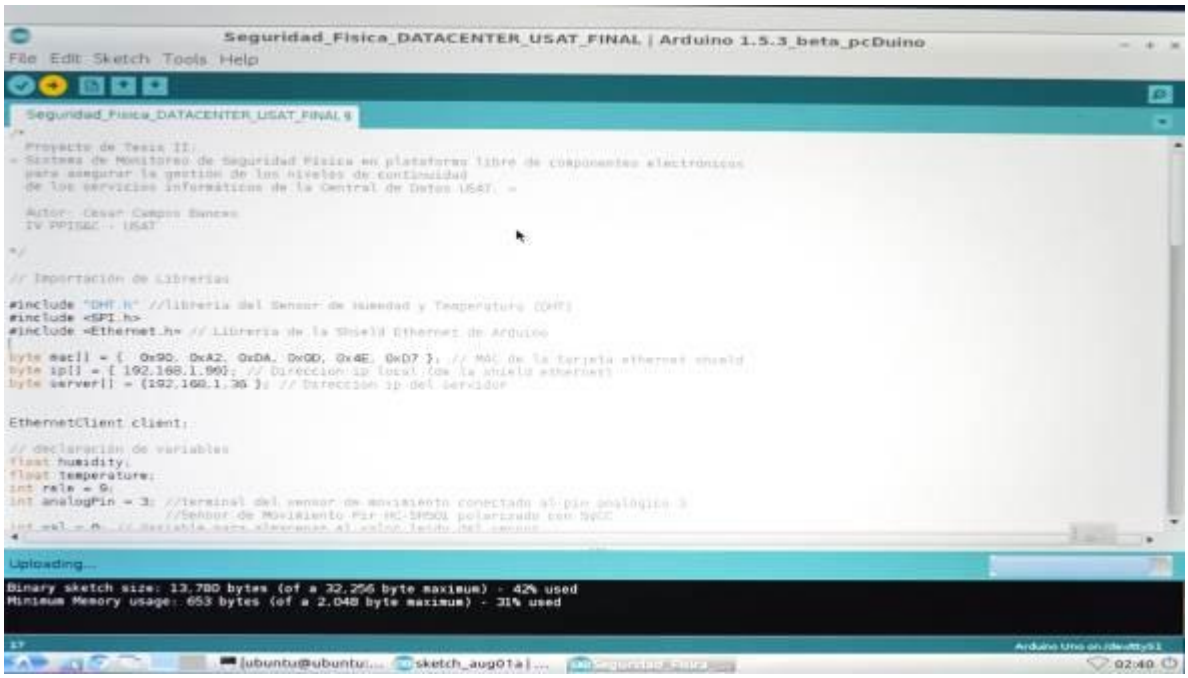



**FIGURA 37.** Ingreso a Phpmyadmin desde Pcduino

**FIGURA 38.** Base de datos y tablas creadas en phpMyAdmin


**Nombre Base de Datos**: **arduino**

**Tablas:**

**Tabla Configuración**

| CONFIGURACION |
| --- |
| tmin |
| tmax |
| hmin |
| hmax |
| actmov |

- **tmin (temperatura mínima)**
- **tmax (temperatura máxima)**
- **hmin (humedad mínima)**
- **hmax (humedad máxima)**
- **actmov (activación de movimiento)**

**Tabla Variable**

| VARIABLE |
| --- |
| t1<br>h1<br>t2<br>h2<br>t3<br>h3 |

- **t1 (temperatura en ºC en gabinete 1)**
- **h1 (humedad relativa en gabinte 1 )**
- **t2 (temperatura en ºC en gabinete 2)**
- **h2 (humedad relativa en gabinete 2)**
- **t3 (temperatura en ºC en gabinete 3)**
- **h3 (humedad relativa en gabinete 3)**

**FIGURA 39. Descripción de la Tabla configuración**

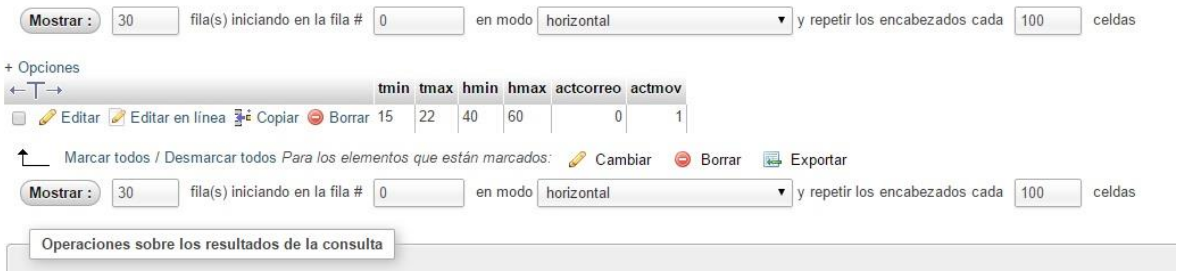
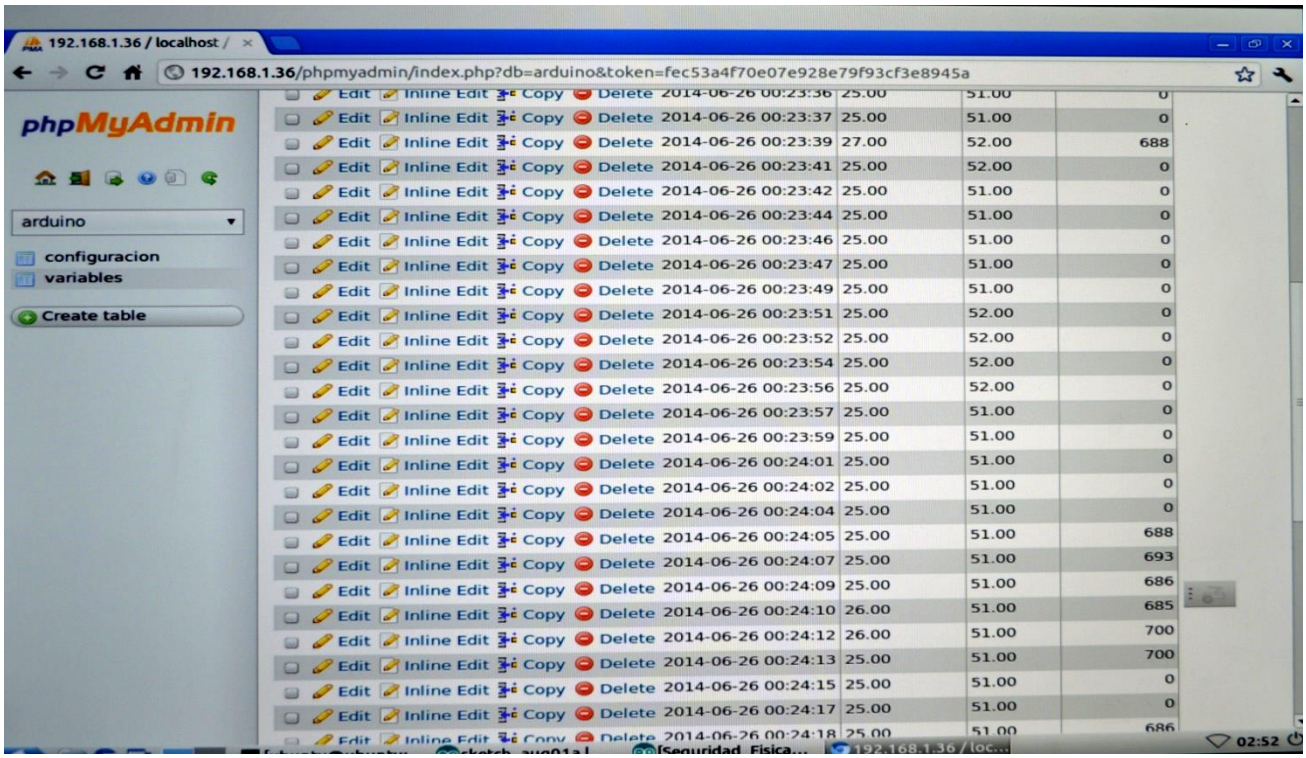


**FIGURA 40. Pruebas de almacenamiento de datos en la tabla "variables" de la base de datos "arduino")**



## V. Discusión:

A continuación se realizará un análisis el cual fue obtenido en la etapa de prueba y resultados con la finalidad de validar nuestra hipótesis, esto nos permitirá también validar la veracidad de la misma y por consiguiente la viabilidad de nuestro proyecto.

**Tabla Nº 19:** Comparación de medidas de factores ambientales entre el sistema tradicional y el sistema de seguridad física

| **Indicador:** Aumentar el Ciclo de Vida útil de los equipos informáticos del CPD | **SISTEMA TRADICIONAL** | | | | **SISTEMA DE SEGURIDAD FÍSICA** | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Fecha** | **T(ºC)** | **HR(%)** | ACCION | T (ºC) **ZONA 1** | T (ºC) **ZONA 2** | T (ºC) **ZONA 3** | HR (%) **ZONA 1** | HR (%) **ZONA 2** | HR (%) **ZONA 3** | ACC |
| | 10/07/2014 | 18 | 60 | NO | 17 | 18 | 19 | 62 | 62 | 64 | N |
| | 11/07/2014 | 17 | 55 | NO | 18 | 19 | 19 | 56 | 58 | 59 | N |
| | 12/07/2014 | 32 | 80 | NO | 33 | 34 | 36 | 82 | 83 | 84 | S |
| | 13/07/2014 | 17 | 54 | NO | 15 | 17 | 18 | 56 | 56 | 57 | N |
| | 14/07/2014 | 19 | 65 | NO | 20 | 21 | 22 | 65 | 67 | 67 | N |
| | 15/07/2014 | 16 | 60 | NO | 17 | 17 | 19 | 62 | 64 | 64 | N |

| **LEYENDA:** | | |
|---|---|---|
| **T (ºC)** = Temperatura en Grados Centígrados | | |
| **HR (%)** = Humedad Relativa en Porcentaje | | |
| **ZONA 1:** GABINETE Nº 01 | | |
| **ZONA 2:** GABINETE Nº 02 | | |
| **ZONA 3:** GABINETE Nº 03 | | |

Como se puede apreciar en la Tabla Nº 18, se ha sensado toda la población de equipos informáticos existentes en la Central de Datos divididos en 3 zonas específicas por seis días consecutivos. Se puede verificar mayor exactitud de datos de temperatura y humedad relativa en los sensores del sistema de seguridad física, asimismo se logra aumentar el ciclo de vida útil de los equipos informáticos ya que el sistema de seguridad física toma acción frente a excesos de temperatura y humedad (como se puede apreciar en el día 12/07/2014 de la tabla anterior) activando extractores de aire que tienen la función de renovar el aire interior para regular los grados de temperatura y humedad del ambiente.

**Tabla Nº 20. Comparativas entre el Termómetro-Higrómetro Digital Radio Shack y el sistema de seguridad de nuestro proyecto**

| Funcionalidad | Termómetro-Higrómetro Digital Radio Shack | Sistema de Seguridad Física de Nuestro Proyecto |
|---|---|---|
| **Alcance Funcional de Temp** | 0ºC a 40ºC / 32ºF-104ºF | 0ºC a 50ºC / 32ºF-122ºF |
| **Alcance Funcional de Hum.** | 20% RH a 95% RH | 20% RH a 95% RH |
| **Operatividad** | Mide la Temperatura ambiental general y en un solo ambiente específico gracias a un cable incorporado<br><br>Permite guardar un número limitado de registros de temperatura y humedad dentro del equipo<br><br>Mide la Humedad Relativa solo en un ambiente<br><br>No toma ninguna acción frente a excesos de temperatura y humedad. Es solo reactivo | Realiza lecturas de temperatura ambiental en diversas zonas específicas<br><br>Permite guardar una gran cantidad de registros de temperatura y humedad a manera de históricos almacenados en una base de datos local o en la nube.<br><br>Realiza lecturas de Hemperatura ambiental por zonas específicas pudiéndose interconectar varios sensores<br><br>Si toma acciones específicas frente a riesgos de excesos de temperatura y humedad activando, por ejemplo, estractores de aire, enviando alertas mediante correo electrónico o activando alarmas sonoras. Es preventivo |
| **Portabilidad** | La Lectura de Temperatura y humedad se realiza en el mismo equipo | La lectura de Temperatura y humedad se puede visualizar online a través de una pagina web |
| **Escalabilidad** | Su sistema no es escalable, no se le puede agregar mas funcionabilidad | El sistema Si es escalable con la posibilidad de agregar mas funcionalidad como la interconexión de varios sensores de termperatura y humedad |

La anterior tabla nos muestra comparativas en relación a tres enfoques: Operatividad, Portabilidad y Escalabilidad, donde se demuestra las ventajas que ofrece nuestro sistema de seguridad física frente al sistema tradicional.

## Pruebas de las medidas de temperatura y Humedad Realizadas con el sistema tradicional.

En las pruebas mencionadas se midió la temperatura y humedad relativa con el termómetro - higrómetro (Sistema Tradicional) utilizado en el Centro de Datos, de las siguientes características técnicas.

**TABLA Nº 21: Características Técnicas del Termómetro-Higrómetro Radio Shack**

| EQUIPO | Termómetro – Higrómetro con cable |
|---|---|
| Marca | Radio Shack |
| Modelo | 6300699 |
| Resolución de Temperatura | 0,1 ºC / 0,1 ºF |
| Alcance Mostrado de temperatura | -50ºC a 70ºC / -58ºF a 158ºF |
| Alcance Funcional de Temperatura interior | 0ºC a 50ºC / 32ºF-122ºF |
| Resolución de la Humedad | 1% RH |
| Alcance de la Humedad | 20% RH a 95% RH |
| Accesorios | Cable para medir la temperatura y humedad en otro ambiente |

Esta tabla nos muestra datos relevantes como la resolución y alcance de Temperatura y Humedad soportado por este Termómetro.

**Figura Nº 41:** Termómetro-Higrómetro Digital Radio Shack Modelo: 6300699


**Figura Nº 42:** Valores Mostrados en Termómetro – Higrómetro Digital Radio Shack

**LEYENDA:**

**OUT:** Valor de temperatura en grados centígrados medido a través del cable incorporado del equipo instalado en un gabinete de servidores).

**IN:** Valor de Temperatura medido en grados centígrados de todo el ambiente.

**HUMIDITY:** Porcentaje de humedad relativa medido en todo el ambiente (no en el gabinete)

Se puede apreciar los siguientes valores:

**OUT:** 16.5 ºC

**IN:** 17º C

**HUMIDITY:** 51 %

**Figura Nº 43:** Valores Mostrados en Termómetro – Higrómetro Digital Radio Shack

Se puede apreciar los siguientes valores:

**OUT:** 18.8 ºC

**IN:** 18.7 ºC

**HUMIDITY:** 55 %

**Figura Nº 44:** Valores Mostrados en Termómetro – Higrómetro Digital Radio Shack


Se puede apreciar los siguientes valores:

**OUT:** 32.9 ºC

**IN:** 29 ºC

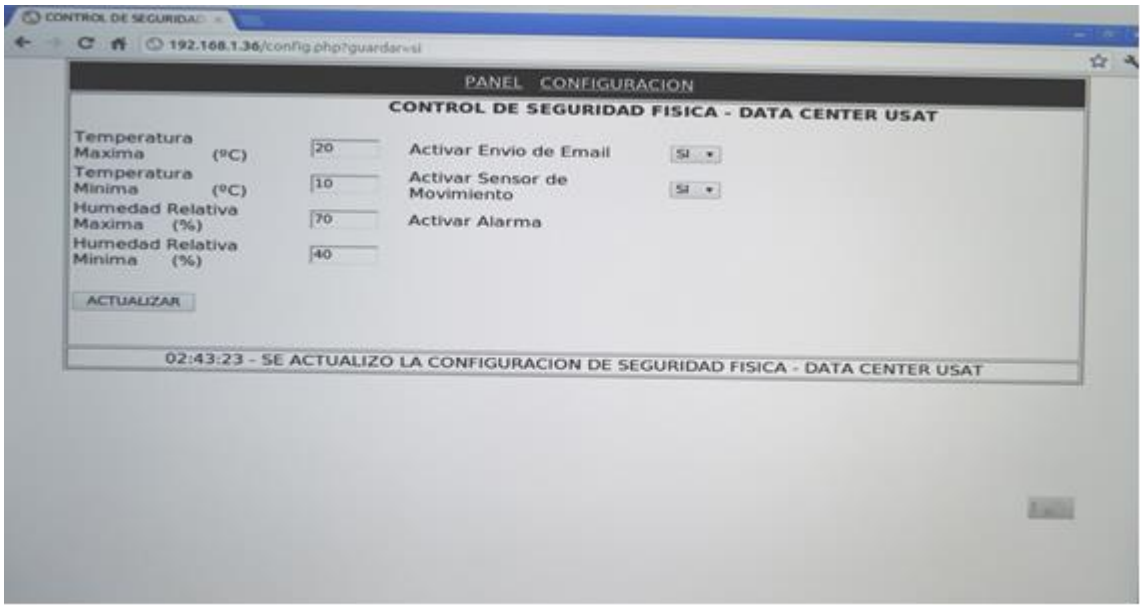
**HUMIDITY:** 69 %

Estos valores fueron tomados en días distintos en las cuales se puede apreciar las variaciones de temperatura y humedad que ha detectado este equipo en solo una zona específica sin darnos la posibilidad de saber las lecturas en otras zonas críticas (como en la zona de los UPS y transformadores de aislamiento) para poder actuar a tiempo ante estos excesos de temperatura y humedad.

**Figura Nº 45:** Pruebas de medición de Valores de Temperatura y Humedad mostrados en el sistema de seguridad física de nuestro proyecto

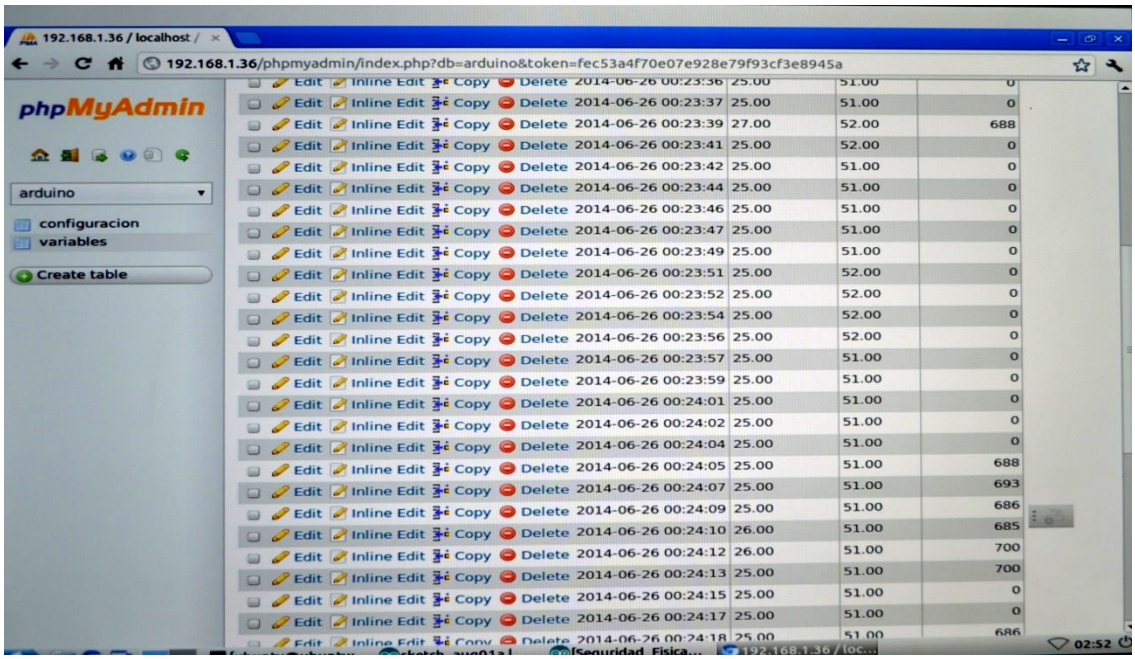

En nuestro sistema se puede visualizar en una página web los valores de temperatura y humedad relativa a cada minuto en diferentes ambientes del CPD en una interfaz gráfica precisa a manera de indicadores visuales y además se puede visualizar las alertas que se activaron en cada condición. Se han tomado mediciones por seis días consecutivos, donde se pudo comprobar también que el hardware de seguridad física reacciona perfectamente frente a funcionamiento continuo.

**Figura Nº 46:** Pruebas de Configuraciones de valores máximos y mínimos de temperatura y humedad en el sistema de seguridad física de nuestro proyecto



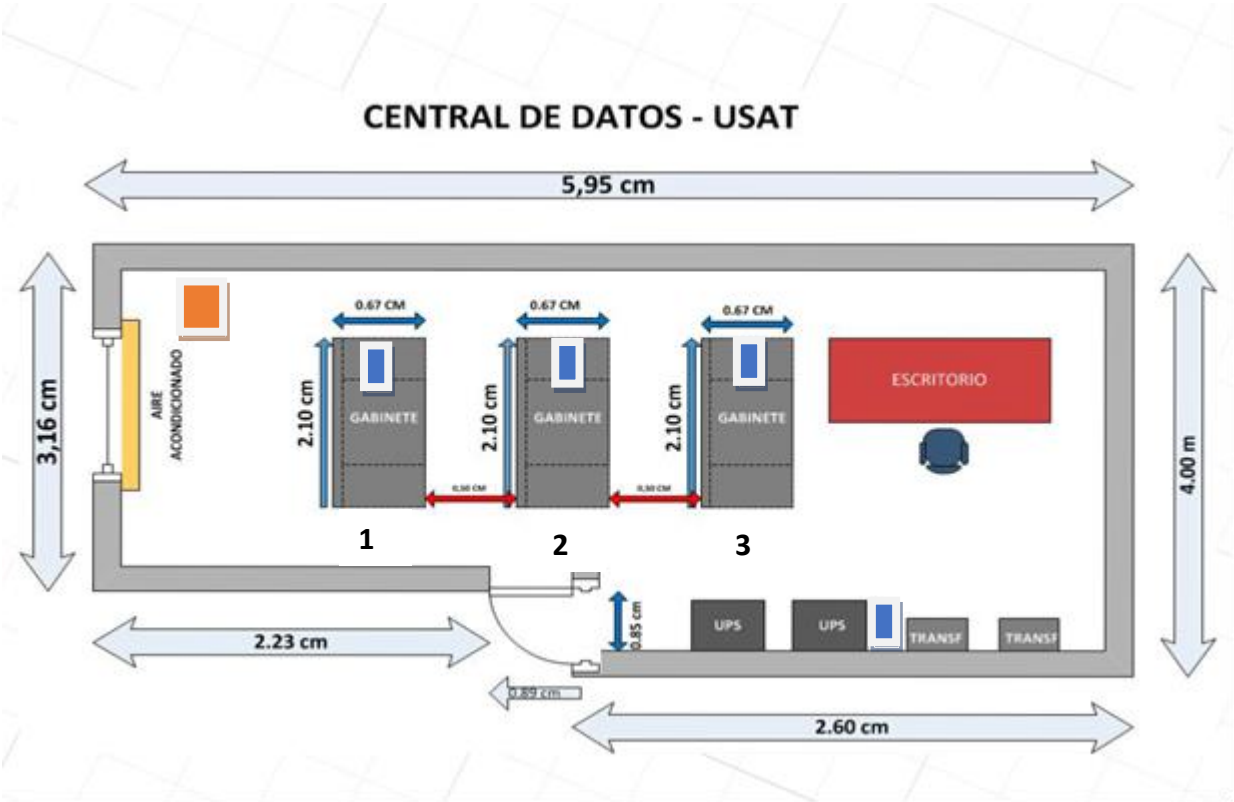

Esta tabla muestra la interfaz web donde el usuario puede configurar manualmente parámetros como valores máximos y mínimos de temperatura y humedad según el entorno del Centro de datos de acuerdo al nivel de operatividad del mismo (TIER).

**Figura Nº 47:** Visualización de los valores de temperatura, humedad y alertas por fecha (días, horas, minutos) en las pruebas realizadas de nuestro sistema de seguridad física de nuestro proyecto



La tabla anterior muestra la captura de datos de temperatura y humedad realizados en uno de los días en que se tuvo a prueba nuestro sistema de seguridad física. Podemos visualizar también la fecha y hora en que se tomaron dichas medidas.

**Figura Nº 48:** Puntos de ubicación del sistema de seguridad física y de los sensores de temperatura y humedad dentro del Centro de Datos de la USAT




**LEYENDA:**

Sensores Instalados en zonas estratégicas

Sistema de Seguridad Física de nuestro proyecto

El plano anterior muestra los puntos estratégicos en que se instalaron los sensores de temperatura y humedad. En cada gabinete existen numerosos equipos informáticos que tienen rangos específicos de temperatura y humedad de operación, las cuales se describen a continuación:

**Tabla Nº 22:** Equipos informáticos instalados en el gabinete 1 (Refiérase a la figura Número Nº 48)

| CANTIDAD | EQUIPOS | MARCA Y MODELO |
|---|---|---|
| 02 | Discos Duros NAS | Simple Share |
| 5 | Switch | 3Com 5500 Series/28p |
| 3 | GSM Fixed Wireless Terminal | BBK-BKG330T |

**Tabla Nº 23:** Equipos informáticos instalados en el gabinete 2 (Refiérase a la figura Número Nº 48)

| CANTIDAD | EQUIPOS | MARCA Y MODELO |
|---|---|---|
| 02 | Router | Cisco 1900 Series |
| 02 | Router | 3Com 5012 Series |
| 02 | Tipping Point | TP 50 |
| 03 | Switch | 3Com 500G |
| 01 | Central Telefónica | NBX |
| 02 | Discos Duros Externos | A-data |

**Tabla Nº 24:** Equipos informáticos instalados en el gabinete 3 (Refiérase a la figura Número Nº 48)

| CANTIDAD | EQUIPOS | MARCA Y MODELO |
|---|---|---|
| 02 | Servidores | IBM System X3550 |
| 02 | Servidores | IBM X Series 235 |
| 03 | Servidores | IBM SC5295BRP |
| 01 | KVM | Trendnet TK-802R |
| 02 | Pcs de Escritorio | Advance Core I5 |

**Tabla Nº 25:** Temperatura y Humedad de trabajo de los equipos informáticos instalados dentro de los gabinetes de la Central de Datos USAT

| EQUIPO | Temperatura de trabajo | Humedad de trabajo |
|---|---|---|
| Switch 3Com 5500 | 0° - 40°C | 10% to 95% non-condensing |
| Servidor IBM System X3550 | 0° - 38°C | 10 - 90% |
| Discos Duros Externos NAS | 5°C - 35 °C | 30 – 60% |
| Tiping Point | 0°C – 45°C | 20 – 65% |
| Router Cisco 1900 Series | 0°C – 40°C | 5 – 95% |

Como podemos apreciar en las tablas anteriores, cada equipo informático presenta especificaciones de temperatura y humedad mínimas y máximas en las cuales pueden trabajar. Para escenarios óptimos no se recomienda trabajar en los valores límites pues esto significaría un riesgo de deterioro de los mismos por exceso de estos factores.

**Tabla Nº 26:** Equipos que sufrieron daños por problemas de seguridad física

| | Equipos | Fecha | Problema-Daño | Consecuencia |
|---|---|---|---|---|
| **Indicador:** Cantidad de equipos que sufrieron daños por problemas de seguridad física | **UPS Elise** | Junio 2013 | Recalentamiento de baterías | Fuera de operación por 01 Día. Baterías averiadas por recalentamiento. (Total 80) |
| | **Server IBM X3550** | Agosto 2013 | Recalentamiento de Disco Duro de Servidor | Disco Duro Averiado, al menos un servicio dejó de funcionar por el lapso de 1 hora. |

Como podemos apreciar en la tabla anterior existen equipos que sufrieron daños por una insuficiente seguridad física en la metodología tradicional. No existió ninguna alerta o alarma que pudieran prevenir estos incidentes. Esto se traduce en pérdidas de dinero al tener que reponer estos equipos.

La Central de Datos de la USAT contaba con solo una alerta de corte de energía eléctrica proporcionada por los UPS instalados dentro de esta. Se envía una alerta de correo electrónico solo cuando existe ausencia de energía en cualquiera de los UPS más no cuando existe un incremento de temperatura.

**Figura Nº 49:** UPS instalado en el Centro de Datos de la USAT

**Fuente:** Modelo: PW9155 [imagen]. 2014. (accedido el 01 de julio del 2014)

**Tabla 27:** Características Técnicas UPS Elise instalado en el Centro de Datos de la USAT

| | |
|---|---|
| EQUIPO | UPS |
| Marca | ELISE |
| Modelo | PW9155 |
| Tecnología | True On Line de Doble Conversión Full IGBT |
| Potencia: | 8 - 15kVA (7.2 - 13.5KW) |
| Voltaje: | 220 & 380VAC 50/60Hz |
| Tiempo de autonomía: | 5 min. Expandible + EBM |
| Sistema | Redundante Inteligente HOT SYNC |
| Crecimiento modular | N+1 |

**Sistema de alertas (control ambiental) – Sistema de seguridad Física de nuestro proyecto.**

**Figura Nº 50:** Pruebas de alertas por correo electrónico (enviado a una cuenta de Gmail) cuando el sistema detecta excesos de temperatura o humedad relativa dentro del CPD de acuerdo a parámetros establecidos.


**Figura Nº 51:** Visualización de activación de alertas dentro de la página web del sistema de seguridad física.


Como podemos ver, en nuestro sistema de seguridad física existen alertas programadas para cada variación de temperatura que se encuentre fuera de los rangos preestablecidos. Esto nos ayudará a disminuir los costos que se dispongan al reemplazar un equipo por problemas de esta naturaleza.

Además, se puede visualizar en la página web del sistema de seguridad física de nuestro proyecto las alertas activadas en las que se puede también detectar la ausencia de energía eléctrica de la red gracias a que este sistema será alimentado por un UPS.

**Figura Nº 52:** UPS a utilizar para alimentar nuestro sistema de seguridad física en el Centro de Datos de la USAT


**Fuente:** Back-UPS Pro APC [imagen]. 2014. (accedido el 02 de julio del 2014)

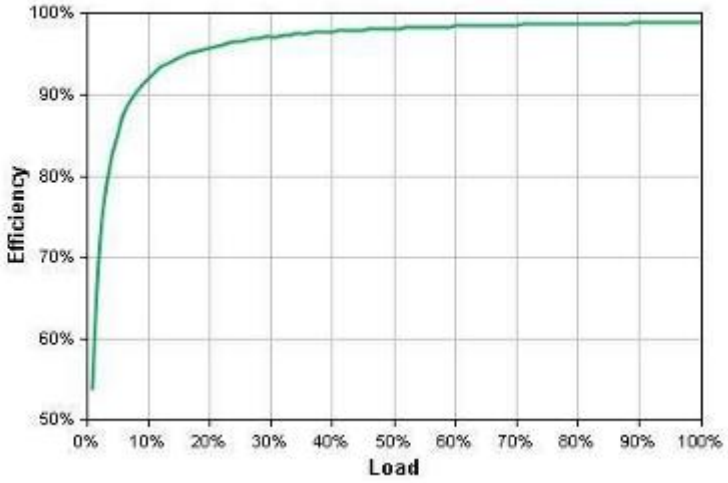
**Tabla Nº 28:** Características Técnicas del UPS que suministrará energía eléctrica al sistema de seguridad física

| **EQUIPO** | **UPS** |
|---|---|
| Marca | APC |
| Modelo | Pro 1500 |
| Potencia | 1.5KVA |
| Tensión de salida de voltaje nominal | 230 VAC |
| Topología | Línea Interactiva |
| Frecuencia de salida | 60Hz |
| Autonomía | 45 minutos (según tabla de uso de energía) |

**Tabla Nº 29:** Uso de energía y Eficiencia del UPS APC Pro 1500

Energy Use/Efficiency

| Load | Efficiency |
|---|---|
| 25% | 96.6% |
| 50% | 98.2% |
| 75% | 98.7% |
| 100% | 98.9% |




**Fuente:** Back-UPS Pro APC [imagen]. 2014. (accedido el 02 de julio del 2014)

Este UPS nos permitirá tener nuestro sistema funcionando por aproximadamente 45 minutos ante un corte de energía eléctrica, en este lapso de tiempo el sistema envía alertas por este inconveniente.

**Tabla Nº 30:** Costos Operativos que implica la adquisición de equipos informáticos nuevos por reposición por pérdidas o robos.

| **Indicador** | **Equipos** | **Costos** | **Pérdidas** |
|---|---|---|---|
| Costos Operativos que implica la adquisición de equipos informáticos Nuevos por reposición por pérdidas o robos | 30 equipos informáticos instalados en la Central de datos | **300000 USS** | Hasta el momento no se ha registrado pérdidas de equipos informáticos por robos. |

Aunque hasta el momento no se ha registrado pérdidas de equipos informáticos dentro del CPD por robos, se tenía un riesgo latente por la insuficiencia de seguridad en lo que respecta a accesos físicos. No se contaba con un mecanismo de alerta de presencia física dentro del CPD debido a que solo se tenía instalada una cámara de vigilancia en su interior que no funcionaba adecuadamente, es decir, no era posible visualizar presencia o actividad en su interior ni tampoco alertar a las personas responsables. Con nuestro sistema de seguridad física se logra reducir en gran proporción este riesgo debido a que se cuenta ahora con una serie de alertas y alarmas.

**Figura Nº 53:** Cámara de Seguridad instalada en el Centro de Datos


**Fuente:** Cámara de Vigilancia D-Link [imagen]. 2010. (accedido el 18 de abril del 2014)

**Tabla Nº 31:** Características técnicas de la cámara de vigilancia instalada en el CPD

| **Equipo** | **Cámara de vigilancia** |
|---|---|
| Marca | D-link |
| Modelo | DSC-3220 |
| Zoom digital | 4x |
| Grabación | vídeo |

**Figura Nº 54: Pruebas de Activación del sensor de movimiento del sistema de seguridad física de nuestro proyecto**


El sensor de movimiento instalado en la Central de Datos detecta cualquier actividad en un rango de 4 metros. Al detectar esta actividad, el sistema muestra una alerta pudiendo visualizar la fecha y la hora del evento.

# VI. CONCLUSIONES

En el siguiente estudio se puede concluir que el planteamiento de nuestros objetivos e hipótesis son aceptados y con gran significancia en los indicadores.

1.- Los costos operativos que conlleva la adquisición de equipos informáticos nuevos por reposición fueron afectados positivamente debido a que se reduce significativamente las averías en los equipos informáticos instalados en la Central de Datos provocadas por problemas de temperaturas y humedades inadecuadas. Asimismo, con el sistema de seguridad física implantado se logró reducir el riesgo de posibles robos de equipos informáticos, salvaguardando de esta manera el patrimonio tecnológico del CPD, asegurando los niveles de continuidad del sistema de información del negocio y reduciendo los costos operativos.

2.- La implementación de la propuesta conllevó a un incremento en el índice de satisfacción de los usuarios de la red USAT por la continuidad de los servicios que brinda esta debido a una mejor gestión de riesgos sobre seguridad física en el Centro de Datos.

3.- Se logró aumentar el ciclo de vida útil de los equipos informáticos instalados en el CPD debido a que estos operan ya en un ambiente que cumple con sus especificaciones técnicas en lo que respecta a niveles de temperatura y humedad recomendados.

# VII. RECOMENDACIONES:

- Si en el futuro se desea integrar varios sistemas de seguridad física en ambientes estratégicos, se propone un estudio de factibilidad sobre implementación de sensores inalámbricos basados en el estándar IEE 802.15 (ZigBee).

- En ambientes tecnológicos donde sea necesario interconectar una red extensa de dispositivos como sensores, principalmente de temperatura y humedad como parte de un sistema de seguridad física, se propone la implementación del protocolo 1-Wire diseñado por Dallas Semiconductor que simplifica la labor de interconexión, captura y manejo de datos de estos dispositivos.

# VIII. REFERENCIAS BIBLIOGRÁFICAS


- Christopher, W.; Holistic Management: Managing What Matters for Company Success, John Wiley & Sons, USA, 2007, p. 10-11

- Contos, B.; W. Crowell; C. DeRodeff; D. Dunkel; E. Cole; Physical and Logical Security Convergence, Syngress, USA, 2007, p. 20-51

-Lawrence J; Effective Physical Security, Elsevier, USA, 2004

- American Society of Heating, Refrigerating and Air-Conditioning Engineerss, INC; Indoor Air Quality Guide, Atlanta, 2011.

- Brian, E; Arduino: Manual de Programación, First Edition, California, 2007

- Artero, O; Arduino: Curso práctico de formación, Alfaomega, México, 2013

- Monk, S; 30 Arduino Projects, McGraw-Hill, USA, 2010

- Karvinen, K.;Karvinen T; Make: Arduino Bots and Gadgets, O'Reilly Media, Canada, 2011

- Gertz, E.; Di Justo, P; Environmental Monitoring with Arduino, O'Reilly Media, USA, 2012

- Banzi, M; Getting Started with Arduino, O'Reilly Media, USA, 2011

- Oxer, J; Bleming, Hugh; Practical Arduino: Cool Projects for Open Source Hardware,

- Margolis, M; Arduino Cookbook, O'Reilly Media, USA, 2012

**REFERENCIAS ELECTRÓNICAS:**

[1] Jeff Sloan, Data Center Dilemma, Estados Unidos.
Disponible en: https://www.ashrae.org/resources--publications/periodicals/ashrae-journal/features/data-center-dilemma#figure1
Consultado en (01/07/2013)

[2] Di Muccio, Carlos. (2011) "Optimizando la capacidad, disponibilidad y eficiencia de la infraestructura de Data Centers", Argentina.
Disponible en: http://www.la.logicalis.com/pdf/LogicalisNow17.pdf
(Consultado: 10/07/2013).

[3] Cisco (2010) "University Builds Physical Security Framework for Growth. USA
Disponible en:
https://docs.google.com/gview?url=http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps9674/ps9687/case_study_c36-611693.pdf&chrome=true
Consultado en: 15/07/2013

[4] ASHRAE TC9.9 Mission Critical Facilities (infraestructura de misión crítica)."Thermal Guidelines for Data Processing Environments" (pautas sobre temperatura para entornos de procesamiento de datos). 2004
Disponible en:
http://www.eni.com/green-data-center/it_IT/static/pdf/ASHRAE_1.pdf
Consultado en: 26/07/2013

[5] Christian Cowan, "Como monitorear las amenazas físicas en un centro de Datos". 2010. Disponible en:
http://www.fasor.com.sv/whitepapers/whitepapers/Monitoreo/Como_monitorear_amenazas_fisicas_en_centro_de_datos.pdf
Consultado en: (8/08/2013)

# Índice de Tablas

# Índice de Figuras.