FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PARA LABORATORIOS DE COMPUTACIÓN DE LA FICA

AUTORES

Gabriela Selene Guerrón Barrera

Daniel Rene Vargas Navas

AÑO

2018

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PARA LABORATORIOS DE COMPUTACIÓN DE LA FICA.

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingenieros en Redes y Telecomunicaciones.

Profesor Guía

Magister Iván Patricio Ortiz Garcés

Autores

Gabriela Selene Guerrón Barrera

Daniel Rene Vargas Navas

Año

2018

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido el trabajo, Diseño e implementación de un sistema de seguridad para laboratorios de computación de la FICA, a través de reuniones periódicas con los estudiantes Gabriela Selene Guerrón Barrera y Daniel Rene Vargas Navas, en el semestre 2018-2, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

Iván Patricio Ortiz Garcés
Magister en Redes de Comunicación
CI: 0602356776

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, Diseño e implementación de un sistema de seguridad para laboratorios de computación de la FICA, de Gabriela Selene Guerrón Barrera y Daniel Rene Vargas Navas, en el semestre 2018-2, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

_____

Carlos Marcelo Molina Colcha

Magister en Gestión de la Comunicaciones y Tecnologías de la Información

CI: 170962421-5

DECLARACIÓN AUTORÍA DEL ESTUDIANTE

“Declaramos que este trabajo es original, de nuestra autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

_____	_____
Gabriela Selene Guerrón Barrera	Daniel Rene Vargas Navas
CI: 1719110049	CI: 1721826327

AGRADECIMIENTOS

Agradezco a Jehová de todo corazón por darme la vida, salud, infinitas bendiciones y amor eterno. A mi papi Edgar por sus sabios consejos y su apoyo incondicional. A mi mami Tere porque ha sido el pilar fundamental para convertirme en la mujer que ahora soy. A mis ñaños Fer y Santy por estar a mi lado, no hay nadie mejor para compartir la vida. A mi querido enamorado Danny por tu paciencia y tu amor empezamos juntos y lo logramos mi amor. A mi jefe Alex Hermosa por su gran ayuda y por esa generosidad que lo caracteriza. A mi tutor Ing. Iván Ortiz por su importante apoyo y su gran apertura. A mis amigos que de una u otra manera estuvieron ahí para compartir esta bonita experiencia.

Gaby

AGRADECIMIENTOS

A mi mami Ceci, papi Rene y mi ñaña Cris, que hubo veces que ya no quería estudiar, pero estuvieron allí para darme ese empuje que necesitaba.

Agradezco a la familia Guerrón principalmente a Don Edgar que, aunque fue escaso el tiempo de conocernos, confió en mí y me ayudo a seguir con los estudios y a Señito Teresa que voy a recordar por siempre sus consejos.

A mi jefe Alex Hermosa quien supo comprender mi situación de estudio y nos ayudó siempre para ello.

A todos mis amigos y profesores que de alguna u otra manera contribuyeron en esta meta cumplida.

Daniel

DEDICATORIA

Dedico este logro a Jehová por brindarme las oportunidades para salir adelante. A mis papitos Edgar y Tere porque ahora sus semillas están dando frutos, lo logramos juntos mis amados papi y mami. A mi ñaña Fer como un día lo soñamos confidente y mejor amiga, este logro te lo dedico a la distancia. A mi ñaño Santy por tu inteligencia y madurez al llegar con el consejo en el momento preciso, espero que llegues tan lejos como lo has soñado. A mi enamorado Danny has sido el mejor compañero que Dios puso en mi camino, nuestras victorias son sueños que jamás dimos por perdidos. Gracias por estar en mi vida son lo más importante que tengo y los llevo en mi corazón siempre.

Gaby

DEDICATORIA

Dedico este proyecto primero a Dios, por estar conmigo y darme su bendición y entre tanta de ellas despertar cada día y poder ver a mi familia, la cual me apoyan el día a día para poder superarme y seguir cumpliendo mis metas.

A mi madre y padre que sin duda sus concejos me han llevado hacer la persona que soy, entre tantas virtudes la humildad y perseverancia.

A mi hermanita que con su apoyo me dio seguridad de darlo todo en el estudio.

A mi Gabbyta con quien tomamos un reto difícil pero junto vimos que nada es imposible.

Daniel

RESUMEN

El presente proyecto implementa un sistema de seguridad física perimetral, mediante elementos convencionales y no convencionales como sensores de movimiento, sistema biométrico por huella digital, puntos de acceso inalámbricos y cámaras IP, en la que todos los servicios convergen en una página web, cuyo servicio se encuentra alojada en el Data Center Académico.

Para la implementación del proyecto se realizó un estudio de los componentes físicos y lógicos que conforman un Data Center, revisando conceptos de virtualización, networking, almacenamiento, computing, seguridad y gestión de Data Center. Se tuvo que revisar estos conceptos ya que la aplicación web está alojada en el Data Center Académico y debemos comprender su funcionamiento.

Esta propuesta de implementación examina los estándares que rigen en la actualidad para sistemas de seguridad con servicios en Data Center.

Con estos estándares se procedió a realizar un diseño físico y lógico de los dispositivos, para posteriormente dar paso a la implementación de los elementos convencionales y no convencionales mencionados anteriormente y en donde se evidencia mediante pruebas realizadas con el Data Center Académico, el correcto funcionamiento de los servicios, comprobando que existe un control de monitoreo de todo el sistema.

ABSTRACT

This project implements a perimeter physical security system, using conventional and non-conventional elements such as motion sensors, biometric fingerprint system, wireless access points and IP cameras, in which all the services converge on a web page, whose service is housed in the Academic Data Center.

For the implementation of the project, an investigation was made of the physical and logical components that make up a Data Center, reviewing concepts of virtualization, networking, storage, computing, security and data center management. These concepts had to be revised since the web application is hosted in the Academic Data Center and we must understand its operation.
This implementation proposal examines the standards currently in place for security systems with Data Center services.

With these standards we proceeded to make a physical and logical design of the devices, to subsequently give way to the implementation of the conventional and non-conventional elements mentioned above and where it is evidenced by tests carried out with the Academic Data Center, the correct functioning of the services, verifying that there is a monitoring control of the entire system.

ÍNDICE

INTRODUCCIÓN 1

Alcance 3

Justificación del proyecto 3

Objetivos 4

Objetivo General 4

Objetivos Específicos 4

1. CAPÍTULO I: FUNDAMENTOS TEÓRICOS. 5

1.1 Data Center. 5

1.2 Sitio Data Center. 7

1.2.1 Planificación de elemento críticos. 7

1.3 Infraestructura Data Center. 8

1.3.1 Networking. 8

1.3.2 Computing. 12

1.3.3 Cloud Computing. 17

1.3.4 Almacenamiento. 19

1.3.5 Virtualización. 21

1.3.6 Seguridad de Data Center. 24

1.3.7 Gestión de un Data Center. 28

1.4 Infraestructura actual del Data Center Académico. 28

2. CAPITULO II: ESTÁNDARES APLICADOS AL DATA CENTER ACADÉMICO. 32

2.1 Definición de estándar. 32

2.2 Historia 33

2.3 Tipos de estándares. 36

2.4 Organizaciones reguladoras de estándares. 36

2.5 Estándar ANSI / TIA 942. 37

2.6 Historia de ANSI / TIA 942. 38

2.7 Definición de ANSI / TIA 942. 38

2.8 Niveles de clasificación de un Data Center según ANSI / TIA 942. 39

2.8.1 Tier I - Nivel 1 (Data Center Básico). 39

2.8.2 Tier II – Nivel 2 (Componentes redundantes). 40

2.8.3 Tier III – Nivel 3 (Mantenimiento concurrente). 42

2.8.4 Tier IV – Nivel 4 (Tolerante a fallos). 43

2.8.5 Tier V – Nivel 5. 44

2.9 Ventajas de uso de los Tier. 45

2.10 Especificaciones ANSI/TIA-942-A. 46

3. CAPITULO III. IMPLEMENTACIÓN DE SERVICIOS EN EL DATA CENTER ACADÉMICO. 57

3.1 Situación actual para el proyecto de seguridad. 57

3.1.1 Ubicación geográfica del Data Center Académico Queri – Udla. 57

3.1.2 Planos de los laboratorios Sede Queri – Udla. 60

3.1.3 Laboratorio 466. 61

3.1.4 Laboratorio 464. 62

3.1.5 Laboratorio 461. 62

3.2 Problemática de la situación actual. 62

3.3 Análisis de requerimientos. 63

3.3.1 Requerimientos Laboratorio 466. 63

3.3.2 Requerimientos Laboratorios 464. 64

3.3.3 Requerimientos Laboratorio 461. 65

3.4 Diseño para Sistema de seguridad. 66

3.4.1 Sistemas de seguridad por cámaras. 67

3.4.2 Sistemas de seguridad por biométrico. 77

3.4.3 Sistemas de seguridad por sensores. 82

3.4.4 Seguridad por Access Point. 91

3.5 Dispositivos que se van a implementar. 93

3.6 Diseño de sistema de seguridad. 96

3.7 Manuales de configuración de dispositivos a implementar. 97

3.7.1 Instalación de cámaras FOSCAM. 97

3.8 Instalación de biométrico ZKTECO MA300. 101

3.9 Instalación de access point HG110. 110

3.10 Instalación de página Web 112

3.11 Diseño de la red de comunicación. 119

3.11.1 Áreas de seguridad. 119

3.11.2 Direccionamiento para los equipos de red. 119

4. CAPITULO IV. PRUEBAS DEL SISTEMA. 121

5. CONCLUSIONES Y RECOMENDACIONES. 130

5.1 Conclusiones.....132
5.2 Recomendaciones.....135

REFERENCIAS.....134

ANEXOS.....140

ÍNDICE DE FIGURAS

FIGURA 1. COMPONENTES DATA CENTER. 6
FIGURA 2. SOLUCIÓN DE UNA RED CABLEADA/INALÁMBRICA. 9
FIGURA 3. ARQUITECTURA LEAF-SPINE. 10
FIGURA 4. ARQUITECTURA TOR. 11
FIGURA 5. ARQUITECTURA EOR. 11
FIGURA 6. EVOLUCIÓN DE DATA CENTER. 13
FIGURA 7. SERVICIOS IAAS, PAAS, SAAS. 18
FIGURA 8. ARQUITECTURAS DE ALMACENAMIENTO. 20
FIGURA 9. SEGURIDAD FÍSICA DE DATA CENTER. 25
FIGURA 10. ESTÁNDARES EN DATA CENTER 32
FIGURA 11. LOGO DE LA COMISIÓN INTERNACIONAL ELECTRÓNICA. 34
FIGURA 12. LOGO DEL AMERICAN NATIONAL STANDARDS INSTITUTE. 35
FIGURA 13. LOGO DE LA UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. 35
FIGURA 14. ESQUEMA TIER I. 40
FIGURA 15. ESQUEMA TIER II. 41
FIGURA 16. ESQUEMA TIER III. 42
FIGURA 17. ESQUEMA TIER IV. 43
FIGURA 18. ESQUEMA TIER IV. 45
FIGURA 19. ESQUEMA TIER IV. 47
FIGURA 20. TOPOLOGÍA DE DISTRIBUCIÓN DATA CENTER. 48
FIGURA 21. MANEJO DE LA TERMINOLOGÍA. 49
FIGURA 22. CONECTORES DE FIBRA. 50
FIGURA 23. DISTRIBUCIÓN DE PASILLOS CALIENTES Y FRÍOS. 51
FIGURA 24. SEGURIDAD FÍSICA POR CAPAS 53
FIGURA 25. UBICACIÓN GEOGRÁFICA CAMPUS QUERI. 58
FIGURA 28. LABORATORIO 464. 59
FIGURA 29. LABORATORIO 461. 60
FIGURA 30. LABORATORIOS PLANTA BAJA. 60
FIGURA 31. LABORATORIO466. 61
FIGURA 32. SISTEMA DE GESTIÓN DE VÍDEO. 68
FIGURA 33. GRABADOR DE VÍDEO. 68

FIGURA 34. SOFTWARE DE ADMINISTRACIÓN DE VIDEOVIGILANCIA. 69
FIGURA 35. EQUIPOS DE VISUALIZACIÓN. 69
FIGURA 36. LEDS INFRARROJOS. 70
FIGURA 37. DOMOS DE PROTECCIÓN. 71
FIGURA 38. SENSORES. 71
FIGURA 39. CABLE ETHERNET. 72
FIGURA 40. CABLE POE. 72
FIGURA 41. CÁMARA BULLET, MARCA DAHUA. 73
FIGURA 42. CÁMARA DOMO, MARCA DAHUA. 74
FIGURA 43. CÁMARA DOMO, MARCA EPCOM. 74
FIGURA 44. CÁMARA OCULTA. 75
FIGURA 45. CÁMARA CON LENTE INFRARROJO. 75
FIGURA 46. CÁMARAS IP. 76
FIGURA 47. HUELLA DACTILAR. 79
FIGURA 48. PROCESAMIENTO DE HUELLA DIGITAL. 79
FIGURA 49. PROCESAMIENTO DE LA VOZ. 80
FIGURA 50. PROCESAMIENTO PARA ANÁLISIS DE LOS OJOS. 81
FIGURA 51. SENSORES PERIMETRALES. 85
FIGURA 52. SENSOR DE VIBRACIÓN. 86
FIGURA 53. SENSOR MAGNÉTICO. 87
FIGURA 54. CABLE SENSOR MICROFÓNICA DE SEGURIDAD. 88
FIGURA 55. SENSOR DE MOVIMIENTO POR MICROONDAS. 89
FIGURA 56. SENSOR INFRARROJO. 89
FIGURA 57. PÁGINA WEB DE CÁMARAS. 97
FIGURA 58. APP DE CÁMARA. 97
FIGURA 59. APP WINDOWS DE CÁMARA 98
FIGURA 60. CONFIGURACIÓN DE IP CÁMARA. 98
FIGURA 61. INGRESO CONFIGURACIÓN DE CÁMARA. 98
FIGURA 62. CONFIGURACIÓN CÁMARA. 99
FIGURA 63. VISTA DE CÁMARA. 99
FIGURA 64. CONFIGURACIÓN DE RED DE CÁMARA. 99
FIGURA 65. ACTIVACIÓN DE SENSOR DE MOVIMIENTO DE CÁMARA. 100

FIGURA 66. CONFIGURACIÓN SMTP DE CÁMARA. 100
FIGURA 67. INFORMACIÓN DE LA CÁMARA. 101
FIGURA 68. PÁGINA PRINCIPAL NAVEGADOR ZKTECO. 101
FIGURA 69. CARPETA DE DESCARGA DE SOFTWARE. 102
FIGURA 70. PÁGINA PRINCIPAL PARA LA INSTALACIÓN DE ZKACCESS 3.5 102
FIGURA 71. INSTALACIÓN DE ZKACCESS 3.5. 103
FIGURA 72. PETICIÓN DE CREDENCIALES PARA ZKACCESS 3.5. 103
FIGURA 73. SOFTWARE ZKACCESS. 104
FIGURA 74. CONFIGURACIÓN EN PARÁMETROS DEL SISTEMA. 104
FIGURA 75. AGREGAR DISPOSITIVO. 104
FIGURA 76. CONFIGURACIÓN PARÁMETROS TÉCNICOS DE BIOMÉTRICO. 105
FIGURA 77. ELECCIÓN DE DISPOSITIVOS DE CONTROL. 105
FIGURA 78. EQUIPO AGREGADO. 106
FIGURA 79. SINCRONIZACIÓN DEL DISPOSITIVO. 106
FIGURA 80. AGREGAR USUARIOS AL EQUIPO. 106
FIGURA 81. CONFIGURACIÓN DE USUARIOS. 107
FIGURA 82. CONFIGURACIÓN DE DEPARTAMENTOS. 107
FIGURA 83. AGREGAR DISPOSITIVOS A LAS PUERTAS DE ACCESO. 108
FIGURA 84. MONITOREO EN TIEMPO REAL. 108
FIGURA 85. CONFIGURACIÓN TIEMPOS DE ACCESO. 109
FIGURA 86. BITÁCORA DE EVENTOS. 109
FIGURA 87. INGRESO A LA CONFIGURACIÓN INTERNA DEL MÓDEM. 110
FIGURA 88. ACCESO A CREDENCIALES. 110
FIGURA 89. CAMBIO DE NOMBRE DE RED WIFI. 111
FIGURA 90. CAMBIO DEL MODO DE SEGURIDAD. 111
FIGURA 91. CAMBIO DE LA CONTRASEÑA DE LA RED WIFI. 112
FIGURA 92. PÁGINA PRINCIPAL PARA DESCARGAR WAMPSERVER. 112
FIGURA 93. INTERFAZ DE DESCARGA. 113
FIGURA 94. PÁGINA PARA ACEPTAR TÉRMINOS Y CONDICIONES. 113
FIGURA 95. ELEGIMOS LA UBICACIÓN PARA INSTALAR WAMPSERVER. 114
FIGURA 96. CASILLAS PARA CREAR UN ICONO DE ESCRITORIO. 114
FIGURA 97. EJECUTAMOS LA INSTALACIÓN. 115

FIGURA 98. INSTALACIÓN EN EJECUCIÓN. 115
FIGURA 99. ELEGIMOS QUE NAVEGADOR UTILIZAR. 116
FIGURA 100. CONFIGURACIÓN SMTP. 116
FIGURA 101. PROCESO DE INSTALACIÓN FINALIZADO. 117
FIGURA 102. WAMPSERVER EJECUTÁNDOSE EN SEGUNDO PLANO. 117
FIGURA 103. ACTIVAR COMPONENTES PHP. 118
FIGURA 104. APERTURA WAMPSERVER. 118
FIGURA 105. DIAGRAMA DE INSTALACIÓN DE LOS EQUIPOS DE RED. 120
FIGURA 106. DISEÑO FÍSICO DE LA RED. 121
FIGURA 108. LOGIN PÁGINA WEB 122
FIGURA 109. CONTRASEÑA ENCRIPTADA. 122
FIGURA 110. INTERFAZ DE LA PÁGINA WEB. 123
FIGURA 111. FORMULARIO DE USUARIOS. 123
FIGURA 112. FORMULARIO DE USUARIOS CON TODOS LOS CAMPOS. 124
FIGURA 113. REGISTRO DE INCIDENCIAS. 124
FIGURA 114. CORREO DE ALERTAS DE LAS CÁMARAS. 125
FIGURA 115. CORREO CON IMÁGENES DE LAS CÁMARAS. 125
FIGURA 116. ESTATUS CÁMARAS. 126
FIGURA 117. FIGURA CÁMARA 1 126
FIGURA 118. CÁMARA 2. 127
FIGURA 119. CÁMARA 3. 127
FIGURA 120. REGISTRO DE TIEMPOS OPERATIVOS. 128
FIGURA 121. DATOS DE BIOMÉTRICO. 128
FIGURA 122. TABLA ARP DEL AP. 129
FIGURA 123. ESTADOS DISPOSITIVOS. 129

INDICE DE TABLAS

TABLA 1. COMPARACIÓN DE LA EVOLUCIÓN DE LOS DATA CENTER. 13
TABLA 2. COMPONENTES SUBSISTEMA NETWORKING. 29
TABLA 3. COMPONENTES SUBSISTEMA CÓMPUTO. 29
TABLA 4. COMPONENTES SUBSISTEMA ALMACENAMIENTO. 29
TABLA 7. EL OBJETIVO Y MEDIDAS DE SEGURIDAD POR CAPA 53
TABLA 8. MUESTRA DE CADA CAPA DE LA TIER-492-SEGURIDA FISICA. 54
TABLA 9. SEGURIDAD POR CAPAS PARA LOS TIER. 55
TABLA10. PROBLEMÁTICA DE LA SITUACIÓN ACTUAL. 62
TABLA 11. REQUERIMIENTOS LABORATORIO 466 BLOQUE 4 SEDE QUERI – UDLA. ... 63
TABLA 12. REQUERIMIENTOS LABORATORIO 464 BLOQUE 4 SEDE QUERI – UDLA. ... 65
TABLA 13. REQUERIMIENTOS LABORATORIO 461 BLOQUE 4 SEDE QUERI – UDLA. ... 65
TABLA 14. VENTAJAS Y DESVENTAJAS DE LAS CÁMARAS DE SEGURIDAD 76
TABLA 15. VENTAJAS Y DESVENTAJAS DE LOS SISTEMAS BIOMÉTRICOS. 81
TABLA 16. VENTAJAS Y DESVENTAJAS DE USO DE SENSORES. 91
TABLA 17. MOTIVO DE ELECCIÓN DE EQUIPOS A IMPLEMENTAR. 93
TABLA 18. ELEMENTOS DE SISTEMA DE SEGURIDAD. 94
TABLA 19. DISEÑO DEL SISTEMA DE SEGURIDAD. 96
TABLA 20. USUARIOS POSIBLES PARA CONECTARSE. 119
TABLA 21. DIRECCIONAMIENTO DE EQUIPOS DE RED. 120

INTRODUCCIÓN

Actualmente nos encontramos en un siglo donde la mayoría de las cosas tecnológicas se han automatizado y sin duda los beneficios que nos brindan los sistemas de seguridad, conectividad de las redes, sistemas informáticos, servidores, sistemas de comunicación, entre otros han sido exitosos y van evolucionando día a día para brindar más comodidades ante los usuarios.

El crecimiento empresarial y comercial en el mundo trae consigo la rápida evolución en la infraestructura de TI en una organización o institución, para el almacenamiento de datos y soporte de información, por lo que es necesario contar con un Centro de Datos (Data Center) que funcione de manera óptica.

En las grandes empresas el manejo de datos e información cada vez contienen volúmenes más altos por lo que se usan dispositivos móviles los cuales sirven para realizar búsquedas, manejar datos o utilizar aplicaciones cuya información principal esta almacenada en un Data Center, pero el acceso se lo realiza de forma remota para trabajar con la información necesaria para el momento.

El manejo y la funcionalidad de un Data Center es fundamental para que las actividades de desarrollo de un negocio cada vez crezcan más, por lo tanto, es muy importante llevar el control, seguridad y monitoreo de los equipos que conforman el Data Center así como también los espacios donde se maneja los activos más importantes y valiosos de una organización mismos que solo se puede operar por un grupo de personas autorizadas bajo las políticas de seguridad establecidas de manera que no se generen pérdidas.

Un Data Center ayuda al almacenamiento y distribución de la información de cualquier organización brindando mayor productividad y resguardo de los datos, teniendo como objetivo brindar disponibilidad, seguridad y eficiencia.

En la actualidad el Data Center Experimental adquirido por la UDLA, se lo está utilizando para el desarrollo e implementación de proyectos de base tecnológica y altamente escalables e innovadores, pero no existe un sistema de vigilancia y

monitoreo que sea apoyado en el Data Center actual con el fin de tener un cuidado de los laboratorios de la FICA.

Las tecnologías implementadas en los Data Center de hoy están cambiando rápidamente por lo cual muchas empresas se encuentran integrando nuevas soluciones tecnológicas para que sus organizaciones se modernicen y evolucionen. La mayoría requieren niveles adecuados de prestación de servicios, la eficiencia de costos y la alineación con los objetivos empresariales. Para algunos Data Center significa brindar niveles de vanguardia en disponibilidad, flexibilidad y escalabilidad; a la vez que para otros la meta puede ser proporcionar niveles de servicios “suficientes” mientras reducen a un mínimo los nuevos gastos de capital. (IBM, 2014).

La video vigilancia IP tiene como modelo, que la velocidad de fotogramas de video es menor, pero permite el almacenamiento de copias de seguridad con el ancho de banda disponible o que los usuarios deben asumir el costo para administrar dicho sistema, además de facilitar la virtualización de servidores, la monitorización de recursos en tiempo real y la automatización de aprovisionamiento del servicio.

Uno de los servicios que están entrando en auge es el servicio de video vigilancia con almacenamiento en el Data Center ya que el almacenamiento de video vigilancia representado en los últimos años por los VHS, DVR y NVR entre otros servidores de almacenamiento y sus soluciones IP se están enfrentando hoy en día a una nueva transformación en la parte económica, confidencial y sobre todo alta disponibilidad.

Los servicios de las redes y telecomunicaciones son de suma importancia en cualquier ámbito de la vida empresarial, por lo que se llama sistemas críticos, ya que se deben proveer prestaciones ininterrumpidas para las operaciones de las empresas. Por lo que se debe tener sumo cuidado en el lugar donde se albergan los distintos servicios, para garantizar su seguridad física y estándares que mejoren la funcionalidad y disponibilidad.

Alcance

Consiste en realizar un análisis de la situación actual del Data Center Académico de la UDLA tomando en cuenta soluciones de seguridad y almacenamiento a fin de alojar una herramienta WEB de código abierto para monitoreo proactivo capaz de remitir mensajes de alerta temprana hacia los administradores de red.

Adicionalmente contará con un sistema de vigilancia controlado por puntos de acceso inalámbrico, sensor de movimiento, control mediante un sistema biométrico con huella digital y Cámaras IP, que registrarán accesos y conexiones no autorizadas fuera de horarios establecidos a las instalaciones del Data Center Académico de la UDLA – SEDE QUERI.

Justificación del proyecto

Al desarrollar este proyecto mediante la implementación de servicios de seguridad que serán almacenados en el Data Center Experimental de la UDLA, garantizamos tener un sistema moderno, proactivo, confiable y escalable para soluciones de seguridad futuras mediante dispositivos convencionales y no convencionales. Este servicio es escalable ya que se podrá implementar para otros laboratorios de la UDLA – FICA que requieran seguridad y monitoreo constante.

Además, este proyecto puede servir de apoyo para temas de titulación futuros en los que se requiera dar servicios trabajando en conjunto con el Data Center para avances de la universidad.

El proyecto beneficia a todos los usuarios de la comunidad UDLA y como un sistema para implementarlo en un proyecto real donde se brinda seguridad e integridad de los datos almacenados o procesados en el Data Center con disponibilidad y accesibilidad, de tal manera que las solicitudes hechas por los usuarios sean atendidas con prontitud.

Este proyecto piloto será una base consolidada con el fin de seguir añadiendo sistemas de alta escalabilidad y diferentes servicios de acuerdo con la necesidad

que se vaya presentado en el futuro, en donde para validar el funcionamiento del mismo se realizarán las respectivas pruebas en todos los escenarios posibles.

Objetivos

Objetivo General

Implementar un sistema de vigilancia mediante Puntos de Acceso Inalámbrico, Sensor de Movimiento, Sistema Biométrico por Huella Digital y Cámaras IP, anclados a una herramienta de monitoreo proactivo capaz de remitir mensajes de alerta temprana utilizando la infraestructura del Data Center Académico.

Objetivos Específicos

- Analizar la situación actual referente a la infraestructura tecnológica del Data Center Académico de la UDLA – Sede Queri.

- Analizar parámetros de Marco Regulatorio para instalar los servicios de video vigilancia IP, sensor de movimiento, sistema biométrico, puntos de acceso inalámbrico y monitoreo proactivo.

- Implementar el sistema de video vigilancia mediante el uso de puntos de acceso inalámbrico, sensor de movimiento, sistema biométrico por huella digital y Cámaras IP.

- Implementar una herramienta de monitoreo proactivo de código abierto anclada al sistema de video vigilancia e infraestructura del Data Center Académico.

- Realizar las pruebas respectivas y validar que todos los servicios trabajen de manera correcta en todos los horarios de control.

1. CAPÍTULO I: FUNDAMENTOS TEÓRICOS.

Los sistemas de seguridad física como lógica son de vital importancia para una empresa u organización, ya que resguardan la confidencialidad integridad y disponibilidad. El sistema de seguridad que vamos a implementar es un servicio que está tomando auge en estos años, donde las empresas no invierten en adquirir espacio de almacenamiento, procesamiento, tecnología o red, si no que invierten en servicios en Data Centers.

Este proyecto maneja la descripción de lo que es un Data Center y las tecnologías que intervienen en él, además que al finalizar este capítulo 1 tendremos un análisis de cómo está el Data center Académico de la UDLA en cuanto a los recursos mencionados.

1.1 Data Center.

Un Data Center es un sitio que tiene infraestructura con servidores cuyo software se está ejecutándose para el servicio de páginas web, correo, aplicaciones, entre otras.

Según Gartner (2018), El centro de datos es el departamento de una empresa que alberga y mantiene sistemas de tecnología de la información (TI) y almacenes de datos: sus mainframes, servidores y bases de datos. Este departamento y todos los sistemas residían en un solo lugar físico, de ahí el nombre del centro de datos.

En un Data Center el objetivo principal es cumplir con servicios sin interrupciones cumpliendo con características:

- Escalable: soportar el crecimiento exponencial sin interrupciones cumpliendo con una planificación y estimación correcta así también con el orden que los equipos que estarán instalados para una mejor administración.

- Flexible: La evolución de la tecnología trae consigo nuevas tendencias tanto en la parte de hardware como software y en

un Data Center es importante que se adapte fácilmente a cualquier cambio que se realice o se decida migrar.

- Confiable: Todo Data Center debe tener un plan de contingencia para tener alta disponibilidad y robustez sin interrupciones.

- Seguro: Para mantener un sistema seguro se debe pensar en el peor escenario posible ya que existen varios posibles ataques que trataran de interrumpir los servicios.

- Modular: es un diseño donde nos va a permitir replicar, mover, balancear, y manejar la información o aplicaciones en Data Center.

- Estandarizado: Hay que tener procedimientos de operación cumpliendo políticas internacionales o nacionales establecidas.

Un Data Center cuenta de varios recursos que son importantes para su funcionamiento y se complementan unos con otros y las clasificaremos como se muestra en la siguiente figura 1:

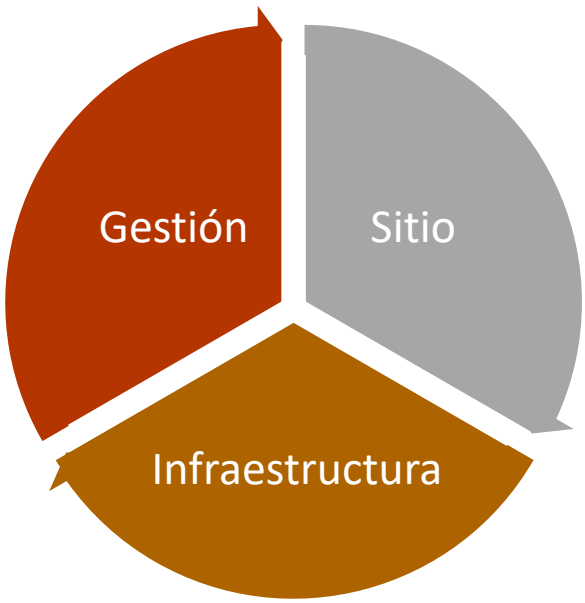


Figura 1. Componentes Data Center.

1.2 Sitio Data Center.

Para escoger un sitio adecuado para un Data Center tenemos que tener claro diferentes limitaciones como geográficas, legales y económicas. En cuanto a lo geográfico, es mejor elegir un lugar donde existan bajas temperaturas, para tener un ahorro económico en la ventilación de los equipos del Data Center además de escoger regiones donde se tenga una adecuada comunicación, suministros eléctricos y acceso entre otras.

Ya al término legal, hay regiones en las que existen prohibiciones de que estas infraestructuras estén cerca de sitios domiciliarios, aeropuertos, industrias, etc.

Es así como las empresas tratan de ahorrar en recursos para estos centros utilizando energía renovable, como por ejemplo según el portal el ComputerWorld (2015), informa que Facebook construye un Data Center de Fort Worth que se refrigerará utilizando el aire frío recogido de las áreas externas en lugar de recurrir a sistemas intensivos basados en equipos de aire acondicionado. El sitio también utilizará energía renovable generada en granja eólica basada en Clay County que permite la creación de 200 megavatios.

1.2.1 Planificación de elemento críticos.

Los Data Center tienen que cumplir con las expectativas y requerimientos para tener un tipo de negocio rentable, es por eso por lo que se debe planificar la:

- Seguridad
- Espacio
- Energía
- Condiciones ambientales
- Conectividad

1.3 Infraestructura Data Center.

La infraestructura de un Data Center contamos con la parte de software y hardware. En las que describimos la parte del networking, cómputo, almacenamiento, seguridad, virtualización y las aplicaciones.

1.3.1 Networking.

Este término ha evolucionado desde 1944 cuando apareció el Mark1 el primer computador construido por IBM en donde sus conexiones internas eran conectadas mediante buses de baja latencia. En ese periodo lo primordial era la extracción de información en medios físicos para su transporte.

La tecnología siguió con su desarrollo y nacieron las redes interconectadas mediante redes no estandarizadas esto fue previo a la estandarización de Ethernet que después de evolucionar más de 30 años ha mejorado en redes de mayo velocidad y ancho de banda y hasta el momento han cumplido con las demandas del mundo actual.

Según el portal de Cisco (2018), Ethernet se utiliza para aproximadamente el 85 por ciento de las PC y estaciones de trabajo conectadas a LAN del mundo. Ethernet es la principal tecnología LAN debido a que es fácil de entender, implementar, administrar y mantener además de permitir implementaciones de red de bajo costo y una amplia flexibilidad topológica para la instalación de la red y garantizar la interconexión y operación exitosas de productos que cumplen con los estándares, independientemente del fabricante.

1.3.1.1 Networking campus vs Networking Data Center.

Tenemos que tener en claro que en el mundo de las redes existen dos diferencias en cuanto al tráfico, capacidad, topologías y conexiones a la red y es así como nacen estos conceptos de Networking campus y Networking Data Center.

- Networking campus son redes LAN (Redes Área Local), en donde los usuarios se conectan a la red junto con sus dispositivos (celulares, ordenadores, Tablets, etc.) en donde los equipos de red más común

utilizados son los switch y routers que manejan un IOS (Sistema Operativo) con un Kernel Monolítico que ejecutan tareas en primer y segundo plano, además que su medio de transmisión es la fibra óptica, cobre, cable coaxial, entre otras.

Cabe recalcar que el tráfico de este tipo de red crece de norte a sur, puesto que si queremos conectar tres switch estos los vamos a conectar en cascada, en si crece la red de norte a sur. A continuación, se detalla un gráfico del tipo de topología.

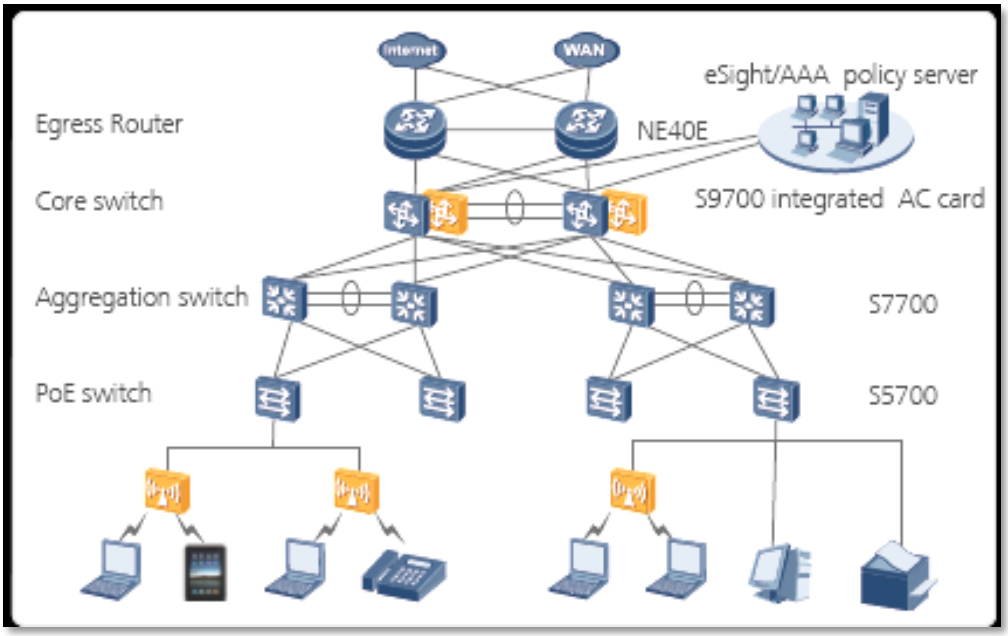


Figura 2. Solución de una red cableada/inalámbrica.
Tomado de (Huawei, 2011).

- Networking Data Center este tipo de red no es más que un conjunto de almacenamiento, red, cómputo que administran una carga de trabajo y responden a solicitudes de acciones de los clientes. En este tipo de red estamos hablando de los Data Centers actuales donde se necesitan redes escalables, eficientes y redundantes.

Utilizan equipos que ya manejan gran capacidad de datos, como por ejemplo los switch Nexus de cisco, que utilizan un IOS (Sistema Operativo) con un Kernel Modular, lo que significa que habilita procesos según se los necesite.

Este tipo de red maneja una arquitectura Leaf Spine que es una topología de red doble capa. Tiene un tráfico de datos de la red en sentido este-oeste en lugar de tráfico norte-sur.

La topología es sencilla de entender ya que se pone de Leaf swiches y Spine swiches. Los Leaf swiches conectan hacia los servidores y el almacenamiento mientras que los Spine swiches se conectan a los Leaf swiches.

Los Leaf swiches se conectan hacia los Spine formando una conexión tipo malla, de esa manera forman la capa de acceso la cual genera los puntos de conexión hacia los servidores. Una topología Leaf Spine puede ser capa 2 o capa 3 dependiendo de cómo estén conectados los equipos. Como se puede ver en la siguiente figura3.

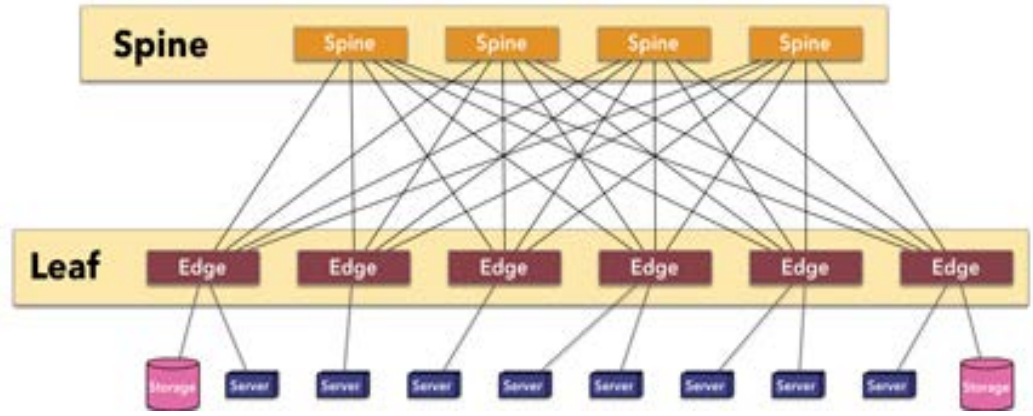


Figura 3. Arquitectura Leaf-Spine.
Tomado de (Ferro, 2013).

1.3.1.2 Diseño físico del Data Center.

Para el diseño físico de un Data Center tenemos dos modelos:

- Top of Rack (ToR), es un diseño donde a los switch se les conectan en la parte superior del rack en donde no se requiere demasiado cableado y se reduce costos en implementación.

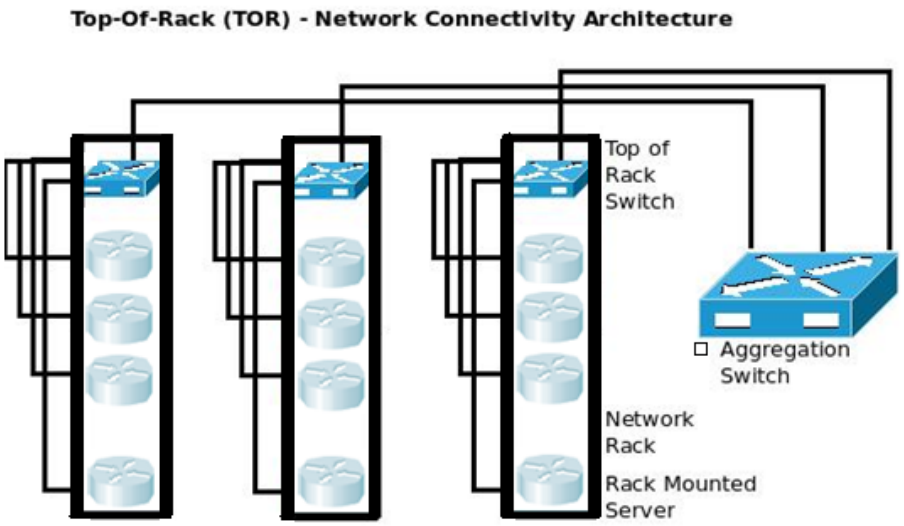


Figura 4. Arquitectura ToR.
Tomado de (Kan, 2012).

- End of Rack (EoR), es un diseño que admite varias conexiones de servidores, en si cada servidor está en un rack y estos conectados a un switch común, lo que hace que se tenga una ventaja de menos switch y una vida útil con alta disponibilidad.

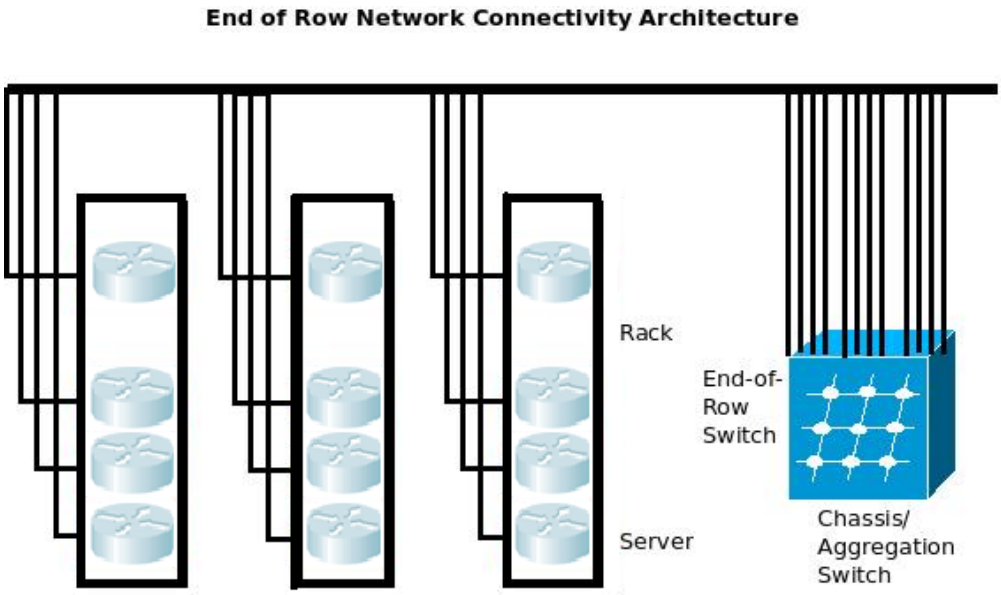


Figura 5. Arquitectura EoR.
Tomado de (Kan, 2012).

1.3.1.3 Futuro de Networking.

Actualmente las redes siguen encaminadas a mejorar la velocidad con un ancho de banda amplio, una de estas tecnologías es la llamada InfiniBand, que es una tecnología desarrollada por Infiniband Trade Association, esta tecnología lo que hace es tener una comunicación de alta velocidad con un bus de serie direccional, llegando a ofrecer velocidades de hasta 2.0 Gbps, en un nodo doble hasta 4 Gbps y en un nodo cuádruples de 96 Gbps, utilizando la codificación de 8B/10B, para la transmisión de bits en líneas de alta velocidad.

1.3.2 Computing.

Los Data center han ido evolucionando con forme la tecnología hace nuevos descubrimientos, desde que apareció el primer computador utilizando ya un sistema centralizado, se hablaba de los Data Center 1.0 en cual se tenía una sola función de guardar archivos.

Se poseía una sola ubicación física que significaba menor redundancia y acompañado de menor poder de procesamiento y la administración por una organización, donde su crecimiento dependía de los equipos que iban adquiriendo.

Los Data Center 2.0 nacieron con la necesidad de ser sistemas distribuidos ya que se iban manejando conjunto de datos más significativos además de gran variedad de datos.

Y dio paso a nuevas herramientas de gestión de datos, estándares de metadatos, protocolos de interoperabilidad además de compartición de recursos, sistemas escalables, concurrentes y tolerantes a fallos, pero tenía su desventaja de la complejidad de desarrollar estos sistemas, así como tener segura la información.

Pero esto dio paso a los Data Center 3.0 donde combinamos la virtualización y facilita el uso de la red y servidores. En esta nueva evolución podemos tener varios nodos, como una cuadricula de datos, donde existe un mayor intercambio

dinámico, transferencia y cálculo de gran conjunto de datos y cuyos protocolos brinden claridad y facilidad de uso, reduciendo redundancia y la confusión.

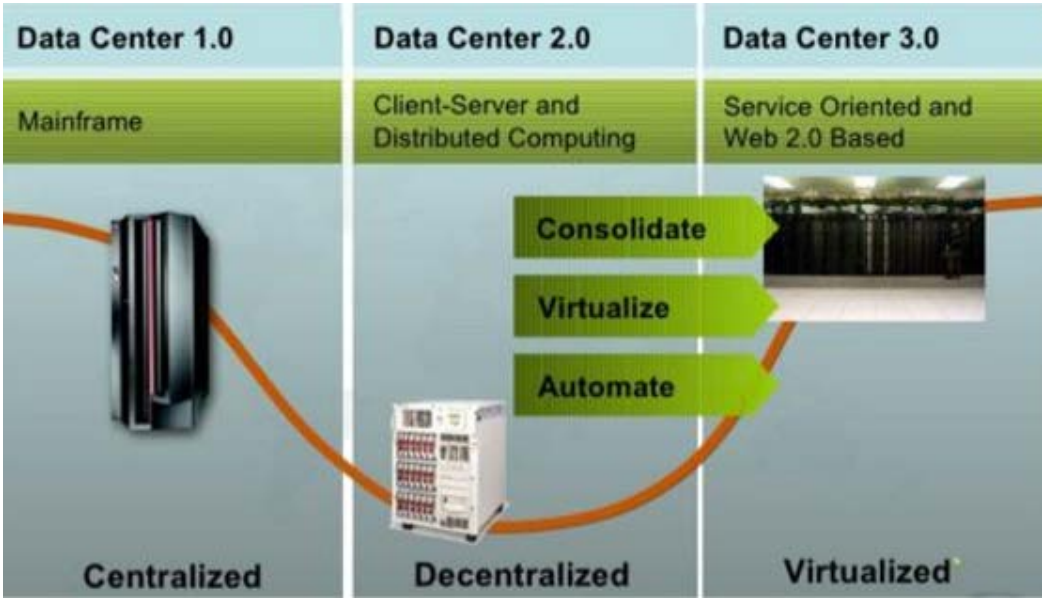


Figura 6. Evolución de Data Center.

Tomado de (Spera, 2012).

A continuación, veremos una tabla 1. donde se puede identificar la evolución de los Data Center según el desempeño en su infraestructura, cómputo, red, entre otras.

Tabla 1.

Comparación de la evolución de los Data Center.

Attribute	Data Center 1.0 (past)	Data Center 2.0 (current)	Data Center 3.0 (future)
Infrastructure	Centralized	Centralized	Distributed
Storage Capacity	Limited, dependent on data center resources, physical media	Centralized by data center, dependent on data center resources	Distributed, potentially un-limited in terms of capacity
Computation	Limited to user's own resources, done on user's own system	Limited number of shared tools available, (e.g., webGIS), mostly done on user's own system	Agility in using local resources and community-developed, cloud-based services available in the data grid
Networking	Bitnet, Internet	Internet2	Software Defined Networking
Discovery	Domain knowledge, hard copy catalogs, beginnings of basic online catalog systems	Websites run by each repository; sophisticated digital data catalogs	Custom search algorithms and recommendation engines
Access	User accesses data on physical media, obtains "complete" dataset	Internet-based distribution; user must access each data collection separately from host data center	Federation of data systems
Protocols	FTP, Globus, some web services, some middleware	Open APIs, web services, advanced middleware	Seamless interoperability, curation, and compute
Metadata Standards	Nascent standards	Determined by domains and research communities	Standardized and automated via middleware
Data Curation	Driven by data "owner"	Open Archival Information System (OAIS), ISO 16363	Agile, community-based; mix of decentralized and centralized, curation throughout data life story
Software Curation	N/A	Beginnings of efforts to archive scientific models	Open code development, community-based sustain-ability; increasing linkages between data and software
Publication - Dissemination	Centralized at data center	Centralized at data center	Integrated into data grid; involves data centers, journals and other relevant institutions

Tomado de (Renci, 2016).

1.3.2.1 Convergencia e Hyperconvergencia.

En un ambiente de Data center se escucha muchas las operaciones de hardware que recomienda las TI (tecnologías de la información), para el desempeño del centro de datos, en cuanto a su infraestructura y nos recomienda dos operaciones.

Partimos del principio de convergencia que es una solución de hardware para minimizar los problemas de compatibilidad y simplificando la gestión de trabajo del Data Center, estas soluciones unen la computación, la red, el almacenamiento, sistemas de administración en un solo sistema convergente. Permitiendo que las empresas utilicen los recursos más eficientemente y rentable reduciendo costos e incrementando la velocidad de implementación de los servicios en software.

En la actualidad se está escuchando del principio de Hyperconvergencia para los nuevos Data Centers, donde la infraestructura es definida por software y permite que el hardware gestione almacenamiento, el procesamiento, las redes, la virtualización y las converge a nivel de hipervisor en bloque único.

Los beneficios de las infraestructuras convergentes para el negocio incluyen ahorros en costes de inversión, porque aprovechan la infraestructura existente de los centros de datos de tus clientes; componentes probados que trabajan juntos basados en arquitecturas de referencia; y flexibilidad para acomodar componentes adicionales de cara al futuro crecimiento del centro de datos.

Mientras que las infraestructuras hiperconvergentes para el negocio incluyen un proceso simplificado de adquisición e instalación; una fácil solución de problemas, ya que tu personal técnico tiene que tratar con menos proveedores; la reducción del número de certificaciones que tu personal técnico necesita y el establecimiento de relaciones más profundas con menos proveedores. (Itreseller, 2017).

1.3.2.2 Modelos de implementación Cloud.

Se conocen tres modelos de servicios Cloud:

- Nube pública: Como su propio nombre lo indica es útil para el público, utilizando infraestructura y recursos lógicos que son propiedad de otros proveedores, las implementaciones de nube publica se las hace para correo electrónicos web, almacenamiento, y entornos de desarrollo en el portal de Microsoft Azure (2018). Donde indica las ventajas de la nube publica:

    - Costos inferiores: no es necesario adquirir hardware o software, y solo paga por el servicio que usa.
    - Sin mantenimiento: su proveedor de servicios se encarga de ello.
    - Escalabilidad casi ilimitada: existen recursos a petición para satisfacer sus necesidades empresariales.
    - Gran confiabilidad: una amplia red de servidores garantiza que no se produzcan problemas.

- Nube privada: Este tipo de recurso las utilizan comúnmente agencias gubernamentales, instituciones privadas y financieras por el motivo que se puede ubicar físicamente el Data Center en su organización donde administran sus recursos cumpliendo los más exigentes estándares del mercado. Las ventajas según Microsoft Azure (2018), son:

    - Más flexibilidad: su organización puede personalizar el entorno de la nube para satisfacer necesidades empresariales específicas.
    - Mejor seguridad: los recursos no se comparten con otros, por lo tanto, es posible contar con mayores niveles de control y seguridad.

- Mayor escalabilidad: las nubes privadas todavía pueden ofrecer la escalabilidad y la eficacia de una nube pública.

- Nube Hibrida: Es una combinación entre la nube pública y la nube privada, en donde adoptan infraestructura de los dos recursos, combinan lo mejor de los dos, donde se tiene mayor flexibilidad y opciones de implementación. Las ventajas según Microsoft Azure (2018), son:

    - Control: su organización puede mantener una infraestructura privada para los recursos confidenciales.

    - Flexibilidad: puede aprovechar los recursos adicionales de la nube pública cuando los necesite.

    - Rentabilidad: gracias a la posibilidad de escalar a la nube pública, solo pagará por la capacidad informática adicional cuando sea necesaria.

    - Facilidad: realizar la transición a la nube no tiene por qué ser compleja, ya que puede realizar una migración gradual; es decir, trasladando cargas de trabajo en etapas.

1.3.3 Cloud Computing.

Los servicios de TI (Tecnologías de la Información), ofrecen servicios flexibles, rentables y probados uno de ellos es el cloud computing donde los usuarios pueden acceder rápidamente a las capacidades de cómputo, almacenamiento y redes que son rápidas. A continuación, vamos a describir varios beneficios:

- Infraestructura virtual, donde no importa el espacio físico de servidor y los datos no se encuentran en un solo sitio.

- Provisión de servicios, en el que los servicios se puedan acceder en segundos.

- Pago de uso, en donde tenemos que diferencia la nube pública y la nube privada donde dependiendo el uso algunos servicios no pueden tener costos.

1.3.3.1 Modelos del Cloud Computing.

Las organizaciones que mantiene su servicio en nubes públicas crean centro de virtualización donde se puede tener varios escenarios:

- IaaS (Infraestructura como servicio). Es donde se provee a los usuarios acceso a servicios de almacenamiento, servidores y redes sin adquirir hardware, y contando con una infraestructura escalable que ahorran a las organizaciones costos.

- PaaS (Plataforma como servicio). Es un entorno en la nube donde los usuarios pueden desarrollar, gestionar y distribuir aplicaciones mediante herramientas de desarrollo y alojarlas en el mismo entorno.

- SaaS (Software como servicio). Proporciona accesibilidad a los usuarios teniendo la ventaja de no instalar aplicaciones en sus dispositivos locales, desde cualquier dispositivo conectado al internet sin provocar perdida de información.

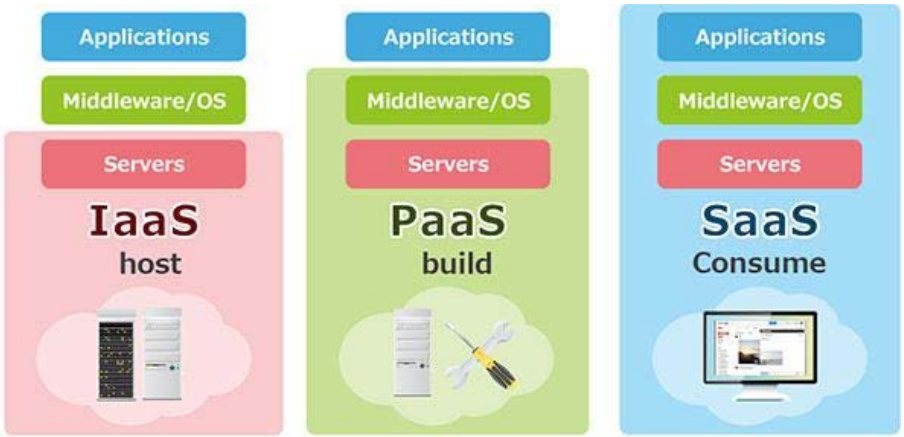


Figura 7. Servicios IaaS, PaaS, SaaS.
Tomado de (Bitec, 2017).

1.3.4 Almacenamiento.

El término almacenamiento es un término muy importante en nuestros días, partiendo su desarrollo desde el año de 1956, con el modelo Ramac1 de IBM, con una capacidad de 5MB, además de su capacidad sorprendía a todos son su peso que se encontraba en 1 tonelada.

Progresivamente con el tiempo los discos han ido incrementando en costo, capacidad, velocidad, pero disminuyendo en tamaño y consumo de potencia. Es así como tenemos los discos (EIDE, SATA, SCSI, SAS, SSD), este último ya no tiene partes mecánicas SSD, maneja una placa de circuitos con chips de memoria y componentes que pueden estar sujetos a golpes sin pérdida de memoria.

En la actualidad la capacidad de almacenamiento los Data Center se lo calcula siguiendo un criterio de diseño en cuanto a redundancia entre controladoras, protocolos de acceso, crecimiento, protección soportada, rendimiento de los sistemas, compatibilidad con sistemas y aplicativos entre otras.

1.3.4.1 Arquitectura de almacenamiento.

- DAS (Direct - Attached Storage) es un tipo de arquitectura de almacenamiento que maneja discos y funciona conectando un servidor a un dispositivo, para que sea tolerante a fallas se necesita realizar soluciones RAID (Combinación de varios discos).

- NAS (Network - Attached Storage) consiste en el almacenamiento por parte de la red, en donde un conjunto de computadoras una va a funcionar de servidor y va a aceptar las solicitudes de su conjunto, el problema de esta arquitectura es que atiende varias solicitudes y se producen los cuellos de botella. Pero todo depende de la administración ya que es una arquitectura escalable y de alta disponibilidad.

- SAN (Storage Área Network) es una arquitectura que se encuentra en su auge, ya que los usuarios pueden leer y escribir sobre cualquier información compartida, cuya información se puede encontrar geográficamente distribuida. Para esto se debe contar con tecnologías actuales que sean capaces de soportar altas velocidades dedicadas al almacenamiento y backup.

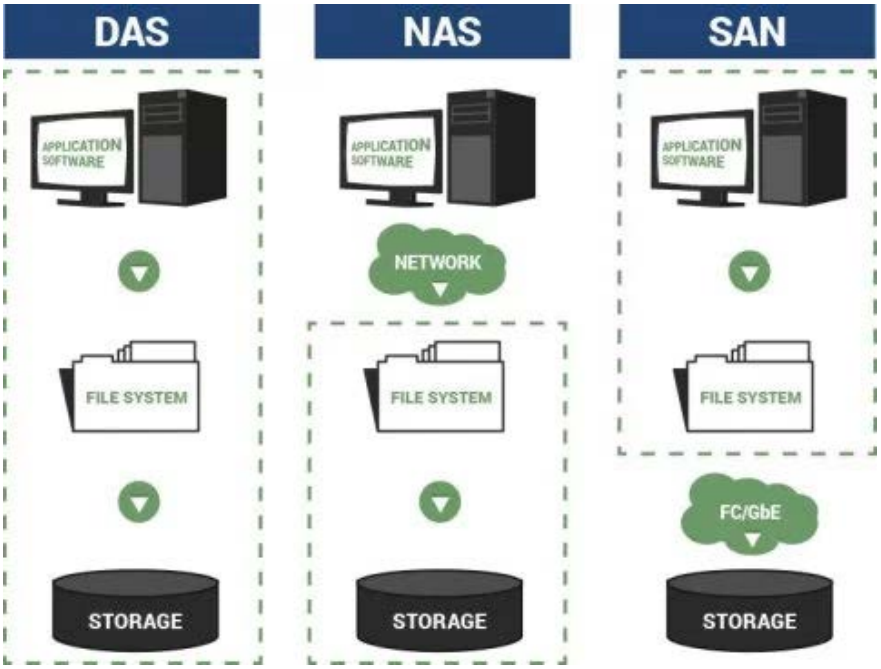


Figura 8. Arquitecturas de Almacenamiento.
Tomado de (Anlorenro, 2016).

1.3.4.2 Nuevas tendencias en almacenamiento para Data Center.

- Tendencia de almacenamiento unificado, donde se conecta a la red proporcionando servicios de almacenamiento basados en bloques. Estos bloques no son más que protocolos como Fiber Channel, ISCI, entre otras que permite que los usuarios obtengan un acceso consolidado a la información almacenada.

- Almacenamiento SSD, es una nueva tendencia ya que se está comenzando a realizar arreglos de unidades de disco sólido para tener mejor redundancia de información y acceder

rápidamente a ella, al tener una conexión SATA y manejar velocidades de lectura, escritura rápida, además su tiempo de vida es mejor que la de discos.

- Tendencias de clusterización, dispone de funciones avanzadas para el almacenamiento ilimitado con una capacidad escalable en donde gracias a las tecnologías de conexión de hoy un cliente pueden usar terabytes a petabytes de información de manera rápida a través de la red.

- Tendencia de deduplicación, que consiste en almacenar información de manera óptima y replicar la información sin que ocasione una transferencia de datos enorme, todos los fabricantes ofrecen este servicio para tener una estrategia conveniente de backup.

- Tendencia Aceleración/Tiering, es una solución donde se optimiza constantemente los datos ya que faculta la información en niveles automatizados para que los datos más utilizados se los pase a niveles de alto rendimiento y los datos menos utilizados se los pase a niveles inferiores, donde se tiene un mejor aprovechamiento de los recursos de almacenamiento.

- Tendencias de replicación, es una técnica donde existen sistemas de compresión entre dos sitios donde la información se replica por medio de envió de bloques, cumpliendo con sistemas síncronos y asíncronos.

1.3.5 Virtualización.

Anteriormente se habló de los Data Center 3.0 en donde la virtualización es uno de los pilares de estos centros de datos y no es más que una tecnología que permite crear múltiples entornos y recursos simulados desde un dispositivo que puede ser un computador, celular, tablet, etc. Esto lo hace mediante un Hipervisor que es el motor de este mecanismo donde se conecta directamente

con el hardware y se divide varios sistemas por separados de una manera diferente y segura.

La virtualización se lo puede realizar mediante máquinas virtuales, donde se tiene un mejor desempeño en potencial de procesamiento, almacenamiento y se puede elegir la memoria que se desea asignar donde se cuenta con mayor protección. Entre los beneficios de virtualización tenemos:

- Reducir los costos
- Menos espacios en rack
- Incrementar la productividad
- Facilita test y desarrollo
- Simplifica las migraciones
- Portable

1.3.5.1 Arquitectura de virtualización.

La virtualización ha tenido varios cambios desde sus inicios, por exigencia de las organizaciones es así como tenemos:

- Virtualización 1.0: Emulación para permitir que el software se ejecute en sistemas operativos de escritorio incompatibles o para crear entornos de prueba de propósito especial.
- Virtualización 2.0: Consolidación del servidor. Ahorro de dinero al mejorar la utilización de las CPU y la memoria y, por lo tanto, requiere menos hardware. También facilitó la implementación de software en el centro de datos.
- Virtualización 3.0: Mejora de la calidad del software brindando a los desarrolladores y probadores acceso a múltiples máquinas

virtuales que se ejecutan a altas velocidades, gracias al multinúcleo. (Zeichick, 2010).

1.3.5.2 Técnicas de virtualización.

Existen cuatro tipos de virtualización:

- Virtualización de plataforma. – Muchas máquinas virtuales son simuladas por una maquina o host que posee recursos adecuados para trabajar sobre el con un software que poseerá un sistema operativo completo, en donde funcionará como un sistema independiente. Aquí nacen las virtualizaciones más conocidas como virtualización para sistemas operativos, aplicativos entre otras.

- Virtualización de recursos. – En esta virtualización contemplamos varios dispositivos para que trabajen como uno solo, un ejemplo claro de esto es los servicios de almacenamientos compartidos donde por medio de una VPN, pueden acceder a los recursos de almacenamiento de una organización.

- Virtualización de redes. – Es un claro ejemplo del futuro de las redes donde se trabaja con redes que están virtualizadas igual que una red física. Según el portal de VMWare (2018), la virtualización de redes brinda dispositivos y servicios de red lógicos (es decir, puertos lógicos, swiches, enrutadores, firewalls, balanceadores de carga, redes privadas virtuales [VPN, Virtual Prívate Network] y mucho más) a las cargas de trabajo conectadas. Las redes virtuales ofrecen las mismas funciones y garantías que una red física, junto con las ventajas operacionales y la independencia de hardware propias de la virtualización.

- Virtualización de escritorio. – que consiste en llevar mediante la virtualización escritorios finales a los usuarios, para poder desempeñar mejor sus actividades. Según el portal de VMWare (2018), La implementación de escritorios como un servicio administrado le permite responder con mayor rapidez a las necesidades y las oportunidades cambiantes. Puede reducir costos y aumentar el servicio mediante el suministro rápido y sencillo de escritorios y aplicaciones virtualizados a las sucursales, a los empleados en el extranjero y tercerizados, y a los empleados móviles con tabletas iPad y Android.

1.3.6 Seguridad de Data Center.

La Seguridad de información es sin duda un tema muy relevante en cuanto a la información que manejan los centros de datos. Es por eso por lo que para muchas organizaciones los datos es dinero y debe integrarse como parte de las operaciones del Data Center.

La seguridad en un Data Center es multinivel y se cumple tres acciones:

- Antes: Control y asegurar los dispositivos.
- Durante: Detectar, bloquear y defender.
- Después: Analizar el porqué de los ataques, definir un alcance y corregir los problemas.

Es así como en la página de cisco (2018), nos da algunos requisitos para entornos de Data Center:

- Aplicaciones de políticas de seguridad entre aplicaciones y cargas de trabajo virtualizados.
- Administración escalable, incluidos usuarios, conexiones y capacidad de procesamiento.
- Gestión consolida entre servicios de seguridad

- Falta de tareas entre el servidor de aplicaciones y mecanismos de seguridad.

Los componentes fundamentales en una arquitectura de Data Center con seguridad son:

- Dispositivos que manejen VPN
- Firewall virtual y firewall físico contra (IPS, instrucciones, prevenciones)
- Control de amenazas
- Módulos de firewall incorporados
- Soluciones de acceso seguras.

1.3.6.1 Seguridad física de Data Center.

Figura 9. Seguridad física de Data Center.
Tomado de (JCB, 2017).

Como podemos verificar en la Figura 9, un Data Center cuenta varios mecanismos de seguridad física, para garantizar a sus usuarios una operación continua sin interrupciones durante todo un año. Para esto debe implementar varios mecanismos cumpliendo con estándares de calidad como Tier IV, en la que poniendo un ejemplo cuentan con techos de acero sólido, y nada

inflamables, el equipo de alta tensión está aislado lejos del piso donde está el Data Center y paredes de hormigón, además de:

- Detección de incendios
- Detección temprana de humo
- Supresión de Incendios.
- Evacuación de emergencia con señalización de emergencia.
- Sistema de aire acondicionado

También cuentan con control de acceso en perímetros, edificios, salas técnicas, armarios con:

- Control de acceso autónomo, donde no tiene un registro de eventos, son sistemas que controlan varios portones, pero no se manejan en una PC.
- Control de acceso con red, estos sistemas podemos ingresar desde la red para poder configurarlos y llevar un registro.

En estos sistemas podemos contar con:

- Cámaras de seguridad.
- Cerradura magnética
- Biométricos de huella digital, tarjeta, facial.
- Control de acceso por teclado
- Sensores de movimiento
- Entre otras.

1.3.6.2 Seguridad lógica.

Al hablar de seguridad lógica, entendemos del resguarden del acceso de los datos que solo personas calificadas pueden ingresar tomando medidas establecidas por los administradores de usuario o recursos. Los objetivos de la seguridad lógica son:

- Restringir acceso a los programas y archivos.
- Asegurar que los operadores no modifiquen la información.
- Hay que asegurar que las aplicaciones funcionen correctamente.
- Que la información sea enviada al remitente que solicita la información sin alterarse.

Todos estos objetivos son con la finalidad de evitar la violación de acceso por medio de personal no autorizado como hackers, exempleados, virus, sistemas operativos inestables, copias de seguridad sin autorización, programas mal diseñados. Es importante llevar un dispositivo de monitoreo de la red ya que se va a tener un tráfico de red entrante-saliente mediante reglas de seguridad este dispositivo es un firewall y constituye una primera línea de defensa de seguridad.

En el portal de cisco (2018) sobre firewall de siguiente generación indica:

“La mayoría de las empresas están implementando firewalls de próxima generación para bloquear las amenazas modernas, como los ataques de la capa de aplicación y el malware avanzado.” Por lo tanto, se han implementado:

- Funcionalidades de firewall estándares, como la inspección con estado.
- Prevención integrada de intrusiones.
- Reconocimiento y control de aplicaciones para ver y bloquear las aplicaciones peligrosas.

- Rutas de actualización para incluir fuentes de información futuras.

- Técnicas para abordar las amenazas de seguridad en evolución.

1.3.7 Gestión de un Data Center.

La Gestión se centra en tres puntos importantes las cuales son los sistemas implementados, otro son los procesos que permiten la comunicación de los servicios sin interrupciones y por último el personal humano que se encuentra en sitio para resolver cualquier problema de los procesos o lo sistemas.

- Sistemas implementados: estos sistemas comprenden sistemas de refrigeración, cableado estructurado, sistema de energía así también como los sistemas que comprende el computo, red almacenamiento y seguridad.

- Procesos: Estos procesos comprenden técnicas que ayudan que una data center funcione según protocolos y normas establecidas por institutos o entidades internacionales.

- Personal Humano: Este factor juega un papel muy importante en la administración de un Data Center ya que de ellos dependerán los procesos, los sistemas implementados y más que toda la seguridad tanto lógica como física de la información.

1.4 Infraestructura actual del Data Center Académico.

El Data Center Académico de la UDLA se encuentra en funcionamiento y posee una infraestructura basada en networking, subsistemas de cómputo y de almacenamiento, a continuación, presentamos como esta implementado.

Tabla 2.

Componentes Subsistema Networking.

SUBSISTEMA NETWORKING				
Centro De Datos: Campus Queri				
No. de parte	**Descripción**	**Cantidad**	**Detalle**	**Observaciones**
N3K-C3524P-10GX	Cisco Nexus 3524	2	Switch • Licenciamiento LAN Basic • 24 puertos licenciados SFP+ • Sistema Operativo NX-OS	Fuente de poder (2) y ventiladores redundantes, cables de poder C13-C14

Tomado de (Universidad de las Américas, s.f.).

Tabla 3.

Componentes Subsistema Cómputo.

SUBSISTEMA CÓMPUTO				
Centro De Datos: Campus Queri				
No. de parte	**Descripción**	**Cantidad**	**Detalle**	**Observaciones**
UCS-SPL-5108-AC2	Cisco UCS Chassis 5108	1	Chassis: • 2 Fabric interconnect 6324	Fuente de poder (4) y ventiladores redundantes, cables de poder C19-C20. UCS Manager Embebido
UCSB-B200-M4-U	Cisco UCS B200M4	12	Servidor Blade • 64GB RAM (4 x 16GB) • 2 CPU (6 cores, 1.9GHz) • Tarjeta VIC 1340	La tarjeta VIC puede virtualizar interfaces NIC y HBA según lo requerido.

Tomado de (Universidad de las Américas, s.f.).

Tabla 4

Componentes Subsistema Almacenamiento.

SUBSISTEMA ALMACENAMIENTO				
Centro De Datos: Campus Queri				
No. de parte	**Descripción**	**Cantidad**	**Detalle**	**Observaciones**
V32D12AN5PS6	VNXe 3200	1	Almacenamiento • Controladoras redundantes	Fuente de poder y ventiladoras redundantes,

			• 3 discos SD de 100GB para Fast Cache • 6 discos SAS de 300GB • 6 discos SAS de 1.2TB	cables de poder C13-C14

Tomado de (Universidad de las Américas, s.f.).

Además, cuenta con un sistema de virtualización con vSphere que entre sus ventajas cuenta con:

Tabla 5.

Ventajas de vSphere.

Eficiencia gracias a la utilización y a la automatización	Se consiguen índices de consolidación de 15:1 o más y mejora la utilización del hardware del 5 al 15% hasta un 80% o más, sin sacrificar el rendimiento.
Reducción drástica de los costes de TI	Brinda una disminución de los gastos de propiedad en hasta un 70% y los costes operativos en un 30%, a fin de conseguir costes de infraestructura de TI un 20 o 30% inferiores por cada aplicación que se ejecute en vSphere.
Agilidad y control	Responde con celeridad a las necesidades empresariales en constante cambio sin sacrificar la seguridad ni el control, y proporcione una infraestructura sin contacto con disponibilidad, escalabilidad y rendimiento integrados y garantizados para todas las aplicaciones de misión crítica que se ejecuten en vSphere
Libertad de elección	Usa una plataforma común basada en estándares para sacar partido a los activos existentes de TI junto con los servicios de TI de próxima generación y mejora gracias a vSphere las API abiertas con soluciones de un ecosistema mundial de los principales proveedores de tecnología

Tomado de (Vmware vSphere, s.f.).

Y entre las características de vSphere tenemos:

Tabla 6.

Características y principales funciones.

Característica	**Detalle**
vSphere Distributed Resource Scheduler (DRS)	Brinda una proporción de balanceo de carga dinámico independiente del hardware y asignación de recursos para máquinas virtuales en clúster. Utiliza la automatización basada en políticas para reducir la complejidad de gestión y reforzar la compatibilidad con los acuerdos de nivel de servicio (SLA)
VMware Distributed Power Management (DPM)	Automatiza el consumo eficiente de la energía en los clústeres de VMware DRS optimizando continuamente el consumo eléctrico de los servidores dentro de cada clúster
vSphere vNetwork Distributed Switch	Simplifica y optimiza la red de máquinas virtuales en entornos de vSphere, además permite usar switches virtuales distribuidos de terceros, como Cisco Nexus 1000V, en entornos de VMware vSphere.
vSphere vStorage Thin Provisioning	Proporciona asignación dinámica de la capacidad de almacenamiento compartido. Con ello los departamentos de IT puede implementar una estrategia de almacenamiento por niveles y reducir al mismo tiempo el gasto en almacenamiento hasta un 50%
vSphere Storage I/O Control	Establece las prioridades de calidad de servicio del almacenamiento para garantizar el acceso a los recursos de almacenamiento.
vSphere Storage DRS	Proporciona una automatización en el balanceo de la carga y utiliza funciones de almacenamiento para determinar la mejor ubicación para que residan los datos de una máquina virtual concreta cuando se crea y cuando se utiliza a lo largo del tiempo.
vSphere Profile-Driven Storage	Reduce los pasos para la selección de los recursos de almacenamiento agrupándolos conforme a una política definida por el usuario
VMware Network I/O Control	Establece prioridades de calidad de servicio de red para garantizar el acceso a los recursos de red

Adaptada de (Vmware vSphere, s.f.).

2. CAPITULO II: ESTÁNDARES APLICADOS AL DATA CENTER ACADÉMICO.

Un Data Center cumple con varios estándares, como se muestra en la Figura 10, en este capítulo mencionaremos algunos estándares, los cuales nos ayudaran a realizar nuestro sistema de seguridad

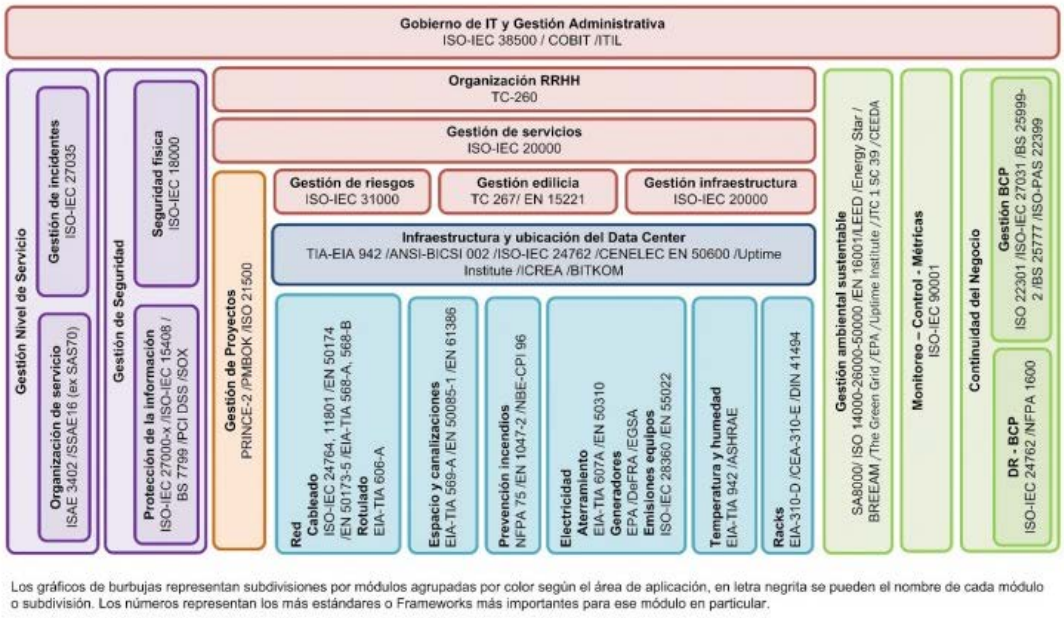


Figura 10. Estándares en Data Center
Tomado de (IT, 2013).

2.1 Definición de estándar.

Se define a un estándar como una norma, regla, referencia, modelo o patrón los cuales son documentados luego de que las entidades reguladoras hayan realizado las pruebas necesarias para alcanzar altos niveles de calidad en los sistemas.

La estandarización se estableció desde el año 1865 con el desarrollo de las comunicaciones en donde se verificó que el crecimiento de las demandas de interconexión entre varios países obligo a una organización a crear estándares en donde todas las empresas deben regirse a los mismos procedimientos, cables

de conexión, precios de comercialización, entre otros con el fin de no crear monopolios, arquitecturas cerradas y organizaciones propietarias.

Desde que se implementaron los estándares se han tenido sistemas en donde un conjunto de diferentes tipos de marcas trabaja de la mano sin generar ningún problema en su funcionamiento ajustándose al bolsillo del usuario sin barreras imposibles de alcanzar.

2.2 Historia

Luego de la evolución del ferrocarril como medio de transporte se creó el telégrafo como primer medio de comunicación en donde un mensaje llegaba más rápido de un punto a otro sin la espera tan larga que se tenía como era la de las cartas.

Al ver todos los beneficios que el telégrafo ofrecía las empresas y los usuarios comenzaron a buscar una estructura definida junto a un sistema de funcionamiento ordenado y factible para brindar este servicio a todas las personas que lo requerían, pero tomando en cuenta que los precios de comunicación estén en los rangos factibles.

Entonces es ahí cuando se crea en 1865 en París la ITU (Unión Internacional de Telegrafía) como organización Internacional e Intergubernamental misma que sirvió para estandarizar parámetros de comunicaciones en varios países bajo el principal deseo de garantizar que las comunicaciones telegráficas trabajen con aranceles simples y reducidos, además de que se mejorara las condiciones de telegrafía internacional para brindar comunicaciones de óptima calidad ante la comunidad. Con la creación de este importante organismo e logró un avance importante en la armonía de las fronteras de Europa, África y Asia con respecto a la estipulación de reglamentos, aranceles y mejoras tecnológicas.

Luego en el año 1884 se crea la IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) organismo que se encarga de analizar estándares para redes de comunicaciones luego de sus respectivas pruebas en campos reales con el fin de garantizar la calidad de los sistemas promoviendo la creatividad, desarrollo e

integración de conocimientos junto con las tecnologías de información, electrónica y ciencias con el principal objetivo de traer grandes beneficios a la humanidad.

Después en 1906 se fundó la IEC (Comisión Electrotécnica Internacional) asociación que especifica estándares para la electrónica y la eléctrica en proyectos de alta y media gama que son implementados en los múltiples proyectos que se crean día a día alrededor del mundo. Actualmente trabaja con un alrededor de 20000 expertos en la industria, comercio, gobiernos, laboratorios e investigadores que en conjunto trabajan de la mano para seguir adelante con mejoras tecnológicas y se toma decisiones en conjunto con cada uno de los países miembros que pertenecen a este gran Instituto.

Figura 11. Logo de la Comisión Internacional Electrónica.
Tomado de (IEC, 2018).

En el año de 1918 se fundó la ANSI (Instituto Nacional Estadounidense de Estándares) mismo que rige normas a nivel mundial y existen sistemas que lo toman en cuenta por completo en la realización de sus proyectos. La misión que cumple ANSI es: “Mejorar la competitividad global de las empresas de EE. UU. Y la calidad de vida de EE. UU. Promoviendo y facilitando normas voluntarias de consenso y sistemas de evaluación de la conformidad, y salvaguardando su integridad.” (ANSI, 2018).

Figura 12. Logo del American National Standards Institute.
Tomado de (ANSI, 2018).

En el año de 1932 se convirtió la antigua ITU en la Unión Internacional de Telecomunicaciones es el organismo especializado en Tecnologías de la Información y Comunicación de las Naciones Unidas. Esta organización trabaja el día a día especialmente con el principal objetivo de interconectar a toda la población mundial sin importar la ubicación en la que se encuentre y que medios de comunicación disponga.

Figura 13. Logo de la Unión Internacional de Telecomunicaciones.
Tomado de (ITU, 2018).

Así con el pasar de los años alrededor del mundo, en varias regiones, países y ciudades se han ido incrementando la creación de organizaciones que luego de sus estudios académicos, pruebas científicas y análisis en laboratorios han ido implementando sus parámetros convencionales para ejecutar proyectos con calidad y el menor porcentaje de fallas posibles.

2.3 Tipos de estándares.

Se han creado tres tipos de estándares los cuales son: propietarios, de facto y de jure. Vamos a analizar cada uno de estos.

- Los estándares propietarios son aquellos que están implementados por propiedad total de una determinada corporación o marca donde su uso es solamente para productos o servicios de dicha empresa. Es una forma de atar por completo a los usuarios en la compra de todos los servicios que esa empresa ofrezca con el fin de crear una fidelidad y adopción de los servicios creando ganancias redondas en el mercado.

- Los estándares de facto son aquellos que son aceptados por el mayor porcentaje del mercado y tiene un alto grado de integración para los usuarios, pero los mismos no son oficiales o declarados por organizaciones oficiales y registradas.

- Los estándares de jure son aquellos que son aprobados por organizaciones internacionales como los son: ANSI, ITU, ISO, entre otras. Dichos estándares son analizados por grupos de ingenieros, universidades, científicos, etc., que contribuyen con ideas, elementos y recursos para nuevos desarrollos y estándares con el fin de lograr las mejoras continuas.

2.4 Organizaciones reguladoras de estándares.

Existen dos tipos de organizaciones de estándares las cuales son: organizaciones de fabricantes y organizaciones oficiales.

- Las organizaciones de fabricantes consisten en fabricantes que construyen grandes empresas las cuales crean su propio software y hardware estableciendo estándares propietarios en el mercado de las redes y telecomunicaciones.

- Las organizaciones oficiales son aquellas que se han constituido internacionalmente por consultores independientes, estudiantes, investigadores, científicos, etc., en donde a base de pruebas y experimentos han logrado levantar estándares comprobados con sinónimos de servicios de excelente calidad sin monopolizar a una marca especifica.

Estas organizaciones se reúnen cada año para seguir analizando las mejores y evolución que se puede brindar día con día. Entre las principales organizaciones que tenemos son: ITU (Unión Internacional de Telecomunicaciones), ISO (Organización Internacional de Normalización), ANSI (Instituto Nacional Estadounidense de Estándares), IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), IETF (Grupo de trabajo de Ingeniería de Internet), IEC (Comisión Electrotécnica Internacional), entre otras.

2.5 Estándar ANSI / TIA 942.

Para realizar el presente proyecto de tesis elegimos trabajar bajo las políticas del estándar ANSI / TIA 942 debido a que es un estándar orientado a trabajar bajo políticas de cableado y de conectividad incluyendo definiciones de redundancia y fiabilidad seleccionándolos bajo la clasificación de TIERS por el Uptime Institute.

Por lo tanto, es importante tomar en cuenta que el sistema de seguridad que vamos a implementar debe estar operativo el mayor tiempo posible para poder registrar todos los posibles peligros o vulnerabilidades que pueden ocurrir en los horarios no autorizados junto con posibles infiltrados que deseen ingresar a cualquiera de los laboratorios sin la debida autorización.

Además, se monitoreará el Data Center para que en caso de que exista alguna falla en el sistema se dé una alerta para revisión de la parte afectada esto con el fin de brindar una pronta solución y no generar pérdidas de ninguna índole.

2.6 Historia de ANSI / TIA 942.

El estándar TIA 942 fue desarrollado por la Asociación de la Industria de Telecomunicaciones (TIA) en donde su primera publicación fue realizada el 2005. La TIA fue creada el 1988 con la fusión de proveedores de telecomunicaciones y proveedores de la información.

Esta organización brinda beneficios considerables para sus miembros, define normas de acuerdo con el desarrollo de la industria de las telecomunicaciones, entre otros. La TIA se presenta mundialmente como la principal asociación de la comunicación e información mediante la creación de normas, oportunidades de negocio, análisis de mercado, certificaciones y estricto cumplimiento de la normativa ambiental.

La TIA cuenta con un total de 600 miembros los cuales trabajan a menudo con las mejoras en el negocio de las telecomunicaciones basándose principalmente en manejo de mayor ancho de banda, redes, cableado, comunicaciones satelitales, comunicaciones inalámbricas, tecnologías de la información y alcances ecológicos de los parámetros de tecnología.

En cambio, el ANSI es el Instituto Estadounidense de Estándares la cual consiste en una organización privada sin fines de lucro misma que fue creada en 1918. Esta organización se encarga de administrar el sistema de estándar voluntario que tiene el sector privado de los EE. UU. Es decir, realiza un análisis y aprueba los estándares que experimentan otras organizaciones, departamentos gubernamentales, empresas, entre otros.

2.7 Definición de ANSI / TIA 942.

El ANSI / TIA 942 es un estándar real creado por una asociación sin fines de lucro con su primera publicación se la realizó en el 2005. Sus participantes fueron fabricantes, usuarios finales, consultores, ingenieros y arquitectos, además de que la TIA cuenta con la acreditación de ANSI. Es un estándar que cubre aspectos físicos, ubicación en sitio, seguridad, arquitectura, seguridad contra incendios, parámetros eléctricos, mecánicos y de telecomunicaciones.

2.8 Niveles de clasificación de un Data Center según ANSI / TIA 942.

Se creó un formato de clasificación de Data Center a cuál se lo puso el nombre de Tier, es una clasificación estándar que sirve para calificar de manera eficaz la infraestructura que tienen los Data Centers para detectar cual es el porcentaje de disponibilidad que dicho Data Center brinde en el transcurso del año.

Este sistema brinda un método para comparar las instalaciones, rendimiento y productividad de una infraestructura de Data Center para las empresas que deseen implementar o hacer el uso de estos. Además de que la clasificación Tier brinda un lineamiento a las empresas para saber qué tipo de inversión se puede realizar para estructurar un Data Center y que crecimiento de puede tener en el transcurso de los años.

Los Tier indican especificaciones, características, requisitos o beneficios que deben cumplir la infraestructura de los Data Center así para cumplir un nivel requerido de acuerdo con el tipo de negocio que se maneje. Además, que los Tier hablan específicamente dentro de la infraestructura sobre la energía, refrigeración, mantenimiento, equipamiento, software, sitio, temperatura y capacidad que tiene para resistir una falla.

La clasificación que se estableció de acuerdo con los Tier se establece desde niveles básicos y sencillos a niveles de estándares altos con una capacidad más alta. A continuación, vamos a hablar sobre cada uno de los niveles de Tier que existen:

2.8.1 Tier I - Nivel 1 (Data Center Básico).

Es el primer estándar que se tomó como base fundamental para la creación de estándares y el mismo cuenta con las siguientes características:

- Tiene una disponibilidad de 99.671 %.
- El servicio puede interrumpirse por actividades planificadas o no planificadas.

- No cuenta con elementos redundantes de corriente o aire acondicionado.
- No cuenta con piso elevado.
- Trabaja con un generador independiente.
- El Data Center debe estar fuera de servicio siquiera una vez al año por temas de mantenimiento.
- Tiempo de implementación medio se estima en 3 meses.
- Se calcula un tiempo total de inactividad de 28.82 horas durante el año.
- No tiene backup para su respectivo mantenimiento o reparaciones del sistema.

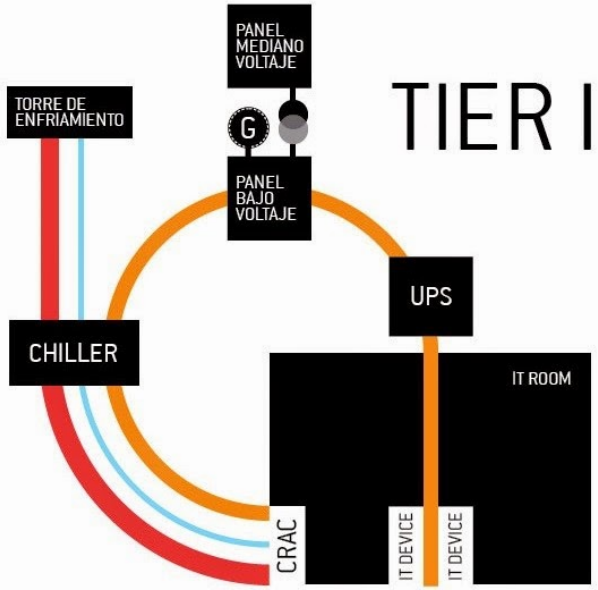


Figura 14. Esquema TIER I.
Tomado de (Acevedo, 2015).

2.8.2 Tier II – Nivel 2 (Componentes redundantes).

Este nivel de clasificación se enfoca para aquellas empresas que están impulsadas por el tiempo de comercialización para un trabajo específico en un

horario determinado que por el tiempo de vida permanente para un trabajo que tenga el servicio. A continuación, hablaremos de las características que lo definen:

- Tiene una disponibilidad de 99.741%.
- Consta de piso elevado.
- Tiene UPS y generador de energía.
- Tiempo de implementación en un plazo de 3 a 6 meses.
- Tiempo de inactividad anual es de 22 horas.
- Constan de una sola conexión de corriente y aire acondicionado con un componente redundante.
- Cuenta con un porcentaje básico de mantenimiento de aplicaciones online.
- Es tolerable a fallos en un nivel bastante básico.

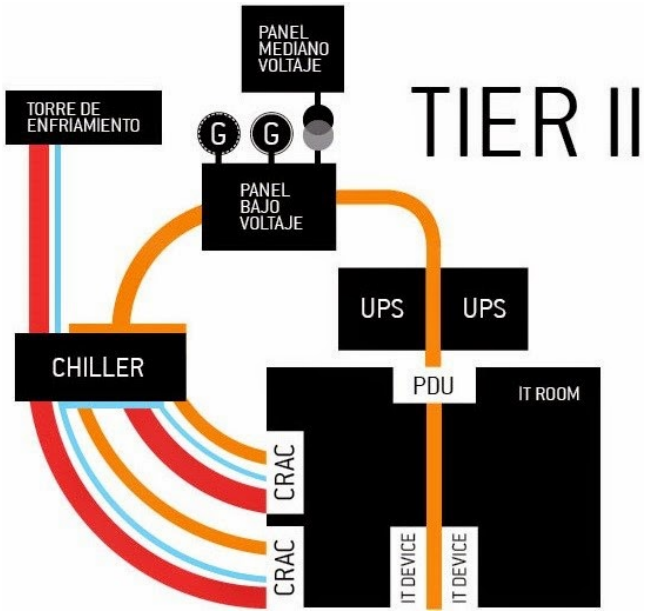


Figura 15. Esquema TIER II.
Tomado de (Acevedo, 2015).

2.8.3 Tier III – Nivel 3 (Mantenimiento concurrente).

Es un nivel que cuenta con una vida efectiva que se usa normalmente por empresas que conocen el costo de una caída del servicio y esto afecta con altos valores monetarios.

- Tiene una disponibilidad de 99.982%
- Trabajos planificados sin problemas de interrupción en el funcionamiento, pero en trabajos no planificados caída del servicio inevitablemente.
- Tiempo de implementación esta de 15 a 20 meses.
- Tiempo de inactividad al año de 1.6 horas
- Múltiples accesos de energía y aire acondicionado. Cuenta con elementos redundantes.
- Cuenta con sistemas configurados como activos / pasivos.
- Conformado por elementos redundantes.

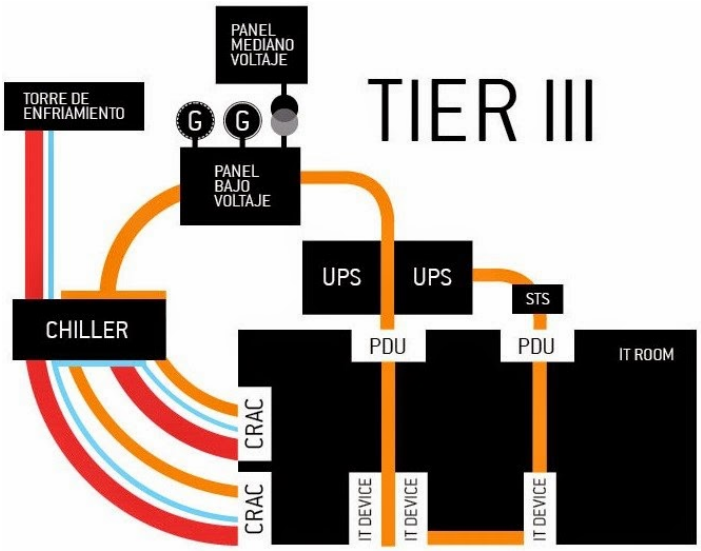


Figura 16. Esquema TIER III.
Tomado de (Acevedo, 2015).

2.8.4 Tier IV – Nivel 4 (Tolerante a fallos).

Es el más alto nivel de Data Centers que se ha creado y se ha implementado para su servicio, sirve para empresas a las cuales las faltas de servicio de un Data Center les pueda causar un alto impacto en la cuota de mercado y problemas en su misión. A continuación, vamos a hablar de las características de este nivel:

- Tipo de disponibilidad del servicio de 99.995%.
- Tiempo de implementación de 15 a 20 meses.
- Tiempo de inactividad al año es de 0.4 horas.
- Interrupciones con trabajos no planificados sin la pérdida de datos críticos y sin daños graves.
- Componentes redundantes de paso de corriente y sistemas de enfriamiento.

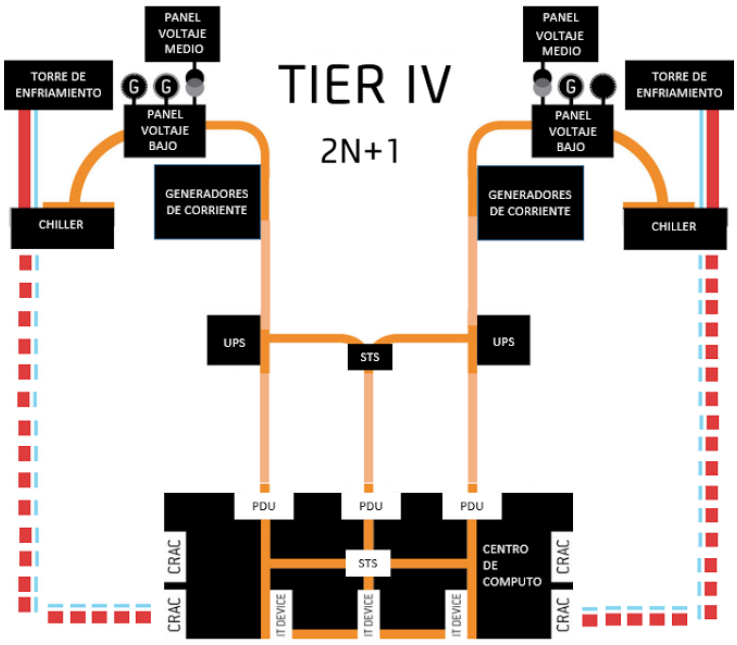


Figura 17. Esquema TIER IV.
Tomado de (Acevedo, 2015).

2.8.5 Tier V – Nivel 5.

Es un estándar desarrollado por la Uptime Institute que está en modo de evaluación y redefinición con los estándares anteriormente planteados lo cual se plantea como una mejora única en el servicio que brinda los Data Centers. Las características que plantea los Tier 5 son:

- Capacidad de funcionamiento solo con agua para el enfriamiento de los equipos.
- Capacidad de detectar contaminantes exteriores y a su vez tenga una capa de protección ante los mismos.
- El almacenamiento de energía tenga redundancia y monitoreo constante.
- Todo el sistema de circuitos debe estar monitorizado de acuerdo con su distribución en el sistema.
- Sistemas de conmutación operativos al 100%.
- Mitigación completa ante ataques de DDoS con los usuarios.
- Protección completa en cada rack de equipamiento.
- Control de acceso a los servicios activos y sistemas de monitorización.
- Cada sitio divido del Data Center debe tener un control de seguridad individualmente.
- No se tiene ningún tipo de material inflamable dentro de las salas de conmutación.
- Contar con un techo de doble superficie que en caso de que sea necesario el mismo sea reemplazable.

- Sitio de instalación no debe ser inundable dentro de los 100 últimos años.

- Debe presentarse un sistema de energía al 100% renovable.

Figura 18. Esquema TIER IV.
Tomado de (Terdiman, 2016).

Este tipo de nivel está siendo analizado por el Uptime Institute con respecto a todos los elementos que se ponen en juego dentro de un Data Center, pero aún no se ha tenido ninguna implementación real del mismo en alguna parte del planeta, claramente se puede verificar que tiene un grado de disponibilidad bastante elemento y sus requerimientos llegan a niveles de exigencia bastantes altos en donde a su vez también el costo como su tiempo de implementación son bastante elevados.

Es por eso el desarrollo de nuestra tesis en donde valoramos que la seguridad es un punto bastante importante y valioso para el desarrollo de un sistema tecnológico en donde los valores monetarios son bastantes altos.

2.9 Ventajas de uso de los Tier.

- Se usa una nomenclatura estándar para la implementación de Data Center.

- Valoración para la protección ante individuos externos.
- Tabulación de acuerdo con el rango en escenarios frente a posibles fallas.
- Basado en probabilidad hacia un futuro para expandir en gran número el sistema sin problemas ni restricciones.

2.10 Especificaciones ANSI/TIA-942-A.

Este estándar crea requisitos para los Data Center y su infraestructura de telecomunicaciones, incluido los Data Center de renta a inquilinos en la nube y los usuarios de Internet multisesión.

La TIA-942 divide la infraestructura de un Data Center en 4 subsistemas:

- Telecomunicaciones
- Arquitectura
- Sistema Eléctrico
- Sistema Mecánico

Estas especificaciones que se tratan con este estándar pueden ser usadas para Data Center que operan en lugares muy pequeños o para aquellos Data Center que ocupan múltiples pisos o salas en las grandes empresas.

Este estándar fue desarrollado en el año 2012 por el subcomité de cableado para edificios comerciales. En esta nueva edición se incorpora contenidos de la normativa ANSI/TIA-942 y anexos donde se trabaja con cable coaxial de 75 ohmios en caso de tendidos de cable en orientación horizontal con longitudes más largas, entre otros.

Entre las principales cosas que se modificaron fueron:

Relación de espacios en los Data Centers: En este literal se toma en cuenta como debe ser la distribución en cuanto al espacio en el que un Data Center debe estar operando.

- Primero se puede verificar que se tiene un cuarto de acometidas en donde se tendrán todas las tomas eléctricas con corriente alterna o continúa dependiendo del diseño del Data Center para poder realizar toda la conexión del equipamiento, racks, entre otros y lograr así su correcto funcionamiento de acuerdo con las necesidades que demande cada equipo.

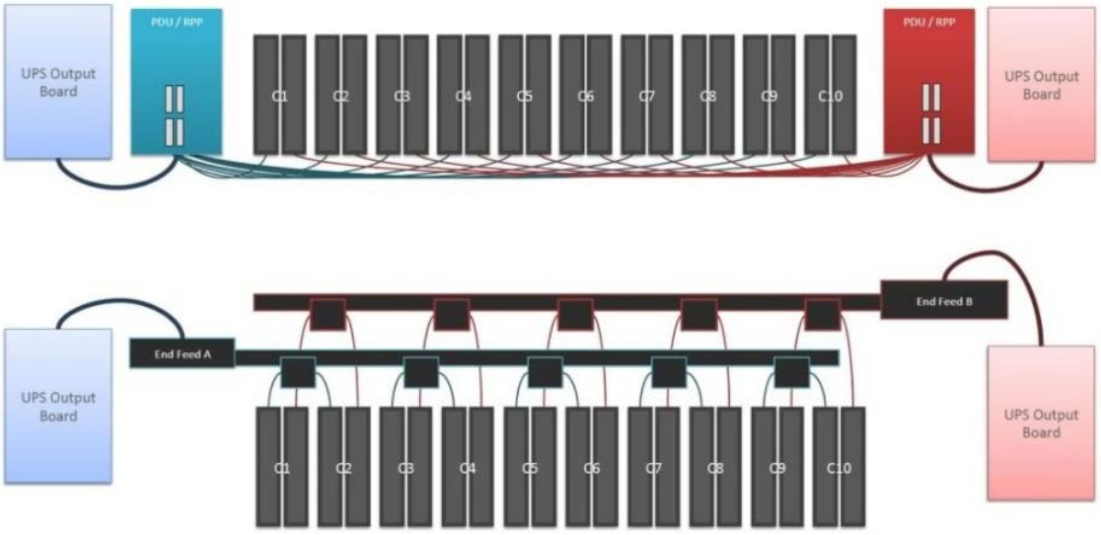


Figura 19. Esquema TIER IV.
Tomado de (POWERNET, 2016).

- Después se tiene un cuarto mecánico en el cual se puede manejar equipos para el sistema de climatización, detención de intrusos o peligro de incendios los cuales son necesarios para el funcionamiento del Data Center.

- Además, se tiene un espacio para el control y monitoreo del trabajo del Data Center para su respectivo análisis de datos constante.

- En la parte exterior se tiene un gabinete para el manejo de todos los equipos de telecomunicaciones mismos que sirven para

extender las redes de comunicaciones en cada una de las oficinas y los pisos que requieran mantenerse comunicaciones de acuerdo con el cargo que cada uno de los empleados necesite.

- Se estableció también una topología estándar con los elementos principales que se necesitan para el manejo de un Data Center.

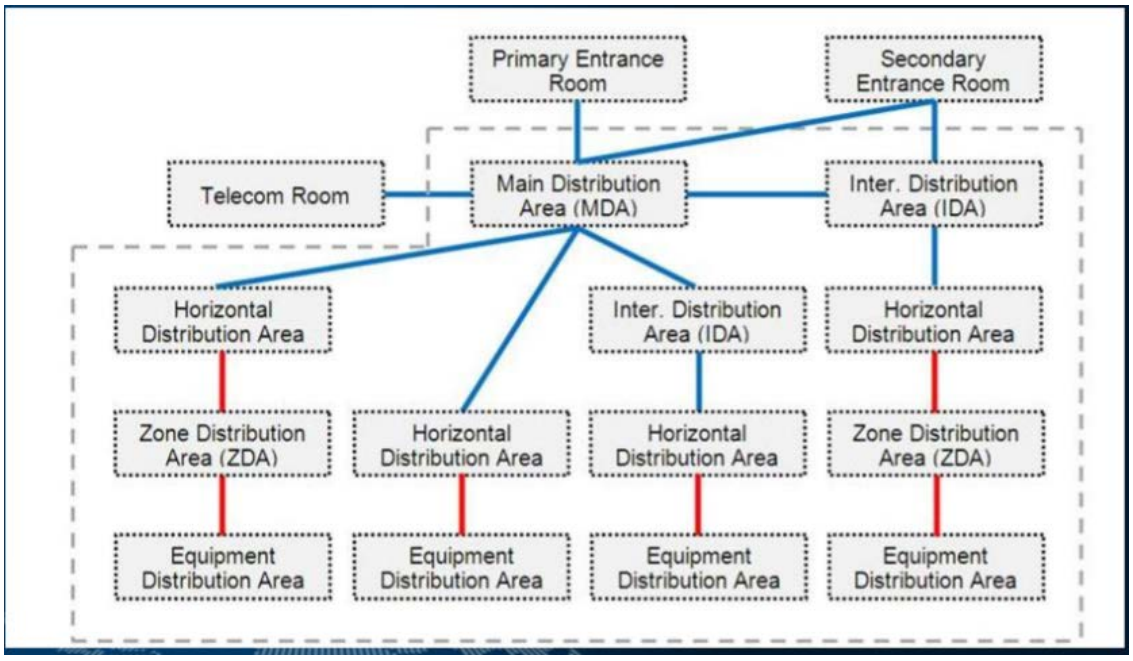


Figura 20. Topología de distribución Data Center.
Tomado de (Siemon, 2018).

- Adopción en la terminología de acuerdo los espacios que se instalaban en el sitio.

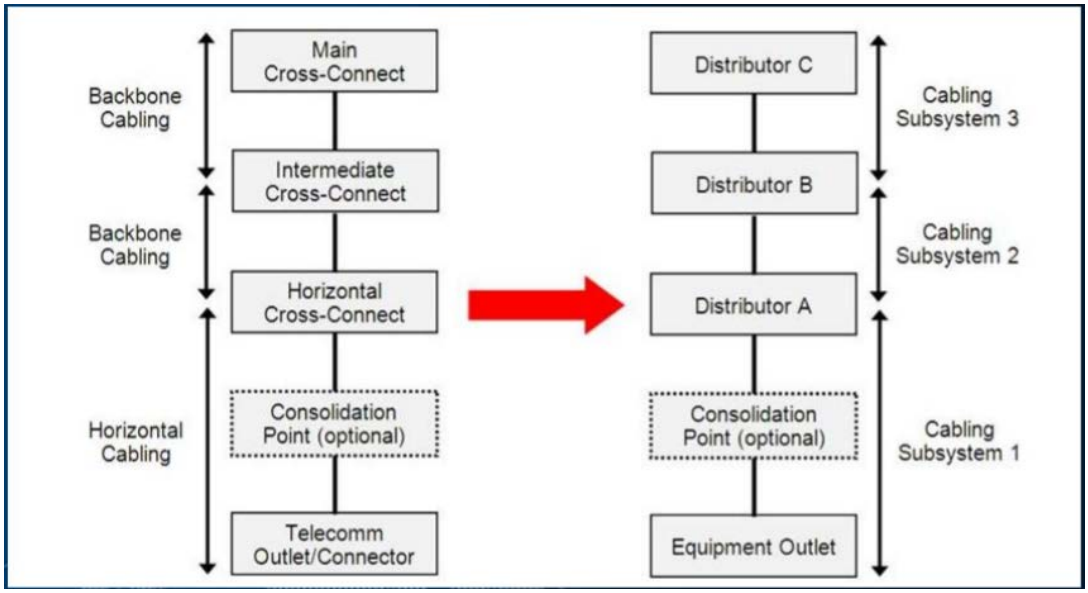


Figura 21. Manejo de la terminología.

Tomado de (Siemon, 2018).

- Se retiró el límite de 100 metros para cableado horizontal de fibra óptica. Ahora el límite depende netamente del sistema que se vaya a instalar.

- Con este nuevo estándar se reconocen solamente categorías 6 y categorías 6A en el uso del cableado.

- Ya no se usan especificaciones de fibra óptica de multimodo con OM1 y OM2. Sino que ahora se reconoce OM3 y OM4 ya que brinda mayores ventajas con respecto a manejo de mayores tasas de tráfico, demanda de ancho de banda, múltiples conexiones a Ethernet y enlaces de conexiones de 10 Gbps a 40 Gbps.

- Se usan conectores LC (conectores pequeños) solamente para 1 o máximo 2 fibras en caso de que se requiera más fibras para la conexión se requiere un conector MPO el cual ofrece una densidad 12 veces más que la densidad de los conectores estándar de manera que se tiene un ahorro de espacio y valores monetarios.

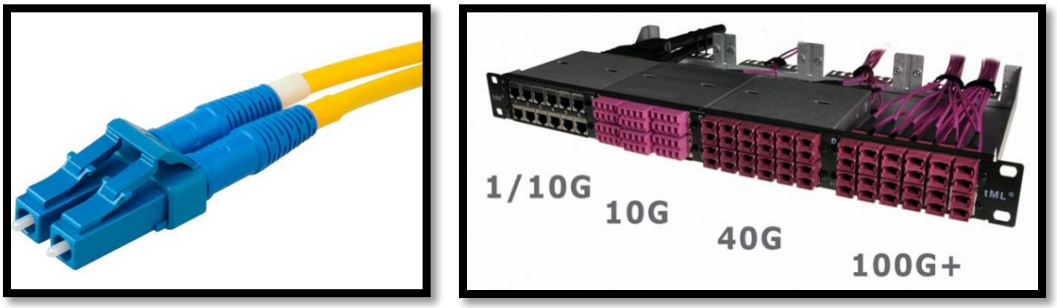


Figura 22. Conectores de Fibra.
Tomado de (fibraopticahoy, 2014).

- Se reconoce el IDA (Área de distribución intermedia) la cual ofrece un alto nivel de flexibilidad para que un Data Center crezca en fases o etapas de acuerdo con la necesidad que se vaya presentando con el desarrollo que se vaya tenido dentro de una empresa. Además de que cada piso o un grupo de pisos pueden tener un IDA en donde basen sus principales conexiones de funcionamiento para el Data Center, así como también para los equipos de telecomunicaciones siendo así escalable según las necesidades lo requieran.

- Se adoptaron términos de EO (Equipment Outlet) lo cuales consiste en asignar un conector en una implementación de servicios de cableado estructurado para su administración y pruebas de sistema como computadoras, teléfonos, automatización en edificios, puntos de acceso inalámbricos, cámaras o cualquier equipo que desee conectarse a la red.

- Además, se adoptó el término ENI (External Network Interface) la cual es una interface para conexión en las redes externas de un sistema de acuerdo con las especificaciones que nos brinde la ISO/IEC 24764.

- Con respecto a trabajar con par trenzado balanceado se utilizan netamente las categorías 3, 5E, 6 y 6A, según las pruebas realizadas la categoría que más se recomienda en la 6A por sus

características eléctricas que son más eficientes en los sistemas eléctricos.

- Con respecto a trabajar con fibra óptica que es el elemento de transmisión más usado hoy en día se tiene que para transmisiones de fibra óptica multimodo 50/125 mm optimizado para láser de 850 nm.

- Para fibra óptica monomodo también se recomienda trabajar con OM3 y OM4.

- Cuando se trata de trabajar con cable coaxial este estándar nos recomienda operar con una cantidad de voltaje en los 75 W.

- Para brindar una eficiencia energética se puede acomodar pasillos fríos y calientes en forma alternada para que ninguno de los equipos obstruya al otro.

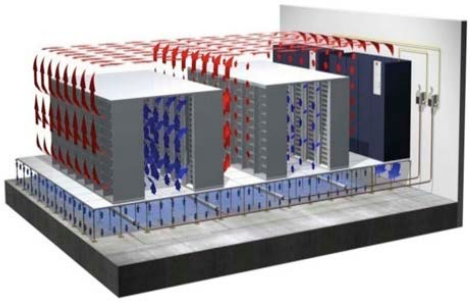


Figura 23. Distribución de pasillos calientes y fríos.
Tomado de (HVACR, 2014).

- Aislar equipos según sus características ambientales.

- Uso del cableado en la parte superior de los racks o gabinetes de equipos.

- En caso de que el cableado vaya a ser instalado en el piso falso del Data Center es decir en la parte inferior de los equipos conectados se recomienda tener un buen sistema de distribución de aire en esta sección.

- La ruta del mismo debe estar de preferencia por los pasillos que manejen temperatura caliente.

- El cableado se debe manejar de manera correcta y ordenada con el fin de que no se obstruya la debita ventilación que manejan cada equipo.

- Es obligatoria la necesidad que se tiene de retirar el cable que ya no se va a utilizar, se obligación del personal de mantenimiento realizar un seguimiento completo lo cual permita retirar todas las conexiones que ya no se vayan a utilizar y no sean útiles.

- Utilizar placas ciegas siempre y cuando sean espacios no utilizados.

- Instalar barras de contactos o PDUs que sirvan para un monitoreo constante y acceso a los niveles de potencia del mismo.

- Trabajos constantes de selladores en paso de cable en el piso falso o manejo de gabinetes.

- Equipos que tenga un tipo de ventilación especifico es decir con la ventilación de frente hacia atrás para manejar de mejor manera la temperatura en general del Data Center con el fin de no generar daños en los equipos.

La TIA-942 en cuanto a Seguridad por TIER recomienda que para mejorar la seguridad física de un centro de datos se debe tomar criterios como la grabación de videovigilancia por velocidades de cuadros y niveles de control de acceso.

La forma más sólida y estratégica para alcanzar la seguridad física óptima es diseñar y administrar un Data Center en términos de capas. La TIA 492 recomienda crear capas en su estructura de protección física, lo que ayuda a

confirmar la falla de un elemento en el sistema, las capas internas también ayudan a prevenir datos maliciosos o incluso no deseados, infracciones de los empleados, hardware y selección del sitio.

Las medidas de seguridad se pueden clasificar en cuatro capas:

• Perímetro de seguridad (Primera Capa)

• Controles de las instalaciones (Segunda Capa)

• Controles de la sala de ordenadores (Tercera Capa)

• Controles del gabinete (Cuarta Capa)

El direccionamiento de cada una de estas capas brinda protección integral e integrada desde el perímetro de la instalación hasta los gabinetes en el centro de datos.

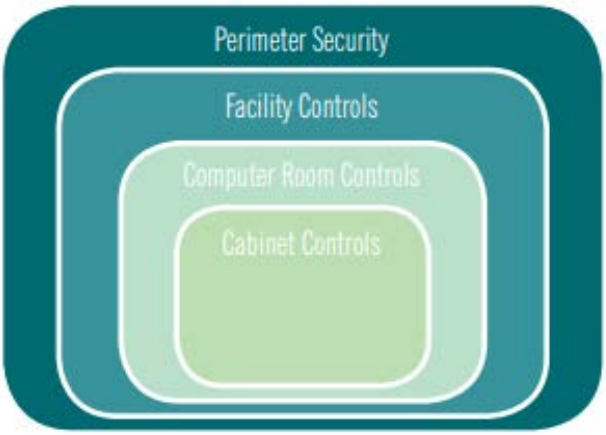


Figura 24. Seguridad física por capas
Tomado de (ANIXTER, 2011)

Tabla 7.
El objetivo y medidas de seguridad por capa.

	Primera capa	Segunda Capa	Tercera Capa	Cuarta Capa
Objetivo	Disuadir, detectar y retrasar Integrar sistemas Proporcionar capas de protección	Restringir el acceso Redundancia en comunicación Sistemas integrados	Restringir el acceso Controlar el acceso no autorizado	Última línea de defensa Restringir el acceso Sistemas integrados para una mayor seguridad
Medidas de seguridad	Barreras físicas Endurecimiento del sitio Iluminación Detección de intrusos Video vigilancia Entrada física y control de acceso	Video vigilancia Control de acceso	Análisis de video Biometría RFID	Bloqueo a nivel de rack Pistas de auditoría Infraestructura inteligente

Tomado de (BISCI, 2015)

Tabla 8.

Muestra de cada capa de la TIER-492-SEGURIDA FISICA.

Primera Capa		

Segunda Capa		
Tercera Capa		
Cuarta Capa		

La TIA-942, seguridad por Data Center por TIER indica:

Tabla 9.

Seguridad por capas para los TIER.

Paredes, ventanas y puertas resistentes	**Tier 1**	**Tier II**	**Tier III**	**Tier IV**

seguridad en el lobby	n/a	n/a	Level 3(min)	Level 3(min)
Contador de seguridad en envío y recepción	n/a	n/a	n/a	Level 3(min)

Tomado de (BISCI, 2015)

CCTV Supervisión	**Tier 1**	**Tier II**	**Tier III**	**Tier IV**
Perímetro y estacionamiento	No requerida	No requerida	si	Si
Generadores	n/a	n/a	si	Si
Accesos de control de puerta	No requerida	si	si	Si
Piso de cuarto de computadores	No requerida	No requerida	si	Si

Tomado de (BISCI, 2015)

Acceso de control de seguridad/monitoreo	Tier 1	Tier II	Tier III	Tier IV
Fibra almacenada	Cerradura industrial	Detención de intrusos	Detención de intrusos	Tarjeta de acceso

Puerta de emergencia	Cerradura industrial	monitoreo	Ingreso por código	Ingreso por código
Accesibilidad de ventanas	Sin monitor	Detención de intrusos	Detención de intrusos	Detención de intrusos
Centro de operaciones de seguridad	n/a	n/a	Tarjeta de acceso	Tarjeta de acceso
Puerta para entrar cuarto de computadores	Cerradura industrial	Detención de intrusos	Tarjeta Biométrica	Tarjeta Biométrica

Tomado de (BISCI, 2015)

3. CAPITULO III. IMPLEMENTACIÓN DE SERVICIOS EN EL DATA CENTER ACADÉMICO.

Para proceder con la implementación, tenemos que elegir una metodología de desarrollo, para esta tesis utilizamos un estudio por fases, donde tendremos una etapa de descripción de la situación actual donde encontraremos las problemáticas, después analizaremos los requerimientos, tendremos una etapa de diseño y por último tendremos la etapa de implementación. Lo anteriormente mencionado se verá en este capítulo.

3.1 Situación actual para el proyecto de seguridad.

3.1.1 Ubicación geográfica del Data Center Académico Queri – Udla.

La Universidad de las Américas consta de cuatro campus ubicados en Quito. Este proyecto se enfoca directamente a la implementación para la Udla sede Queri la cual se encuentra ubicada en la calle José Queri entre Av. De los Granados y Av. Eloy Alfaro, en la ciudad de Quito, en la provincia de Pichincha.

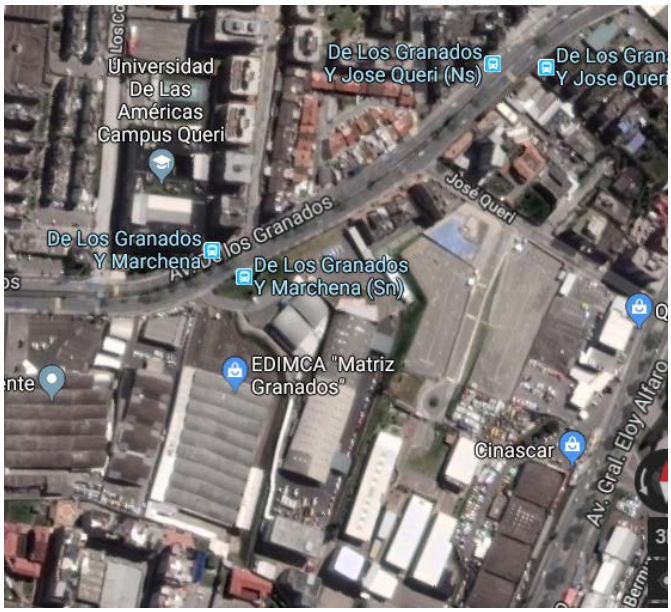


Figura 25. Ubicación geográfica campus Queri.
Adoptado de (Google, s.f.).

Figura 26. Edificio número 4, facultad FICA.

Figura 27. Laboratorio 466 – Data Center Experimental.

Figura 28. Laboratorio 464.

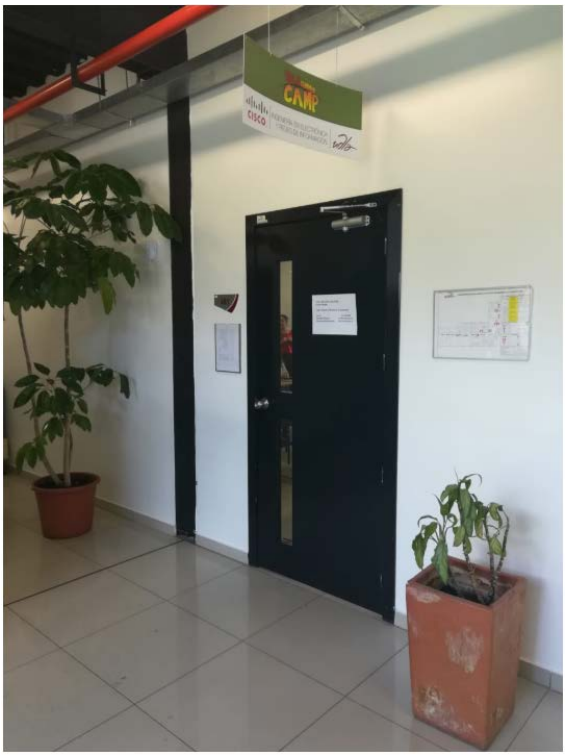


Figura 29. Laboratorio 461.

3.1.2 Planos de los laboratorios Sede Queri – Udla.

El bloque número 4 de la sede Queri de la Facultad de Ingeniería de Ciencias Aplicadas consta de 3 pisos los cuales están divididos en subsuelo, planta baja y un primer piso. Este proyecto será implementado en planta baja del bloque número 4, para tener un control de seguridad más profundo de todo el equipamiento interno que está dentro del mismo.

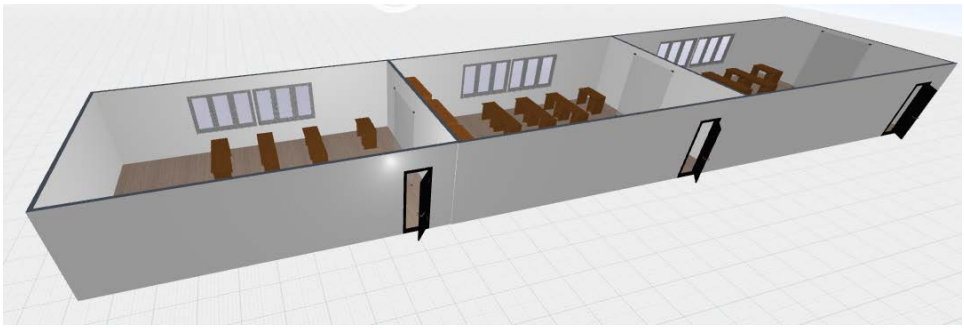


Figura 30. Laboratorios planta baja.

3.1.3 Laboratorio 466.

El laboratorio 466 consta de dos ambientes divididos en su interior de la siguiente manera:

- Cuarto de equipos Data Center Académico: 18 m2
- Laboratorio de clase: 6 m2

Dentro de este laboratorio se trabaja con un conjunto de computadores dividas en dos columnas, en la columna izquierda tenemos dos filas de 4 computadores por cada fila. En la columna derecha tenemos 4 filas de 6 computadoras en las 3 primeras filas y dos computadoras en la última fila. Además de tener una computadora principal frente de todas las columnas que sirve para que el docente pueda manejar el material didáctico que se va a entregar a los estudiantes. En la parte del fondo del laboratorio al lado derecho se tiene un gabinete con equipos de red los cuales sirven para la conectividad de todas las computadoras internas mediante una LAN interna. Al lado izquierdo se tiene un cuarto con los equipos de Data Center que se maneja de manera aislada y solo tiene acceso el personal autorizado. Ver Anexo1.

Figura 31. Laboratorio466.

3.1.4 Laboratorio 464.

El laboratorio consta de un solo espacio general en donde se trabaja con un centro de cómputo las cuales tiene una distribución de 1 columna en el centro con 4 filas de computadoras y 4 equipos computarizados en cada fila. Además, tiene dos filas adicionales de computadoras en cada extremo del laboratorio que maneja un total de 5 computadoras en cada lado. En la parte frontal del laboratorio se tiene un computador designado para el uso solo del docente como herramienta didáctica para impartir sus clases.

Y en la parte de atrás del laboratorio se tiene en la parte céntrica varios anaqueles donde se guardan los equipos y documentación. En la esquina izquierda existe un espacio designado para manejo de switch de conectividad de todas las computadoras del laboratorio formado una LAN interna. Ver Anexo2.

- Laboratorio de clase: 24 m2.

3.1.5 Laboratorio 461.

El Laboratorio consta de dos columnas escritorios con computadores para el uso de los estudiantes, en donde una columna consta de 3 filas que tiene un total de 5 computadoras por fila y la segunda columna tiene 3 filas con dos computadoras por cada fila. Ver anexo3.

En la parte posterior del laboratorio se tiene 3 anaqueles grandes en donde se guardan equipos para las practicas estudiantiles.

- Laboratorio de clase: 24 m2

3.2 Problemática de la situación actual.

Después de examinar la situación actual y recoger datos del capítulo 1 y 2, encontramos que no se está aplicando un estándar de seguridad perimetral para el Data Center Académico.

Tabla10.
Problemática de la situación actual.

	Problemática
Laboratorio 466	No existe un sistema de seguridad, en la que TIA-942 recomienda que se posea un subsistema de Arquitectura, con un control de seguridad perimetral por capas.
Laboratorio 464	No existe un control de seguridad para el laboratorio 464.
Laboratorio 461	No existe un control de seguridad para el laboratorio 461.

3.3 Análisis de requerimientos.

El análisis de requerimientos nos sirve para validar cuales son las verdaderas necesidades que requiere el usuario y con qué respuesta tecnológica se puede cubrir dicha necesidad.

3.3.1 Requerimientos Laboratorio 466.

En este laboratorio se manejan los equipos para estudiantes y un Data Center Experimental motivo por el cual se debe tener un estricto control de quien entra, quien sale y quien administra los equipos internos del Data Center.

Tabla 11.

Requerimientos del laboratorio 466 bloque 4 sede Queri – Udla.

N.-	Ambiente	Requerimiento	Normativa
1	**Laboratorio 466**	Control del correcto funcionamiento del	El Data Center, funciona en un

		equipamiento del Data Center.	ambiente de pruebas.
2	**Laboratorio 466**	Control mediante cámaras IP el ingreso de personas no autorizadas.	TIA 942, del subsistema de arquitectura, control de seguridad por capa 1.
3	**Laboratorio 466**	Control de conexiones no autorizadas mediante el access point.	TIA 942, del subsistema de arquitectura, control de seguridad por capa 4.
4	**Laboratorio 466**	Control mediante un sensor de movimiento interna la presencia de personas no autorizadas.	TIA 942, del subsistema de arquitectura, control de seguridad por capa 2.
5	**Laboratorio 466**	Manejo de una página Web levantada desde el Data Center.	El Data Center, funciona en un ambiente de pruebas.

3.3.2 Requerimientos Laboratorios 464.

En este laboratorio se maneja un total de 3 columnas distribuidas de la siguiente manera: en la parte central se tienen 3 filas que se componen de 4 computadores por fila, una columna ubicada al lado izquierdo que consta de 5 computadoras y de igual manera existe otra columna con las mismas características al lado derecho. En la parte frontal existe un escritorio con una computadora para uso didáctico del profesor que se encuentre a cargo.

En la parte posterior existen dos grandes anaqueles mismos que sirven para guardar equipamiento mismo que se debe tener un control constante es por eso por lo que se desea implementar este sistema de seguridad para el manejo correcto y evitar valores altos de pérdidas materiales cuidando de esta manera los bienes de la Universidad.

Tabla 12.

Requerimientos del laboratorio 464 bloque 4 sede Queri – Udla.

N.-	Ambiente	Requerimiento	Normativa
1	**Laboratorio 464**	Control mediante cámaras IP el ingreso de personas no autorizadas.	Sistema de seguridad de perímetro.
2	**Laboratorio 464**	Control de conexiones no autorizadas mediante el access point.	Sistema de seguridad de perímetro.
3	**Laboratorio 464**	Control mediante un sensor de movimiento interna la presencia de personas no autorizadas.	Sistema de seguridad de perímetro.

3.3.3 Requerimientos Laboratorio 461.

Este laboratorio es una de las que manejan más valores de activos dentro de nuestra carrera, pero nos hemos dado cuenta de que no se tiene la seguridad necesaria para evitar pérdidas o llevar un control más efectivo. Este laboratorio se maneja equipamiento y computadores.

Tabla 13.

Requerimientos del laboratorio 461 bloque 4 sede Queri – Udla.

N.-	Ambiente	Requerimiento	Normativa
1	**Laboratorio 464**	Control mediante cámaras IP el ingreso de personas no autorizadas.	Sistema de seguridad de perímetro.
2	**Laboratorio 464**	Control de conexiones no autorizadas mediante el access point.	Sistema de seguridad de perímetro.
3	**Laboratorio 464**	Control mediante un sensor de movimiento interna la presencia de personas no autorizadas.	Sistema de seguridad de perímetro.

3.4 Diseño para Sistema de seguridad.

Para el diseño de sistema de seguridad tenemos que analizar cada uno de los requerimientos solicitados, estudiándolos cada uno con posibles alternativas para la instalación. Vamos a partir identificando que es un sistema.

Sistema: Se lo define como un conjunto de elementos que trabajan entre sí cumpliendo un ciclo definido con un ingreso de datos de entrada y luego del proceso se tiene un resultado de salida para obtener un resultado deseado. (Cruz, 2013)

Seguridad: Se lo define como ejercer una acción de protección ante un elemento definido puede ser estas personas, animales, vida, equipos, construcciones, entre otros mismos que son muy importantes y que se debe mantener alejado cualquier tipo de riesgo que los eche a perder generando altas perdidas. (Cruz, 2013)

Por lo tanto, un sistema de seguridad es todo un conjunto de elementos que trabajan relacionados unos con los otros con el fin de ofrecer un alto grado de protección contra ciertos peligros que pueden existir generando pérdidas

materiales o económicas y a su vez generando confianza ante los elementos que van a ser monitoreados.

3.4.1 Sistemas de seguridad por cámaras.

Es una tecnología de videovigilancia diseñada para supervisar una diversidad de ambientes y actividades. Puede estar compuesto por una cámara o por un conjunto de estas a una conexión por red de comunicación IP permitiendo de esta manera el monitoreo de las cámaras remotamente con el envío y recepción de imágenes y audio. Presenta grandes ventajas de ahorro de recursos ya que es un sistema que se monta sobre la misma red que normalmente maneja una empresa como el cableado, acceso a Internet y manejo de correo electrónico.

Con el paso de los años día a día se van teniendo cada vez mejores soluciones para implementar cámaras ya que en el mercado se puede encontrar cámaras inalámbricas, cámaras 360, cámaras con altos niveles de megapíxeles en la imagen, cámaras integradas con sensores de movimiento, cámaras con infrarrojo, entre otros.

3.4.1.1 Elementos de sistema de seguridad de cámaras.

Entre los principales elementos que se encuentran para trabajar en conjunto con las cámaras tenemos:

- VMS (Sistema de gestión de video): Corresponde a un elemento que sirve para grabar o visualizar las imágenes de las cámaras mediante conexión local o remota, permite gestionar accesos, gestiona permisos a los diferentes usuarios, permite la configuración de cámaras de manera remota, entre otros.

Figura 32. Sistema de gestión de vídeo.

Tomado de (Security, 2018)

- DVR (Grabador de video): Es un disco duro que va conectado en cascada con las cámaras el cual está programado para ejecutar grabaciones dependiendo de cómo se lo configure como puede ser por horas determinadas dentro del día, de manera constante, al detectar movimiento, entre otros.

Figura 33. Grabador de vídeo.

Tomado de (Sosio, 2013)

- Software: Cada empresa que comercializa cámaras dentro del mercado ofrece un software libre o licenciado dependiendo el caso para hacer uso correcto de monitoreo y control de las cámaras en los puntos instalados. También se puede realizar configuración en las cámaras para que se detecten ciertos volúmenes de cuerpos ante un movimiento para comenzar a grabar de esa manera se descarta la aparición de animales pequeños por ejemplo que no representan un gran peligro.

  Es necesario el control de un administrador de red para que defina todos los parámetros necesarios dentro de un sistema de

videovigilancia de esa manera se puede tener ahorro de recursos y control de eventos verdaderamente importantes dependiendo del escenario que se presente.

Figura 34. Software de administración de videovigilancia.
Tomado de (Cardoso, 2015)

- Dispositivos de visualización: Estos equipos sirven para realizar un monitoreo físico de las cámaras para analizar parámetros de video y audio siempre y cuando estén correctamente conectados a la red IP del sistema por lo tanto estos pueden ser: monitores, pantallas, computadores, entre otros.

Figura 35. Equipos de visualización.
Tomado de (Descargar, 2018)

- Filtros infrarrojos: Son dispositivos que se encienden cuando las condiciones luminarias del sitio donde se va a grabar son bastante escasas. Existen dos tipos principales: filtros de corte los cuales se pueden activar manualmente o automáticamente. También se tiene los filtros duales mismos que se encuentran entre el lente y el sensor de la cámara pero que básicamente tiene el mismo objetivo.

- LEDS infrarrojos: Son puntos que generan luz infrarroja, su tonalidad es casi imperceptible ante la visualidad humana, pero de gran ayuda ante las cámaras IP brindado de esta manera una buena visión nocturna y no tener excusas ante ningún escenario ofreciendo mejor calidad de seguridad.

Figura 36. LEDs infrarrojos.
Tomado de (Electrónica, 2018)

- Carcasas de protecciones en exteriores: Son domos que protegen las cámaras ante los cambios climáticos que se pueden presentar pero que no se interponen ante la capacidad de visualización de las cámaras para no perder ningún detalle dentro de su grabación.

Figura 37. Domos de protección.

Tomado de (SONY, 2018)

- Sensores: Dispositivos que colaboran con el funcionamiento de grabaciones automáticas de acuerdo con los escenarios precisamente necesarios como pueden ser un determinado sonido, un determinado movimiento, grados de temperatura, etc.

Figura 38. Sensores.

Tomado de (Taringa, 2018)

- Cableado Ethernet: Es el cableado que se usa para la unión de las cámaras en conjunto con la red a la que estas van a poder ser monitoreadas y tener acceso a las mismas, normalmente estas trabajan con cableado coaxial.

Figura 39. Cable Ethernet.
Tomado de (Good, 2018)

- PoE: Este tipo de tecnología presenta ventajas en la reducción del uso del cableado ya que por el mismo cable se puede enviar datos y corriente eléctrica así no es necesario estar pendientes de establecer conexiones eléctricas en lugares existe escases de los mismos.

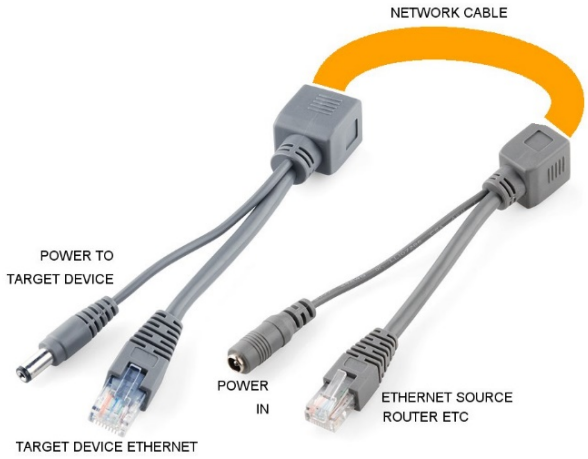


Figura 40. Cable PoE.
Tomado de (Electronics, 2018)

- Firewall: Protección ante posibles personas que son hackers o intrusos en la red de videovigilancia IP para robo de información y perdida de importante información.

3.4.1.2 Tipos de cámaras de seguridad.

Existen varios tipos de cámaras de seguridad dentro del mercado las cuales se adaptan de acuerdo con las necesidades que el cliente o usuario exija de manera que se cumpla totalmente el servicio que se requiera para su uso. A continuación, vamos a revisar que tipos de cámaras existen y en que consiste cada una:

- Cámara Bullet: Estas cámaras se las puede instalar en la pared o en el techo en ambientes internos o externos sin problemas. Estas cámaras tienen una forma cilíndrica, resistente al agua, su enfoque consiste en cubrir un área determinada es decir no se puede mover para captura planos panorámicos y tampoco realiza zoom, por lo tanto, la cámara se la instala en dirección directa al área que se desee monitorear.

Figura 41. Cámara Bullet, marca Dahua.
Tomado de (Dahua, 2018)

- Cámaras Domo: Estas cámaras llevan su nombre debido a la forma que tiene su carcasa de protección misma que son como un caparazón que permite una mayor protección de la cámara interna tratando así que sea discreta ante los ojos de las personas. Estas cámaras tienen la ventaja de que pueden girar 360º a una velocidad rápida.

Figura 42. Cámara Domo, marca Dahua.
Tomado de (Dahua, 2018)

- Cámaras Domo de Velocidad: Estas cámaras son similares a las que nombramos anteriormente, pero tienen la capacidad de inclinarse, captar una imagen panorámica y realizar tomas con zoom. Es decir, dan la libertad a los operadores de control de movilizarse al 100% para obtener mejores resultados.

Figura 43. Cámara Domo, marca epcom.
Tomado de (Epcom, 2018)

- Cámaras ocultas: Estas cámaras son aquellas que vienen disfrazadas dentro de un equipo que simula totalmente otra cosa como un reloj, un sensor o un adorno con el fin de pasar

totalmente desapercibida ante los ojos de las personas y las mismas pueden actuar con total normalidad.

Figura 44. Cámara Oculta.
Tomado de (LineMark, 2018)

- Cámaras infrarrojas: Estas cámaras se basan en amplificar la intensidad o captar longitudes de onda no visibles para el ojo humano, por lo tanto, considera el uso de LEDs infrarrojos para capturar imágenes mostrando luz desde los 0.75 a los 2 micrómetros con el fin de capturar imágenes.

Figura 45. Cámara con lente infrarrojo.
Tomado de (Store, 2018)

- Cámaras IP: Estas cámaras pueden ser cableadas o inalámbricas mismas que pueden transmitir video o imágenes por Internet, normalmente tratan de comprimir el tamaño del contenido para no saturar el ancho de banda de la red. Con este tipo de cámaras nos podemos conectar mediante el smartphone o equipos similares para acceder a las imágenes de la cámara y monitorearlas desde algún lugar lejano.

Figura 46. Cámaras IP.
Tomado de (FireOS, 2018).

3.4.1.3 Ventajas y desventajas del uso de cámaras de seguridad.

Tabla 14.
Ventajas y desventajas de las cámaras de seguridad

Ventajas	Desventajas
Vigilancia que genera tranquilidad	No solo las cámaras realizan el trabajo de atrapar físicamente a un intruso

En monitoreo constante se puede prevenir robos	En los lugares incorrectos puede violar parámetros de privacidad
Acceso remoto para monitoreo de cámaras	Si el lente es tapado ya no se puede obtener ninguna imagen
Captura de pruebas ante un atraco	Solución costosa
Mantener registros al tiempo completo	Difíciles de ocultar

.

3.4.2 Sistemas de seguridad por biométrico.

Estos sistemas son los que hoy por hoy están en auge ya que sea una micro empresa o una gran empresa trabajan con este tipo de control para el manejo de personal interno logrando así resultados reales en los informes que se realizan cuando se valida la hora de entrada, salida, hora de almuerzo entre otros.

Pero primero se debe entender que significa la palabra biométrico o biometría. Biometría: “Es la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos” (Niesteszeck2, 2012).

Cada persona individual tiene su propia identidad biométrica y existen métodos matemáticos y computacionales los cuales sirven para almacenar cada detalle de las personas para tener una identidad biométrica dentro de una base de datos informática.

Los sistemas biométricos que guardan información lo hacen mediante elementos informáticos que capturan datos de las huellas de los dedos de la mano, el iris

de los ojos, tono de voz, manos, etc. de las personas que cada una es diferente a la otra en todo el mundo.

Sistema biométrico: “Es un sistema automatizado que realiza tareas de biometría. Es decir, un sistema que basa sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida y/o verificada de forma automatizada”. (Niesteszeck2, 2012).

3.4.2.1 Tipos de biometría.

- Biometría fisiológica: Estas se basan directamente en tomar medidas e información de elementos importantes y básicos del cuerpo humanos como pueden ser: manos, ojos, voz, rostro, entre otros.

- Biometría conductual: Estas se basan directamente en tomar medidas e información de las acciones que ejercen las personas como reconocimiento único ante el resto de humanos mismos que pueden ser por el uso de teclado o firma de una persona.

3.4.2.2 Tipos de sistemas de biométricos actuales.

Entre los principales sistemas que se tienen hoy en día y se han desarrollado en producción tenemos:

- Rostro
- Termo grama del rostro
- Huellas de la mano
- Geometría de la mano
- Venas de la mano
- Iris de los ojos

- Retina de los ojos
- Voz
- Firma

Por lo tanto, vamos a hacer un análisis general de cada uno de los sistemas antes mencionados:

- Huella de la mano: Como sabemos cada persona tiene una huella dactilar única y diferente por persona. Basando en este principio se crean los sistemas de control por huellas los cuales analizan el conjunto de arcos, ángulos, bucles, remolinos, entre otros característicos que conforman una huella y al analizarlo se forma la identificación de una persona.

Figura 47. Huella dactilar.
Tomado de (Oriente, 2012).

El proceso para procesar una huella digital lo vamos a resumir en la siguiente imagen:

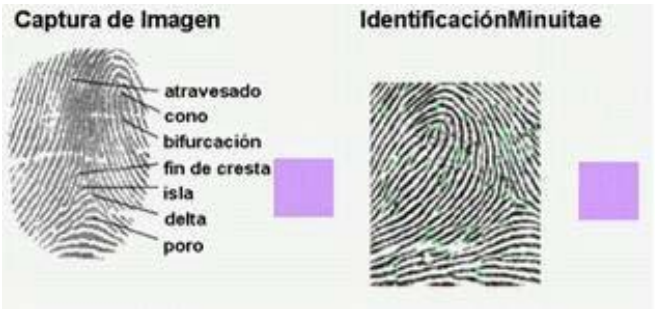


Figura 48. Procesamiento de huella digital.
Tomada de (Murcia, 2018).

- Voz: Este método consiste en grabar una lectura de una frase por parte de los usuarios que van a ser monitoreados, al realizar dicha grabación se toma en cuenta que tono de voz tiene la persona analizada, su gravedad, sus agudos entre otros. Con esa muestra se realiza una comparación entre los intentos de los usuarios para acceder al sistema y la voz grabada para proceder con la autorización o no de un acceso. Los métodos para reconocer la voz son: dependencia, texto aleatorio e independencia de texto.

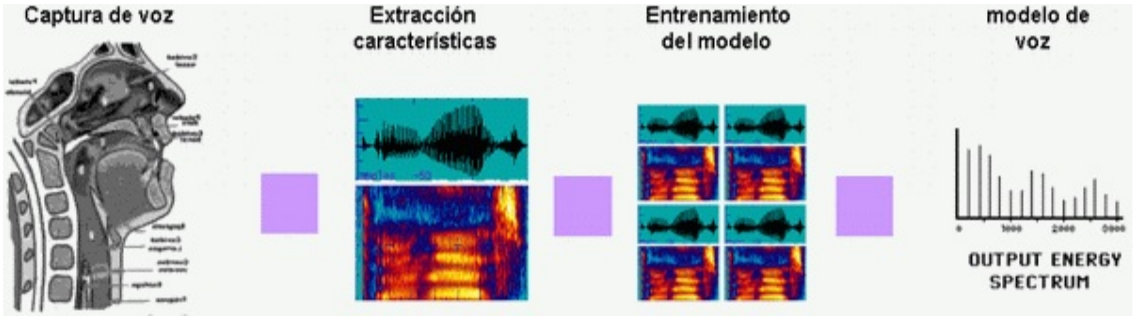


Figura 49. Procesamiento de la voz.
Tomado de (Murcia, 2018).

- Patrones oculares: Los dos factores que se toman para el reconocimiento en el tema de los ojos son el iris y la retina. Se han realizado pruebas con millones de personas en donde la probabilidad de semejanza en casi nula.

Las formas para escanear los ojos consisten en:

- Escáner de iris: Se analiza los colores únicos de los surcos de la parte coloreada de las pupilas de los ojos mediante una videocámara.

- Escáner de retina: Se analiza cuantas venas existen en el fondo de los ojos esto se logra al proyecta una luz infrarroja mediante la pupila para determinar dichas medidas.

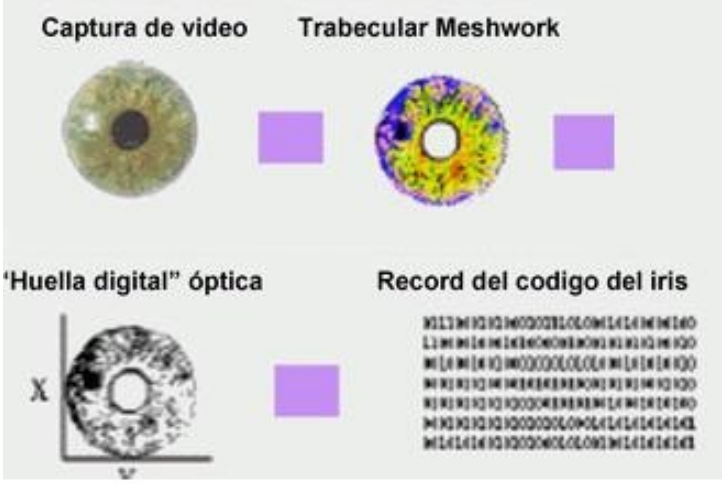


Figura 50. Procesamiento para análisis de los ojos.
Tomado de (Murcia, 2018).

- Identificación personal: Es un conocimiento neto que conoce una persona pero que puede ser compartida con un tercero. Entre los que se toman en cuenta son:

- Asignación de códigos: Se asigna un determinado código de clave para acceder al sistema.

- Posesión de elementos: Se entrega una tarjeta de logueo para su acceso al usuario.

3.4.2.3 Ventajas y desventajas para usar todos estos sistemas biométricos.

Tabla 15.
Ventajas y desventajas de los sistemas biométricos.

Tipo de seguridad	Ventajas	Desventajas
Rostro	Fácil, rápido y barato	Los niveles de iluminación pueden alterar la toma de datos.

Huella de mano	Barato y altamente seguro	Posibilidad de falsificación por duplicación o problemas de identidad por cortes
Iris y retina	Altamente seguro	Entrometido ante la privacidad del usuario.
Contorno de la mano	Poca memoria de almacenamiento	Lento e inseguro
Firma	Barato	Altamente grado de vulnerabilidad
Voz	Barato	Lento, alterado por el estado emocional del usuario, fácilmente vulnerable

3.4.3 Sistemas de seguridad por sensores.

Existen sistemas de seguridad que funcionan mediante el uso de sensores mismos que están diseñados para que al percibir algún tipo de evento se envié una alerta de aviso a un sistema central en el cual se pueda hacer un análisis de las alertas recibidas para ejecutar una acción adecuada con el fin de proteger y cuidar una línea de negocio evitando perdidas grandes.

Los sensores electrónicos son elementos de tamaño pequeño mismos que deben estar alimentados por fuentes o por baterías en el rango de voltaje de 6 a 12 V, además básicamente los sensores funcionan con un interruptor que esta entre abierto y cerrado dependiendo de la situación del medio en la que se encuentre.

Los sensores al percibir algún evento de peligro generan variaciones eléctricas mismas que son recogidas por una unidad de control que a su vez permiten la activación de alarmas o sirenas.

Tenemos un gran número de tipos de sensores los cuales permiten realizar una variedad de acciones como abrir puertas, detectar movimiento en lugares no autorizados, detectar roturas de equipos de vidrio, proteger cajas fuertes, entre otros.

Los sensores tienen dos tipos de conexión en los sistemas de seguridad, la primera forma de conexión es mediante la realización de cableado en las instalaciones o mediante receptores de radio.

Cuando la conexión de los sensores es cableada los costos de instalación son bastante altos ya que además de tener una línea de circuito cerrado se debe conectar una línea de alimentación en forma paralela misma que a su vez puede dañar la estética del lugar a proteger o se debe pensar en techo falso, así como varias maneras de ocultar lo mejor posible el cable que se implementara.

Cuando la instalación es bajo el diseño de sensores vía radio los beneficios son parecidos a los que hablamos anteriormente, pero su diferencia es que se conectan emisores de radio mismos que tiene un alcance de 60 o 70 metros cuadrados de alcance, siendo como principal ventaja respetar la estética del lugar a instalar y a su vez todas las señales son enviadas a una central de alarmas.

3.4.3.1 Tipos de sensores.

Existen diferentes tipos de sensores los cuales están clasificados de la siguiente manera:

Intrusión

Perimetrales

- Sensores de vibración

- Cinta conductora autoadhesiva
- Sensor por contactos magnéticos
- Sensor microfónico o de ruptura de vidrio
- Sensor de doble tecnología
- Volumétricos
- Radar o microondas
- Infrarrojos
- Lineales
- Barreras infrarrojos
- Barreras microondas
- G.P.S

Sensores varios

- Sensores de humo
- Sensor infrarrojo
- Sensor puntual
- Sensor iónico

Vamos a realizar un análisis de todos los tipos de sensores que existen y cuáles son los beneficios de cada uno para su uso e instalación.

- Sensores de intrusión: Estos sensores han sido creados para cubrir un determinado espacio el cual requiere de seguridad y detecta la presencia de individuos extraños al lugar mismos que no autorizados en horarios o lugares especiales.

Estos sensores pueden cubrir áreas perimetrales, volumétricas y lineales.

- Perimetrales: Estos sensores son los que se colocan en las periferias de los edificios estos pueden ser puertas ventanas, cerramientos, etc. Mismos que se activan cuando un intruso las atraviesa sin permiso. Debido a que se colocan en las periferias de un área específica para controlar el acceso interno de los intrusos estos sensores son creados con el fin de soportar cambios climáticos como viento, sol, lluvia, entre otros.

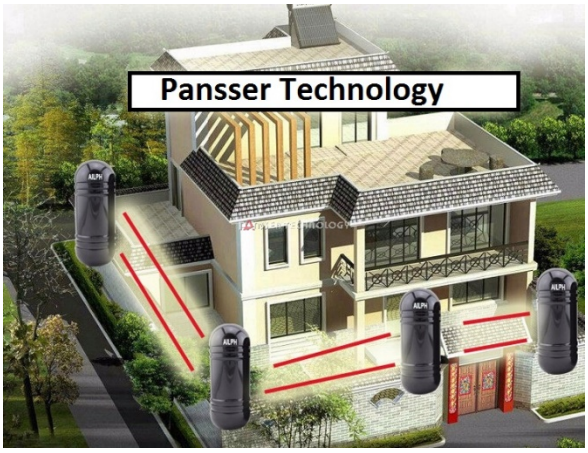


Figura 51. Sensores perimetrales.
Tomado de (panssertechnology, 2018)

- Sensor de vibración: Estos sensores trabajan mediante él envió constante de una señal eléctrica que al detectar un golpe o vibración en su parte interna se separan dos masas lo que causa interrupción en él envió de la señal eléctrica la cual informa que el sistema activo, al no tener esta señal constante directamente se activa una alerta.

Figura 52. Sensor de vibración.
Tomado de (Electan, 2018).

- Sensor piezoeléctrico: Son aquellos que se activan al recibir un golpe cuando se intenta quebrar un cristal. Este tipo de sensores no se recomienda instalar en lugares donde exista la presencia de camiones o elementos que produzcan vibraciones constantes.

- Sensor de mercurio: Estos sensores tienen una gota interna la misma que al moverse se cierra el circuito y envía una alerta de emergencia. Estas alertas se las utiliza en joyería o cristales en donde los cuerpos no deben moverse, pero tienen alta probabilidad de crear falsas alarmas motivo por el cual ya casi no se lo utiliza.

- Sensor por cinta autoadhesiva conductora: Este sensor consiste en una cinta conductora que se instala sobre el objeto al cual se va a proteger misma que al ser quebrada envía directamente una alarma de alerta a la central. Pero es un tipo de sensor ya que la cinta se la puede ver y el intruso al recortarla con cuidado puede retirarla sin generar ningún reporte de peligro hacia la central.

- Sensor por contactos magnéticos: Estos sensores se conforman por laminillas magnéticas que trabajan en el

escenario normal unidas una con otra, pero al separarlas se envía directamente una alerta de peligro como al abrir una puerta o abrir una ventana, generando una señal eléctrica que activa directamente la alarma.

Figura 53. Sensor magnético.
Tomado de (Saltillo, 2018)

- Sensor microfónico de rotura de vidrio: Se instalan cerca de los artículos a proteger máximo a una distancia de 100 metros, estos sensores se activan ante la presencia de sonidos agudos determinados dentro de un rango de frecuencia. Es decir, al romperse un vidrio o un cristal se activa directamente la alarma de seguridad. Los sonidos que se generan son: primer sonido impacto sobre un cristal mismo que se genera en el rango de 200 Hz y el segundo sonido es la ruptura del cristal que genera una frecuencia de 3000 a 5000 Hz. Es un sistema de alarma muy confiable con porcentajes bastantes bajos de generar alarmas falsas.

Figura 54. Cable sensor microfónica de seguridad.
Tomado de (Vende, 2018)

- Detectores de doble tecnología: Estos sensores combinan la detección por microonda y por infrarrojos. Son sistemas los cuales no envían alarmas si los dos no se activan evitando de esta manera alertas falsas.

- Sensores volumétricos: Son aquellos que detectan movimiento dentro de un espacio físico mismos que pueden ser oficinas, bóvedas de dinero, bodegas, etc. Tiene una cobertura bastante limitada de manera que la utilización deben de ser varios de estos para un cubrir un mismo lugar.

- Sensor por radar: Se componen por dos elementos importantes mismos que son un emisor y un receptor, el emisor envía ondas electromagnéticas en donde el receptor al recibirlas mantiene el sistema en equilibrio, pero en caso de no obtener una recepción normal directamente la alerta se activa reflejando un intruso dentro del área. Estas ondas son bastantes delicadas y finas que cubren en tu totalidad el área a proteger.

Figura 55. Sensor de movimiento por microondas.
Tomado de (ServiLuz, 2018)

- Sensor por infrarrojos: Estos sensores envían luces en línea recta dentro de los rangos infrarrojos que el ojo humano no puede percibir, pero protegen un lugar determinado en donde graban cuales son los objetos que por naturaleza se encuentran siempre ahí, pero cuando al percibir una variación en el volumen de estos envían directamente una alerta de peligro debido a la variación existente. Tienen un alcance de 8 a 20 metros.

Figura 56. Sensor infrarrojo.
Tomado de (Editronix, 2018)

- Sensores lineales: Estos sensores cubren áreas horizontales o verticales en forma plana, crean barreras mismas que al romperse envían una alerta.

- Sensores de barreras infrarrojas: Estos sensores están distanciados uno del otro por unos 10 centímetros, es decir, cuando el objeto haya atravesado las dos líneas infrarrojas el sensor envían una alerta de aviso, de esta manera se evita

falsas alarmas y su funcionamiento es igual en donde se cubren espacios por el envío y recepción de señal magnéticas de un punto al otro.

- Sensor de barrera por microondas: El equipo emisor envía impulsos VHF de alta frecuencia que se transmiten por cable, motivo por el cual se produce una onda de superficie que se propaga a lo largo y fuera del cableado transmisor. Al detectar la presencia de un intruso se envía una alerta directamente. Estos tipos de sistemas son utilizados en zonas militares, bodegas especiales, almacenes, etc.

- Sensor G.P.S: Estos sensores están instalados bajo del piso en forma de enterramiento mismos que se activan al ser presionados o cuando son pisados por los intrusos los cuales generan alertas directamente.

Sensores varios:

- Sensor de humo: Es un dispositivo que al detectar humo en el aire emite directamente una señal hacia un módulo de control domótico y mediante la programación del sistema se genera una sirena acústica o además se puede enviar mensaje de aviso para que acuda la ayuda necesaria al lugar y no se generen grandes pérdidas.

- Sensor infrarrojo: Se activa cuando se produzca un efecto que oscurezca el espacio que existe entre el emisor y receptor activando inmediatamente la alerta de peligro.

- Sensor puntual: Cuando al tener la presencia del humo y el emisor envié una señal que el receptor no la pueda captar, sino que se refracte de regreso hacia el emisor automáticamente se encenderá la alerta de peligro.

- Sensor iónico: Estos dispositivos emite una radiación alfa, esta pasa por una cámara abierta y el aire encuentra dos electrodos permitiendo una constante corriente eléctrica. Cuando el humo ingresa se reduce el aire y la señal eléctrica es interrumpida motivo por el cual la alarma se activa.

3.4.3.2 Ventajas y desventajas de los sensores.

Tabla 16.

Ventajas y desventajas de uso de sensores.

Ventajas	Desventajas
Simplicidad de diseño	No detectar todos los intentos de ingreso de un intruso
Pequeñas dimensiones	Factor de conversión
Alta confiabilidad en las propiedades de cada sensor	Falsas alarmas
Ofrece estabilidad	Mala sincronización
Conexión con corriente alterna y continua	Rangos limitados de control

3.4.4 Seguridad por Access Point.

Existen diferentes tipos de seguridad que conocemos en el día a día, pero no hemos analizado elementos ya existentes que nos pueden brindar seguridad. En el desarrollo de esta tesis vamos a desarrollar el uso de un access point de

manera que vamos a controlar que equipos se conectan a la red WIFI en horas no autorizadas y se realizará un registro de los equipos no autorizados de manera que se conocerá la presencia de individuos no autorizados en horarios no laborables.

3.4.4.1 ¿Qué es un access point?

Su significado es punto de acceso, trata de un dispositivo el cual emite una señal inalámbrica dentro de una red local con el objetivo de que los usuarios puedan acceder a la conexión mediante equipos inalámbricos sin el uso de cableado sino mediante el uso de ondas de radio que cubren una cierta distancia en específico.

Estas ondas tienen la capacidad de traspasar ciertos obstáculos, pero dependiendo de su grosor la potencia se va debilitando por lo tanto lo más aconsejable es utilizarlos en espacios que tengan línea recta.

Es un dispositivo el cual trabaja en un rango de frecuencia que está dentro de los niveles permitidos para el ser humano y consta de una antena para su correcta transmisión de información y recepción de ondas.

3.4.4.2 Partes de access point.

- Elementos de cubierta: Es la cuida todos los elementos internos y da una buena vista al producto.
- Luces informativas: Informan al usuario en qué estado se encuentra operando el access point.
- Antena: Sirve para emisor y recepción de señal de manera más confiable.
- Conector DC: Permite la conexión eléctrica desde un adaptador AC/DC para que el access point pueda prenderse y trabajar.

- Conector RJ45: Además de permitir una conexión inalámbrica también nos da la opción de conectar equipos por cable para acceso a la red interna.

3.4.4.3 Funcionamiento de un access point.

Los access point puede trabajar en tres formas diferentes mismas que vamos a definir a continuación:

- Modo Router: Es el tipo de acceso en donde varios equipos se conectan a la vez para recibir la misma conexión por un solo equipo. Cuando trabajan en modo ruteador los dispositivos se pueden conectar mediante WIFI o red cableada.

- Modo repetidor: Este tipo de modo funciona con el fin de expandir la señal con buenos niveles de potencia desde el equipo central hacia los limites más extensos en donde el modo ruteador no alcanza mayores distancias que las normales.

- Modo bridge: Es un modo el cual se lo configura como modo puente y sirve para que la conexión pase directa y fluidamente desde un punto al otro sin configuraciones internas.

3.5 Dispositivos que se van a implementar.

Tabla 17.

Motivo de elección de equipos a implementar.

Equipo	Motivo de Elección
Cámara IP Foscam	Acceso remote Acceso por móvil Costo reducido Flexibilidad Facilidad de instalación Envío de imágenes por email Alarmas con envío remoto de datos Uso de grabadores IP

Biométrico MA300 Marca ZKTECO	MA300 es un innovador lector biométrico de huella digital para aplicaciones de control de acceso el cual adopta el avanzado algoritmo patentado por la organización ZK para ofrecer confiabilidad, precisión y rápida velocidad de verificación. Su cubierta metálica y protección IP65 lo hacen resistente al agua, polvo y daños externos.
Modem Fiberhome HG110	El punto de acceso inalámbricos proporciona un rendimiento Wi-Fi excelente y están preparados para servicios de ubicación; se pueden implementar en el modo gestionado por controlador, sin controlador o como AP de acceso remoto, en función del diseño, el alcance y el tamaño de su red inalámbrica

Tabla 18.

Elementos de sistema de seguridad.

DISPOSITIVOS QUE SE IMPLEMENTARAN		
Nombre	**Función / Características**	**Equipo**
Cámara IP Foscam	- Cámara IP integrada con detector de movimiento. - Envió de alerta hacia un email y FTP. - 1280x720 H.264. - Visión de 130 grados. - DDNS gratis. - P2P. - Estándar ONVIF.	

Biométrico MA300 Marca ZKTECO	- Capacidad de 100 huella digitales. - Capacidad de 10000 tarjetas. - Sensor óptico - Comunicación RS485, TCP/IP, USB-Host, Bluetooth. - 1.15 Kg. - 12 V / DC. - Dimensión de 73x148x34.5. - Temperatura de -10ºC a 60ªC.	
Modem Fiberhome HG110	- Acceso interno PPPoE y PPPoA. - Acceso externo PPPoE. - Protocolo 802.1Q y 802.1P. - Servidor DHCP. - NAT y NAPT. - DNS Relay.	
Sensor de movimiento interno.	- 12 V. - Detección 360º. - 5 a 8 GHz. - 1 a 8 m ajustable.	
Cerradura magnética	- Fuerza de retención 150 Kg. - Tensión de alimentación 12 VDC. - Corriente 500 mA. - Temperatura de funcionamiento -10ºC a 55ºC. - Dimensiones del imán 268x42x67 mm. - Peso 4 Kg.	
Botón de salida aluminio	- Dimensión 86x86x20 mm. - Peso 0.25 Kg. - Voltaje 36 VDC. - Botón de metal.	

Batería para biométrico	- Voltaje 12 VDC - Energía 3 A - Epcom Power Line	

3.6 Diseño de sistema de seguridad.

Tabla 19.

Diseño del sistema de seguridad.

DISEÑO SISTEMA DE SEGURIDAD			
Ambiente	**Dispositivo**	**Cantidad**	**Descripción**
Laboratorio 466	Cámara cam360º	1	Controla la entrada y salida de personas de este laboratorio.
Laboratorio 466	Switch	1	Controla la conexión de todos los equipos de la red.
Laboratorio 466	Access Point	1	Controla la conexión de los equipos inalambricos.
Laboratorio 466	Data Center	1	Control de sistema de seguridad.
Laboratorio 466	Página WEB	1	Control gráfico de los sistemas de seguridad
Laboratorio 464	Cámara FOSCAM	1	Controla la entrada y salida de personas.

Laboratorio 466	Cámara FOSCAM	1	Controla la entrada y salida de personas.

3.7 Manuales de configuración de dispositivos a implementar.

A continuación, se explicará cómo se instalaron cada elemento de seguridad de acuerdo con las configuraciones sugeridas por lo fabricantes y las hemos acoplados de acuerdo con nuestras necesidades.

3.7.1 Instalación de cámaras FOSCAM.

a. Ingresar a la página principal de la empresa FOSCAM mediante el link (https://www.foscam.com/downloads/index.html), para descargar software para configuración de cámara.

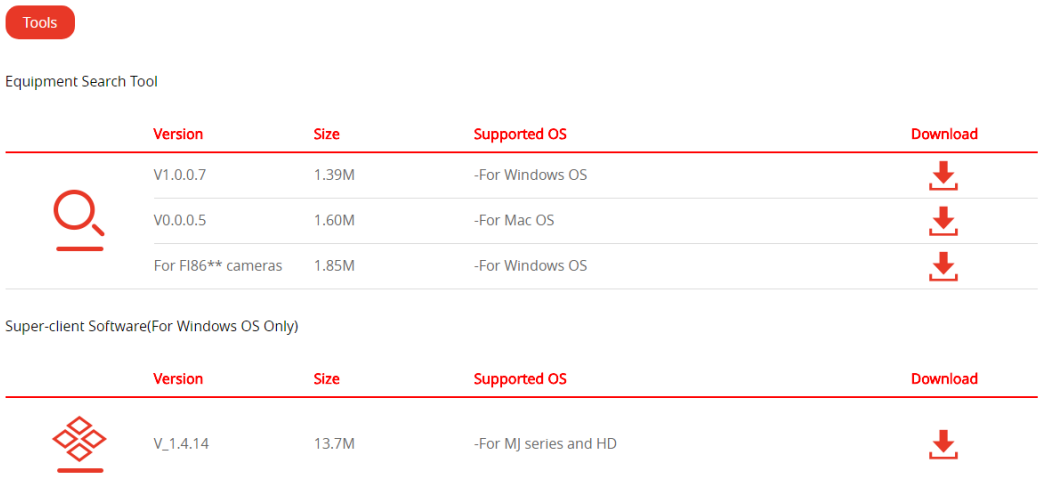


Figura 57. Página Web de cámaras.

b. Descargamos la versión de Windows en donde tendremos la aplicación IPCAMERA.

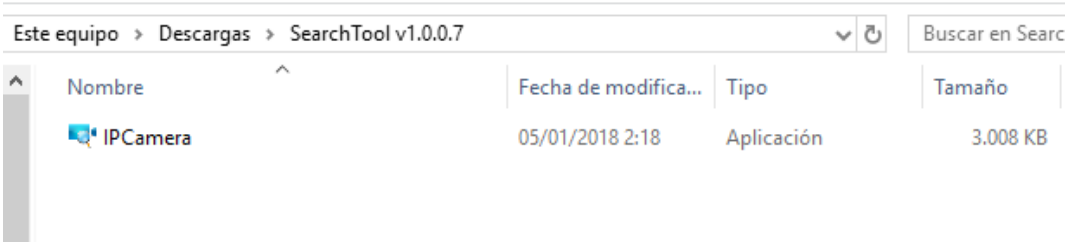


Figura 58. APP de cámara.

c. Ejecutamos como administrador y tendremos que reconocerá inmediatamente a las cámaras.

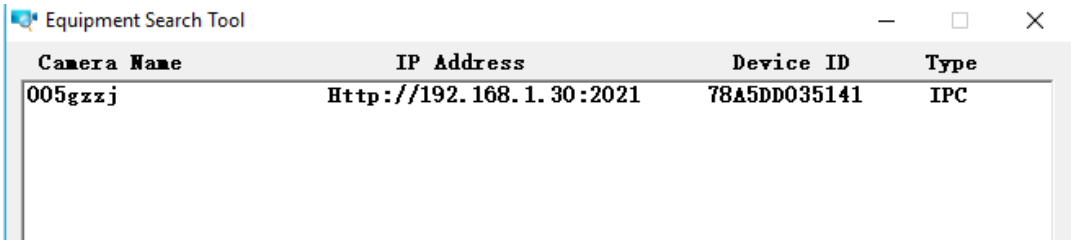


Figura 59. APP Windows de cámara

d. Vemos que vendrá configurada con una IP la cual puede ser editada.

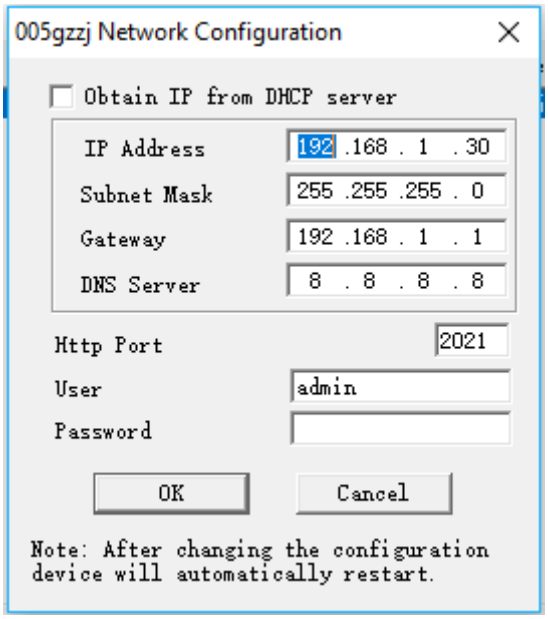


Figura 60. Configuración de IP cámara.

e. Una vez configurada podremos abrirla desde el navegador con la contraseña configurada.

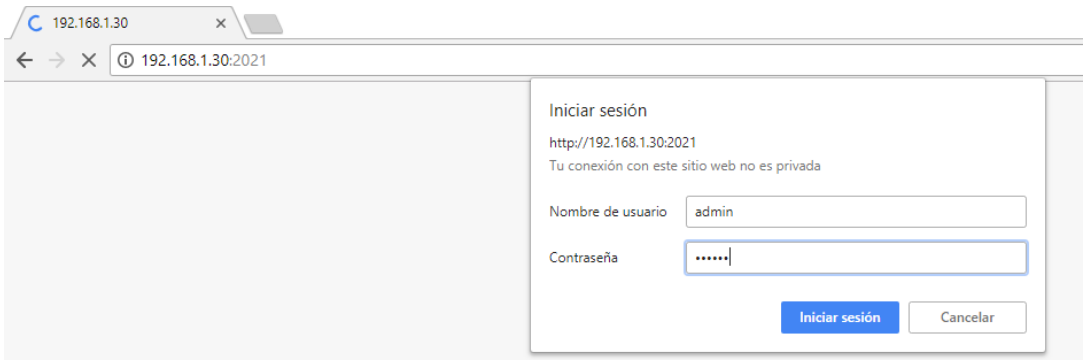


Figura 61. Ingreso configuración de cámara.

f. Ingresado usuario y contraseña tendremos:

Figura 62. Configuración cámara.

g. En la primera Interfaz tendremos la imagen de la cámara en vivo:

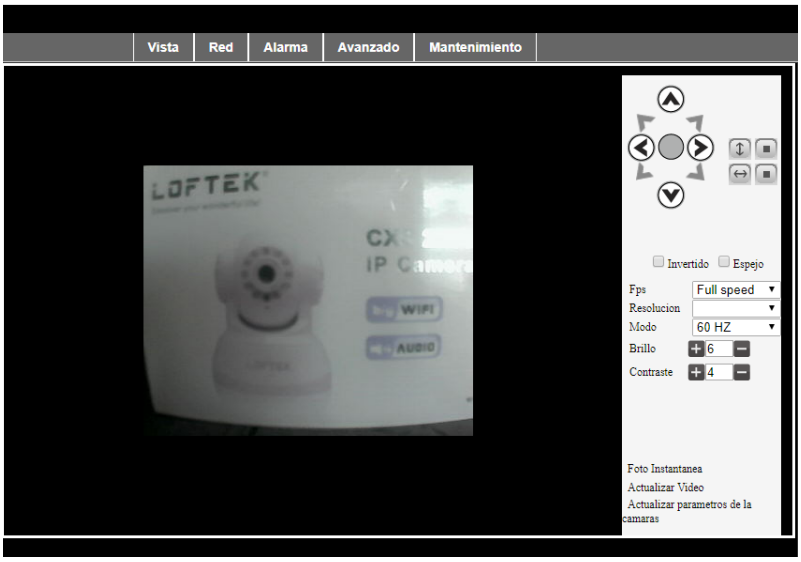


Figura 63. Vista de cámara.

h. En la opción red podremos configurar si deseamos nuevamente la red:

Figura 64. Configuración de red de cámara.

i. Para poder configurar el correo tendremos que activar en la cámara el detector de movimiento en el que podremos configurar la sensibilidad del sensor de movimiento, como se ve en la imagen.

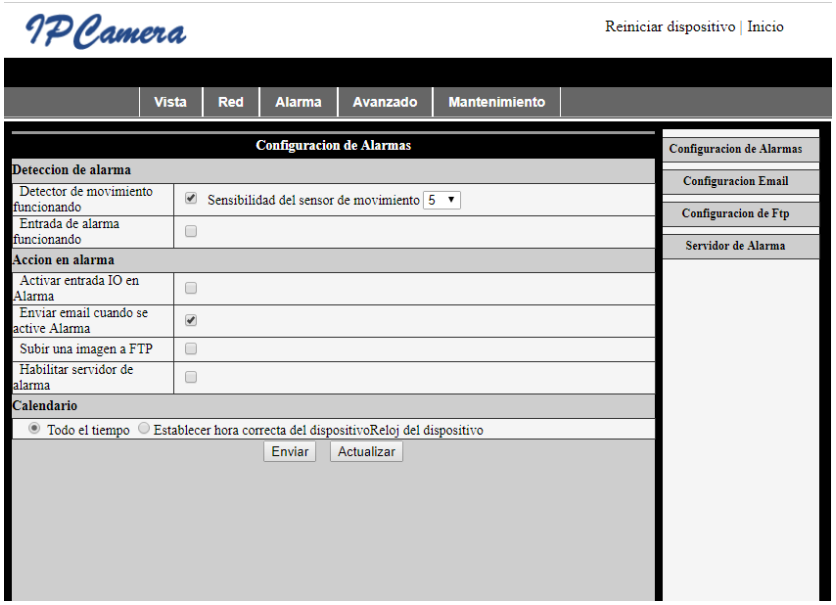


Figura 65. Activación de sensor de movimiento de cámara.

j. En la selección configuración Email tendremos que configurar el usuario que va ser de servidor SMTP de correo en nuestro caso utilizaremos el de Google con el puerto 587. En usuario SMTP ingresaremos una cuenta de correo donde va ser de emisor, y posteriormente va enviar el correo a cuatro receptores con su respectivo remitente.

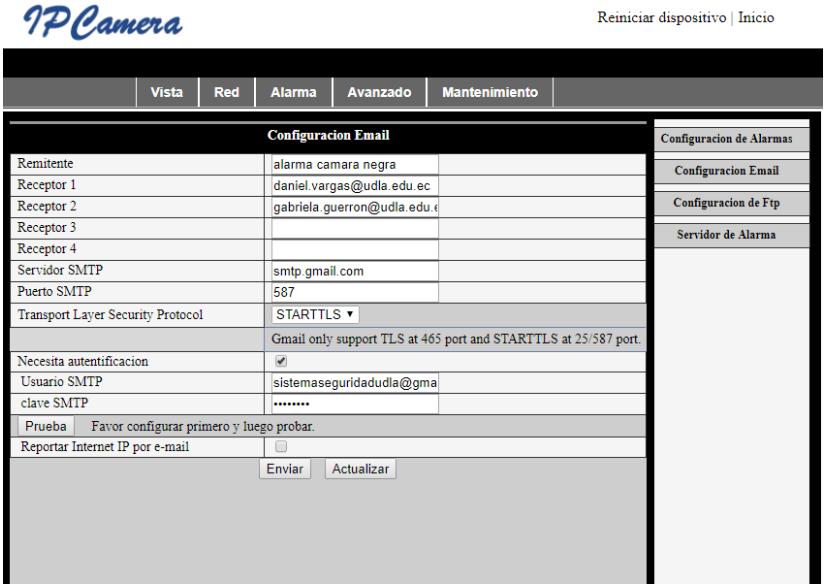


Figura 66. Configuración SMTP de cámara.

k. En la opción de mantenimiento tendremos la información del dispositivo además de configuración como la fecha y hora y para poder resetearlo de fabrica a la cámara IP.

Figura 67. Información de la cámara.

3.8 Instalación de biométrico ZKTECO MA300.

a. Descarga el software que está disponible en la página de https://www.zktecolatinoamerica.com/.

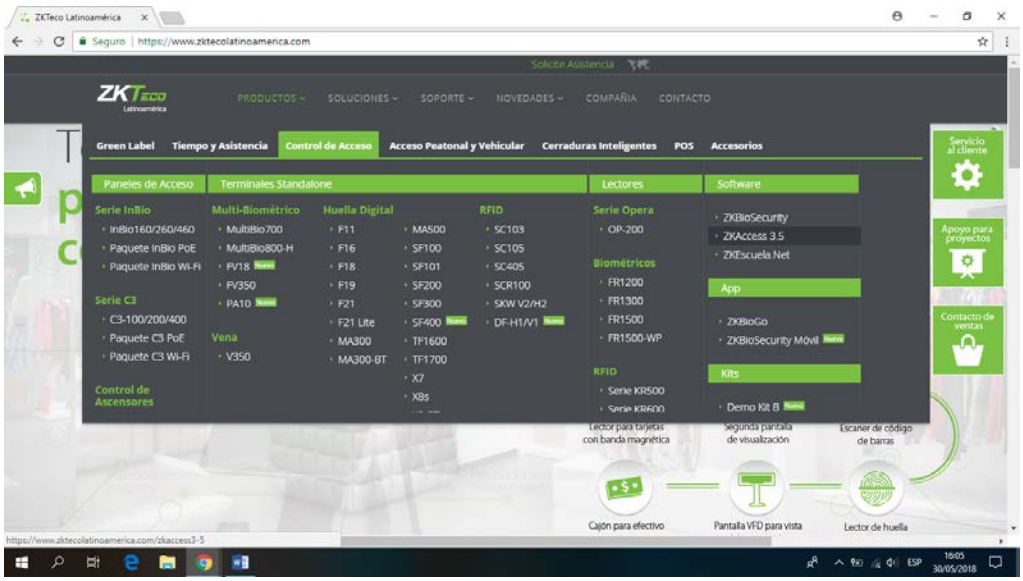


Figura 68. Página principal navegador ZKTeco.

b. Ejecutar el programa.

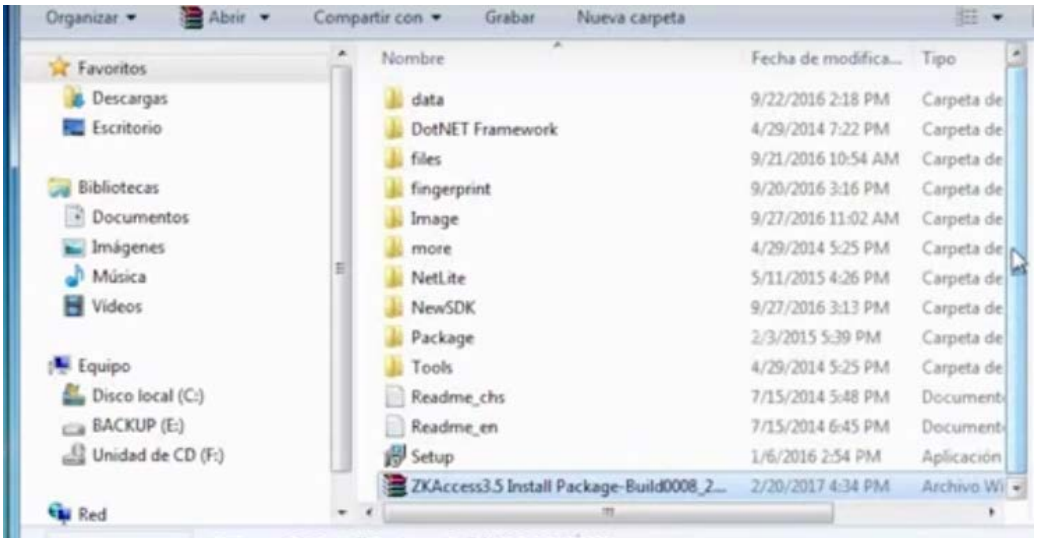


Figura 69. Carpeta de descarga de software.

c. Se puede elegir la base de datos en la que queremos que se lleve el registro.

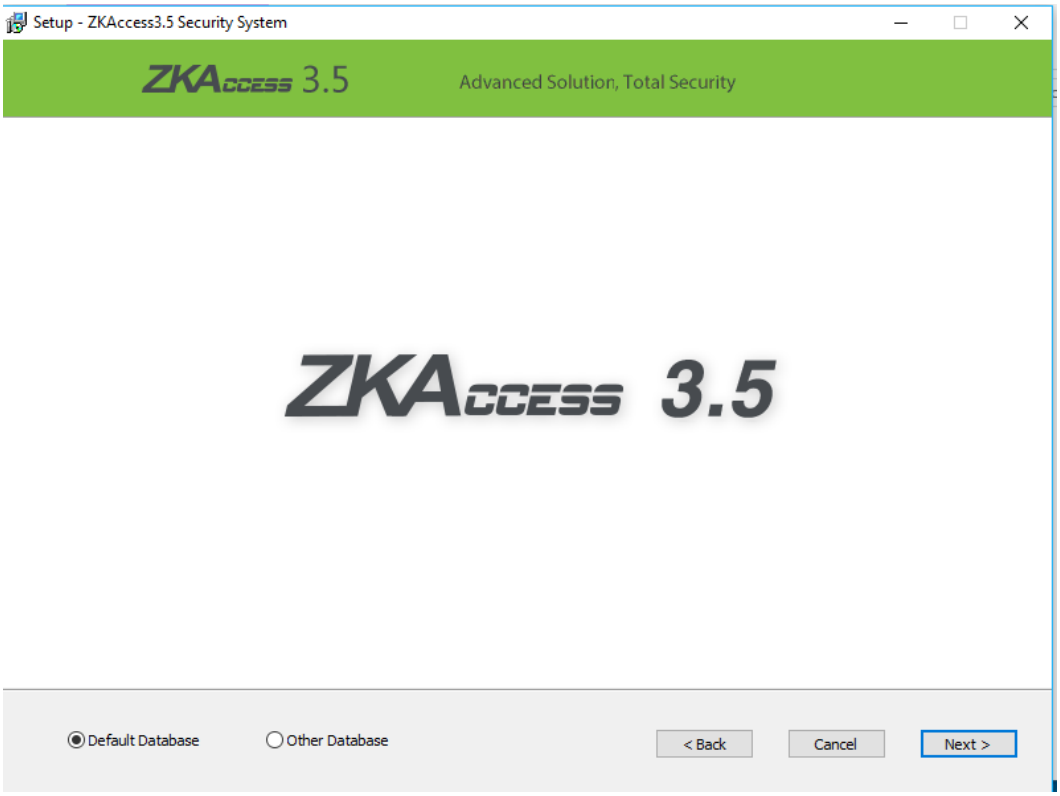


Figura 70. Página principal para la instalación de ZKAccess 3.5

d. Elegimos donde se va a guardar el archivo.

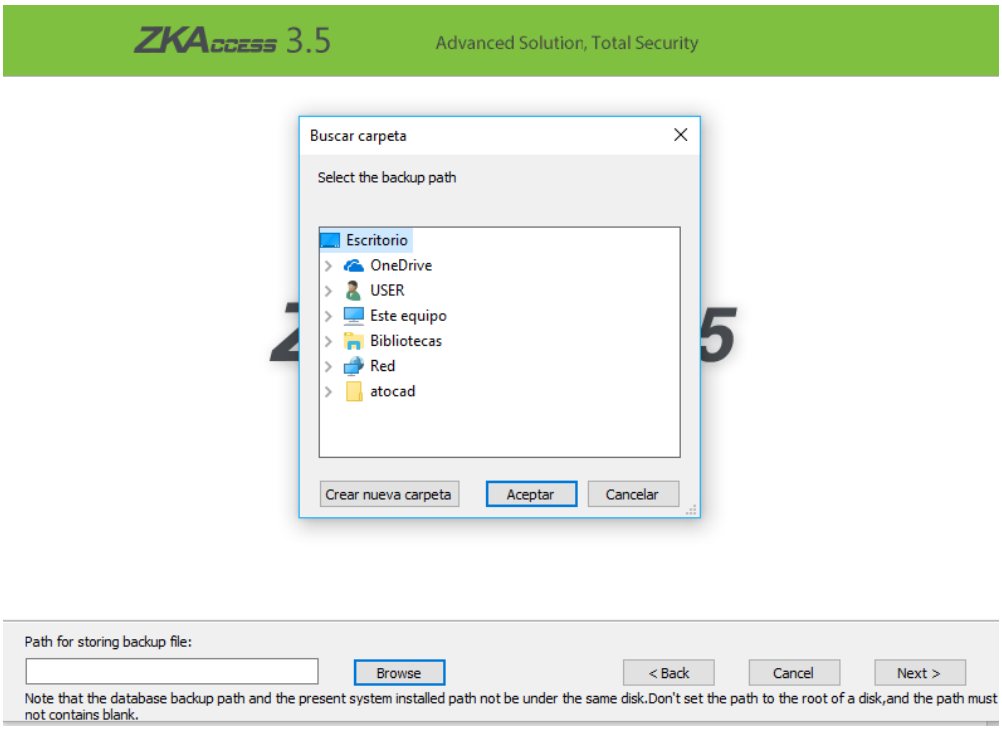


Figura 71. Instalación de ZKAccess 3.5.

e. Procedemos a ingresar al software con el usuario y contraseña “admin”.

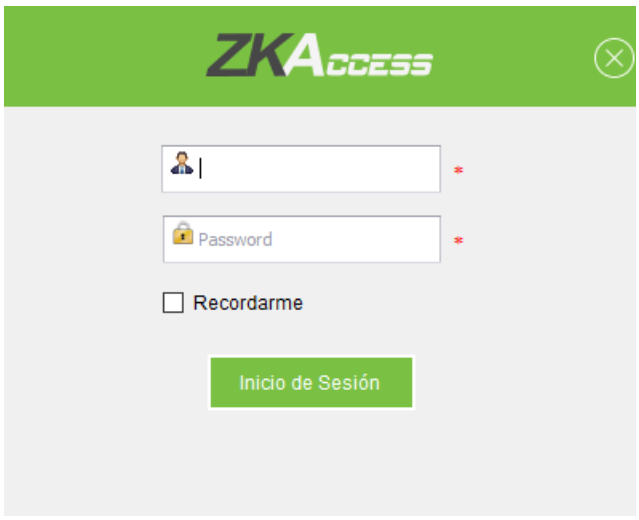


Figura 72. Petición de credenciales para ZKAccess 3.5.

f. Una vez ingresado al software tendremos varias configuraciones como dispositivos, usuarios, departamentos, horarios y reportes.

Figura 73. Software ZKAccess.

g. Configuramos el módulo de asistencia.

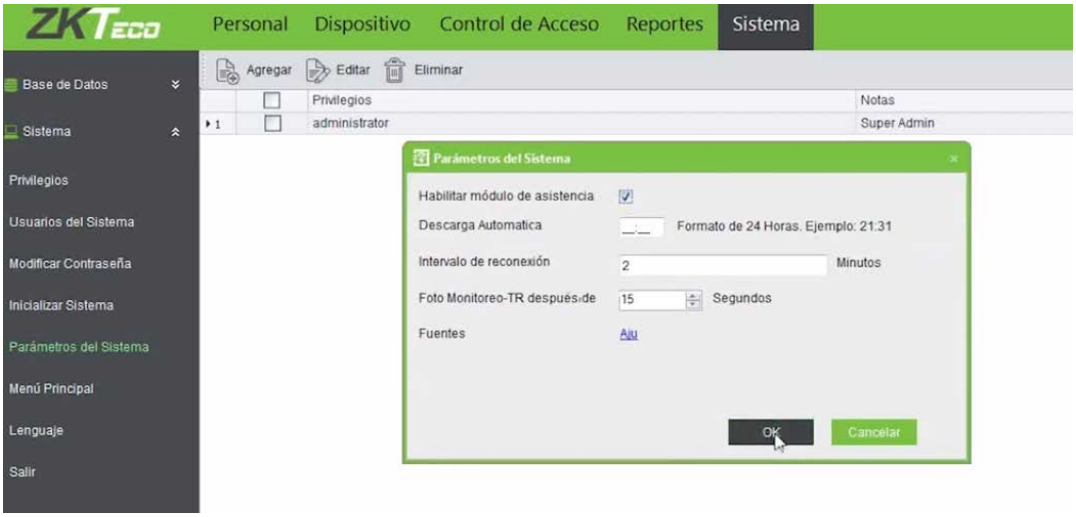


Figura 74. Configuración en parámetros del sistema.

h. Agregamos el o los dispositivos en los que vamos a tener control.

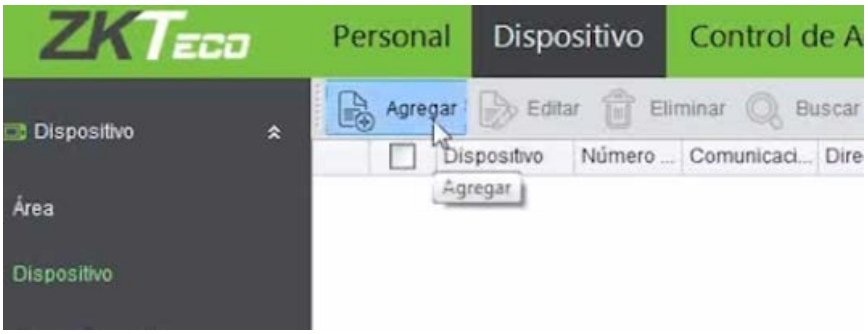


Figura 75. Agregar dispositivo.

i. Configuraremos el modo de comunicación del dispositivo, en nuestro caso utilizaremos IP, con la dirección IP del dispositivo que viene configurado con el equipo.

Figura 76. Configuración parámetros técnicos de biométrico.

j. Escogemos el tipo de dispositivo según lo adquirido que es un control que maneja solo una puerta y es Standalone.

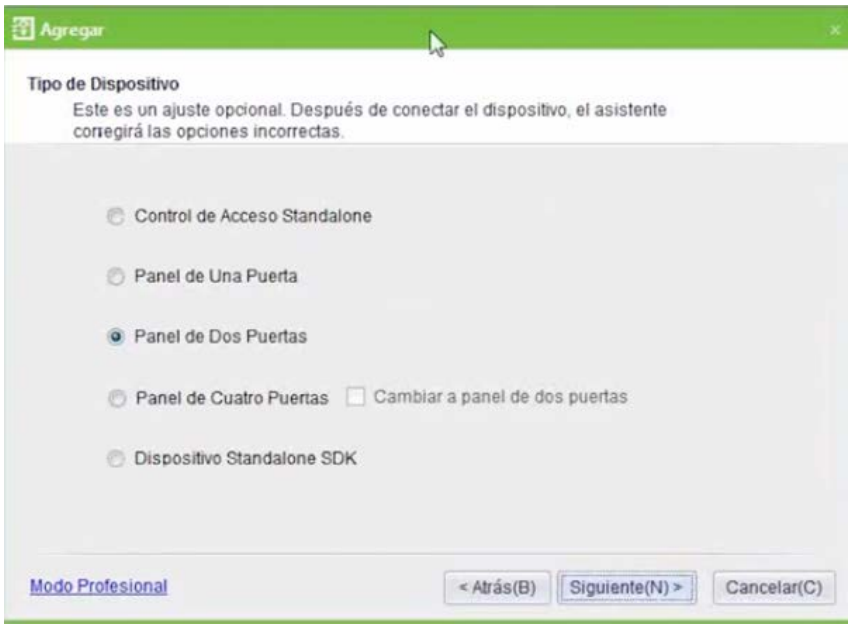


Figura 77. Elección de dispositivos de control.

k. Verificamos que se conectó el dispositivo una vez que se verifica en la celda de habilitado.

Figura 78. Equipo agregado.

l. Descargamos información de usuarios ya almacenados en el biométrico.

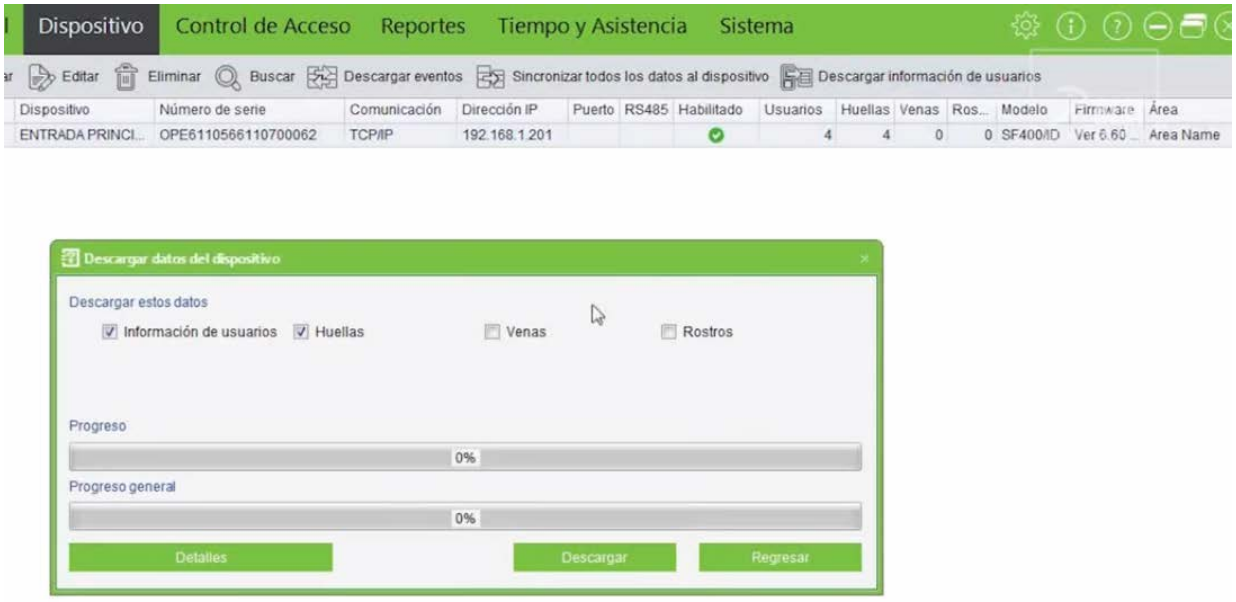


Figura 79. Sincronización del dispositivo.

m. Nos ubicamos en personal y verificamos las personas que están registrada en el biométrico.

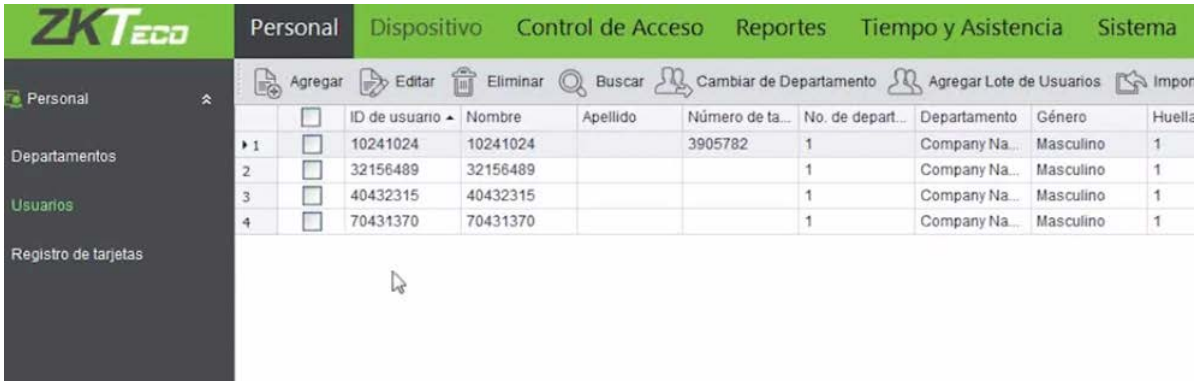


Figura 80. Agregar usuarios al equipo.

n. Podemos editar cada usuario con información personal.

Figura 81. Configuración de usuarios.

o. Además, podemos agregar en categoría a cada usuario por la opción departamentos.

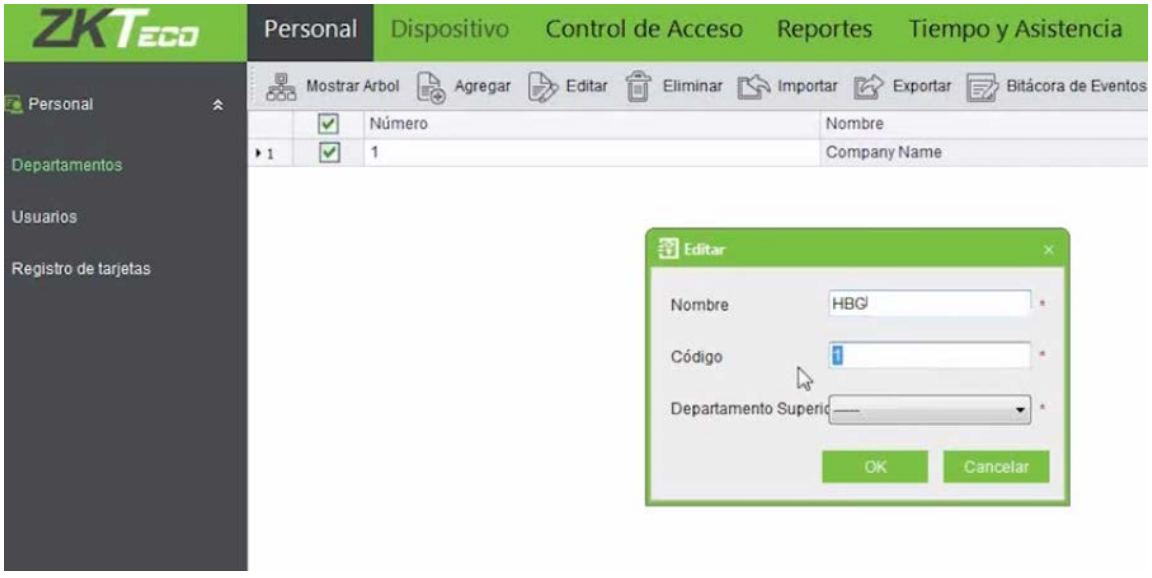


Figura 82. Configuración de departamentos.

p. Agregamos los niveles de acceso para todos los usuarios donde estableceremos reglas.

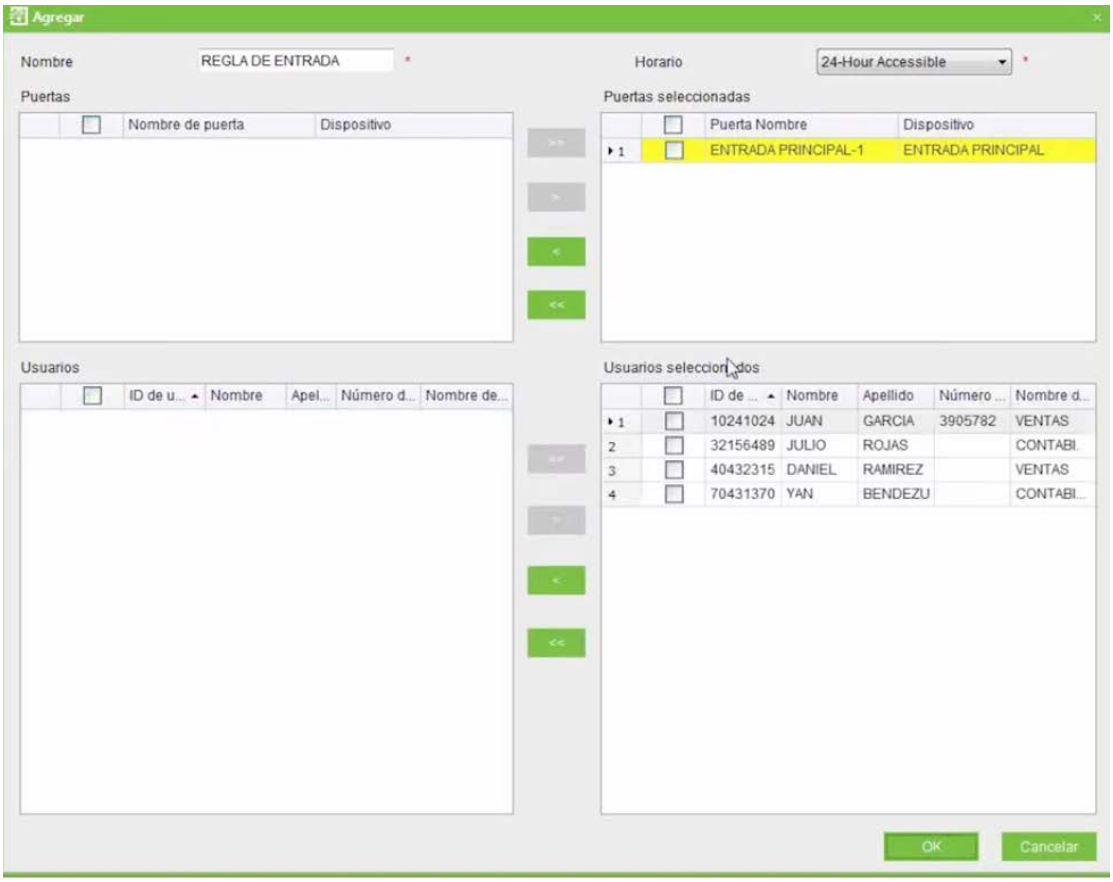


Figura 83. Agregar dispositivos a las puertas de acceso.

q. Después de realizar el paso anterior tendremos la posibilidad de monitorear en tiempo real la entrada de personal.

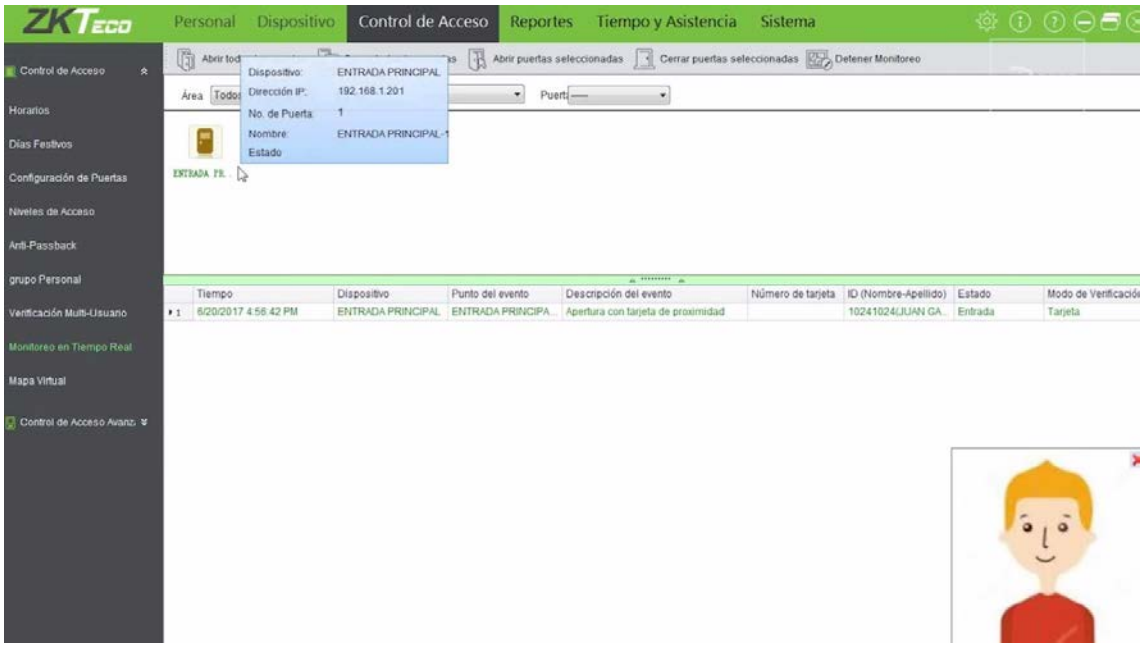


Figura 84. Monitoreo en tiempo real.

r. En la configuración de las puertas tendremos la posibilidad de configurar el tiempo que las puertas estén abiertas además que si pasa ese tiempo nos dé una alarma el dispositivo.

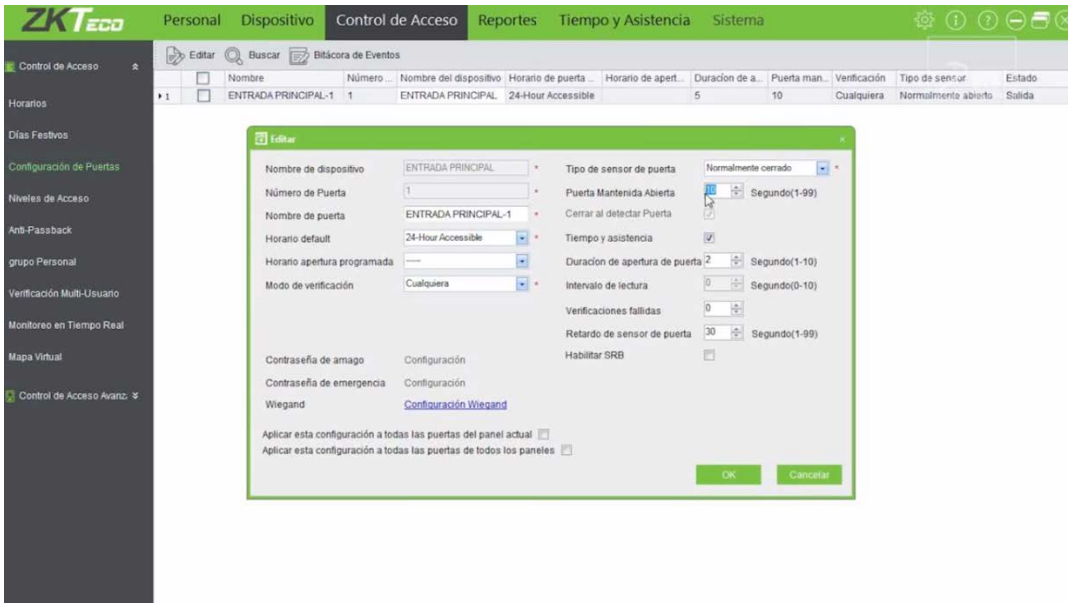


Figura 85. Configuración tiempos de acceso.

s. En la opción del dispositivo podremos realizar las siguientes opciones que se detallan en la siguiente figura 86.

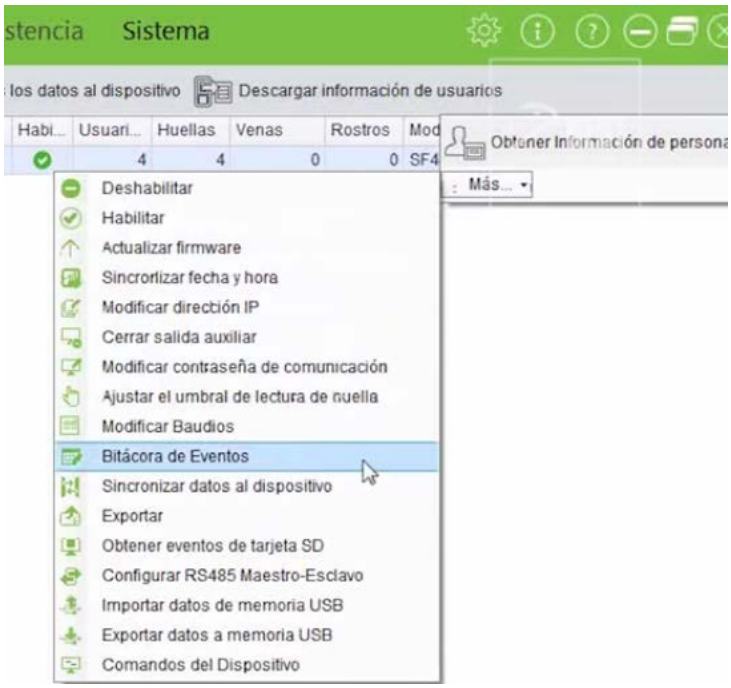


Figura 86. Bitácora de eventos.

3.9 Instalación de access point HG110.

a. Acceso al modem HG110 mediante una página del navegador y en la barra de direcciones se presiona 192.168.1.1. y presionamos el botón configuración avanzada para colocar las credenciales de acceso.

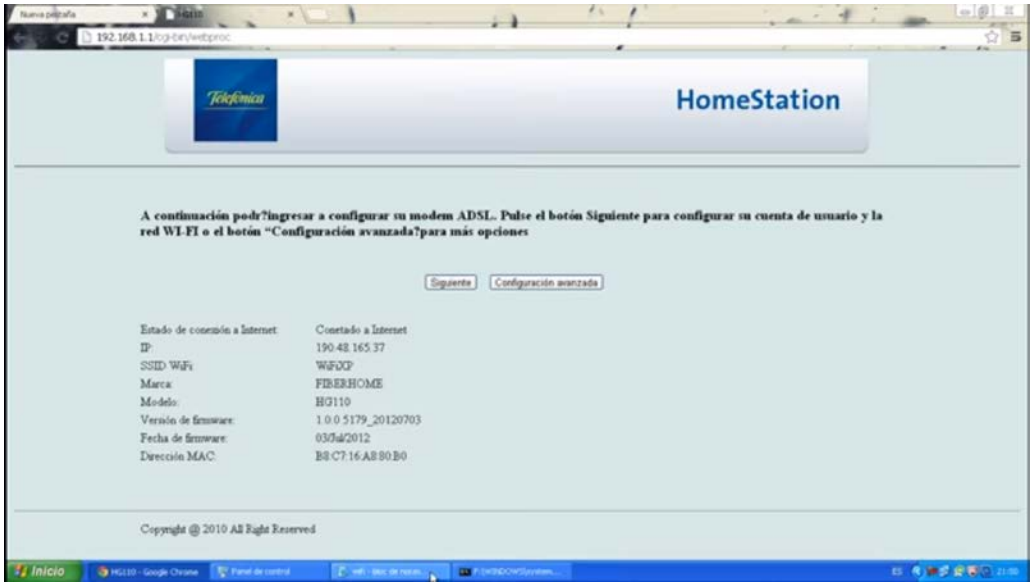


Figura 87. Ingreso a la configuración interna del módem.

b. Ingreso de las contraseñas para acceder al modem. El usuario es: instalador y la contraseña es: cnt2016admin.

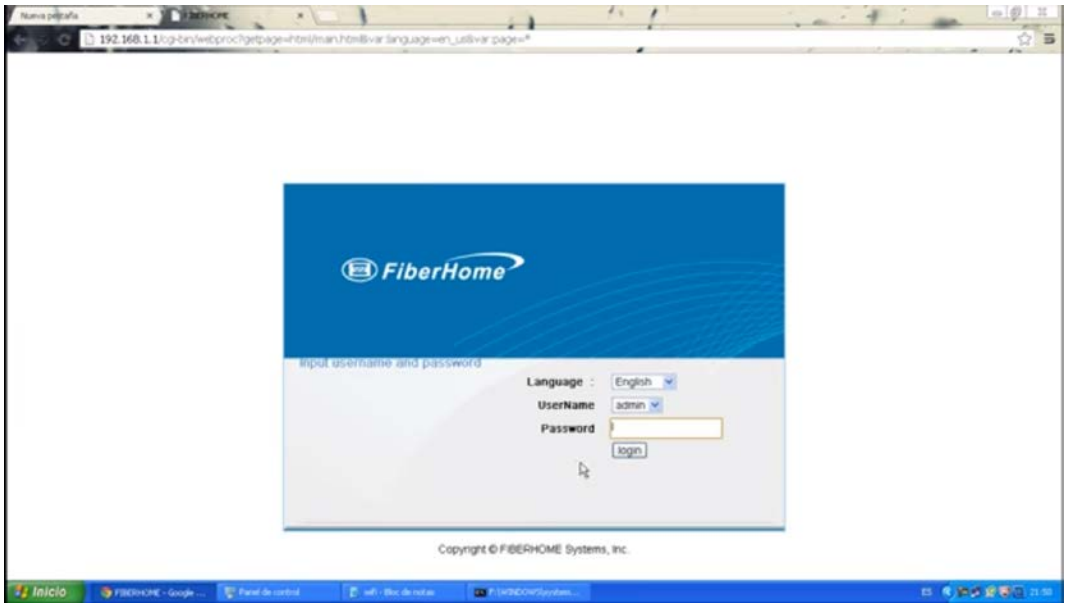


Figura 88. Acceso a credenciales.

c. Seleccionamos la opción Wireless en donde elegimos la opcion Wireless Basic para realizar un cambio en el nombre de la red WIFI.

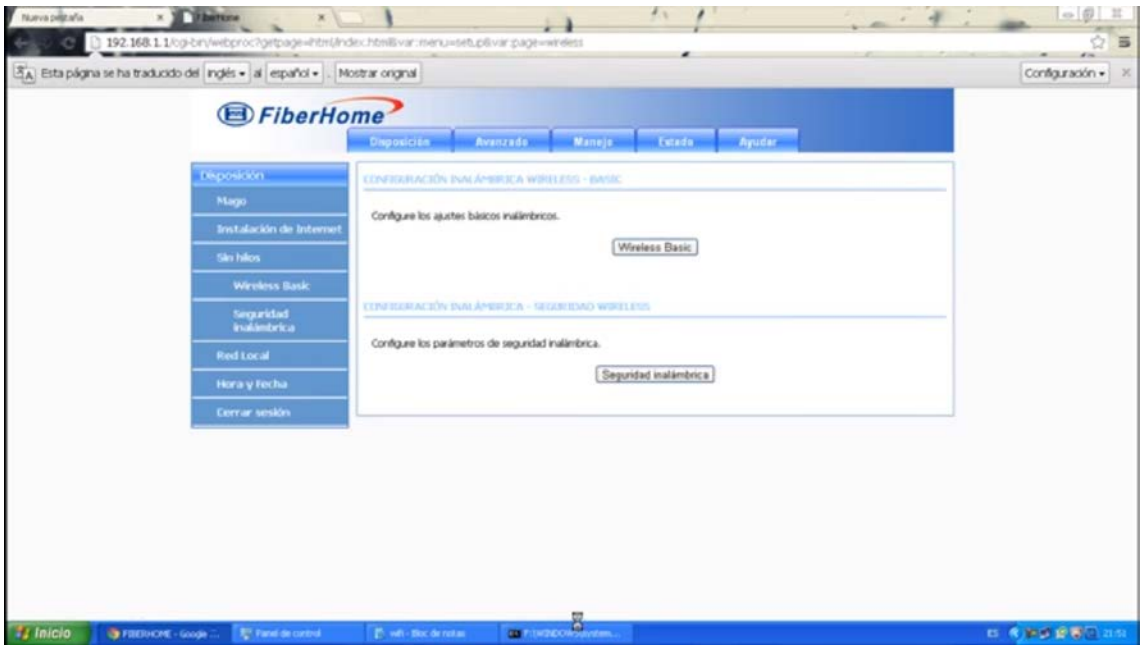


Figura 89. Cambio de nombre de red WIFI.

d. Regresamos a la opción anterior en donde elegimos seguridad inalámbrica y se realiza un cambio de la contraseña de la red WIFI junto con el modo de seguridad.

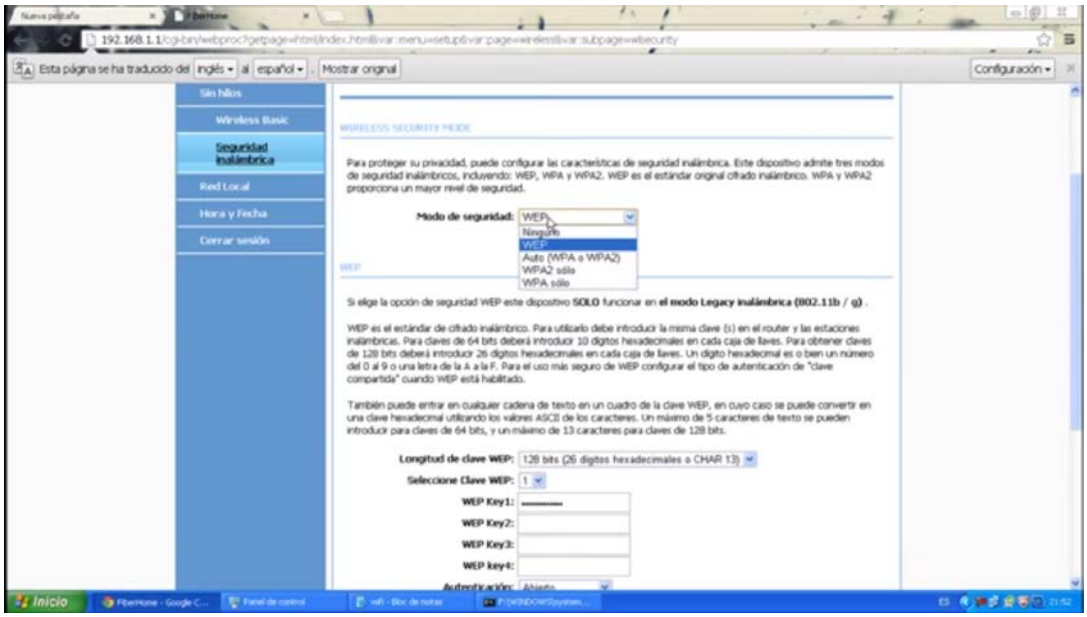


Figura 90. Cambio del modo de seguridad.

e. Se realiza cambio de la contraseña de la red WIFI.

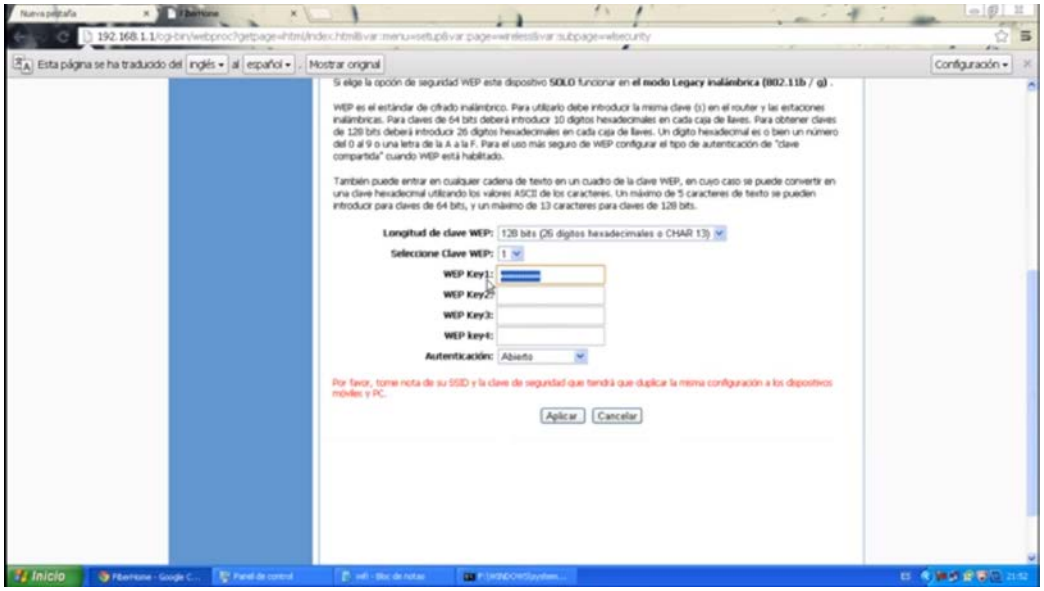


Figura 91. Cambio de la contraseña de la red WIFI.

3.10 Instalación de página Web.

Para poder diseñar la página WEB, elegimos PHP y con esta WampServer que es un entorno de desarrollo web para Windows con el que se puede crear aplicaciones web con Apache, PHP y bases de datos MySQL DataBase.

a. Lo primero que haremos es descargar WampServer.

Figura 92. Página principal para descargar WampServer.

b. Ya descargado lo ejecutamos.

Figura 93. Interfaz de descarga.

c. Aceptamos los términos y condiciones para seguir con la instalación.

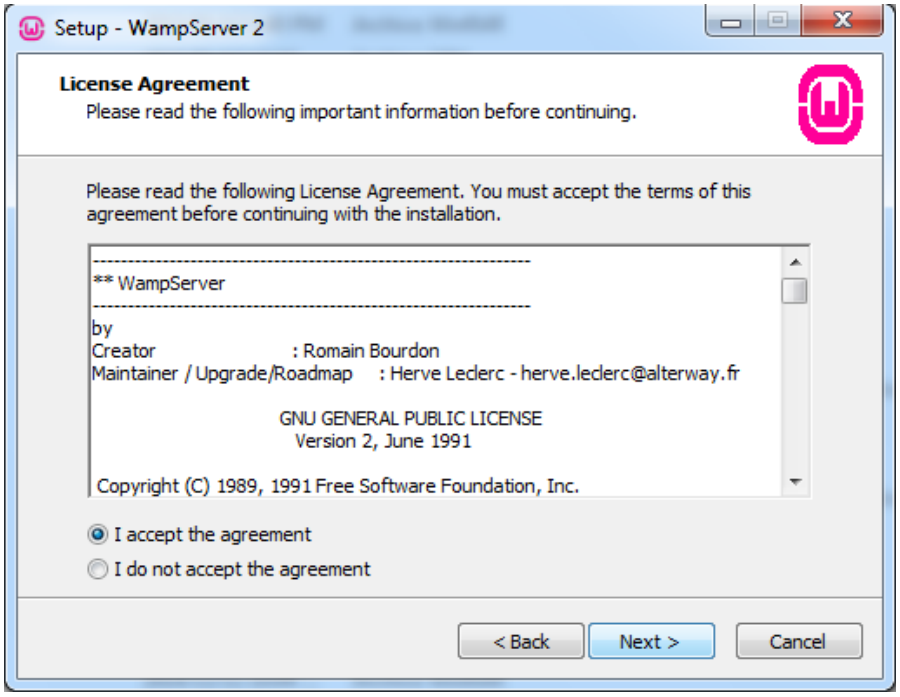


Figura 94. Página para aceptar términos y condiciones.

d. Seleccionamos el destino de instalación, por defecto.

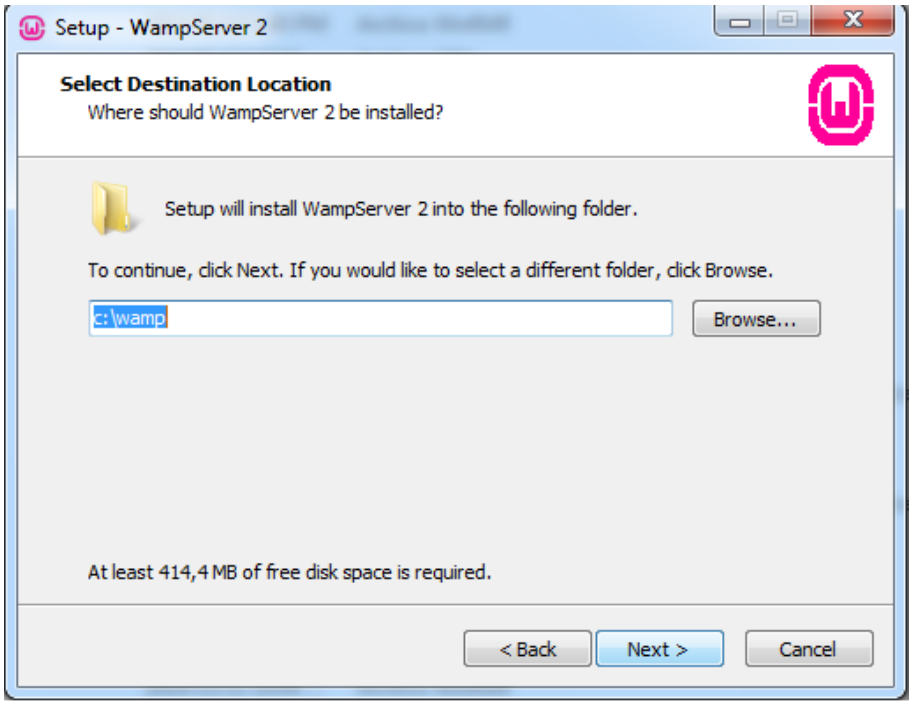


Figura 95. Elegimos la ubicación para instalar WampServer.

e. Si deseamos creamos un acceso directo Selecciona una de las casillas.

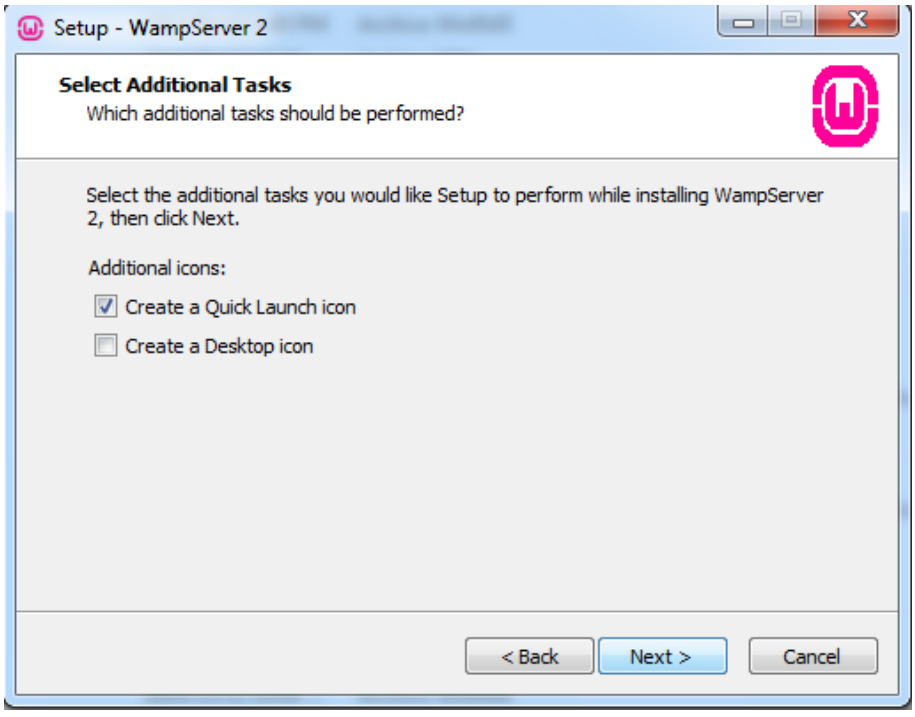


Figura 96. Casillas para crear un icono de escritorio.

f. Procedemos con la instalación.

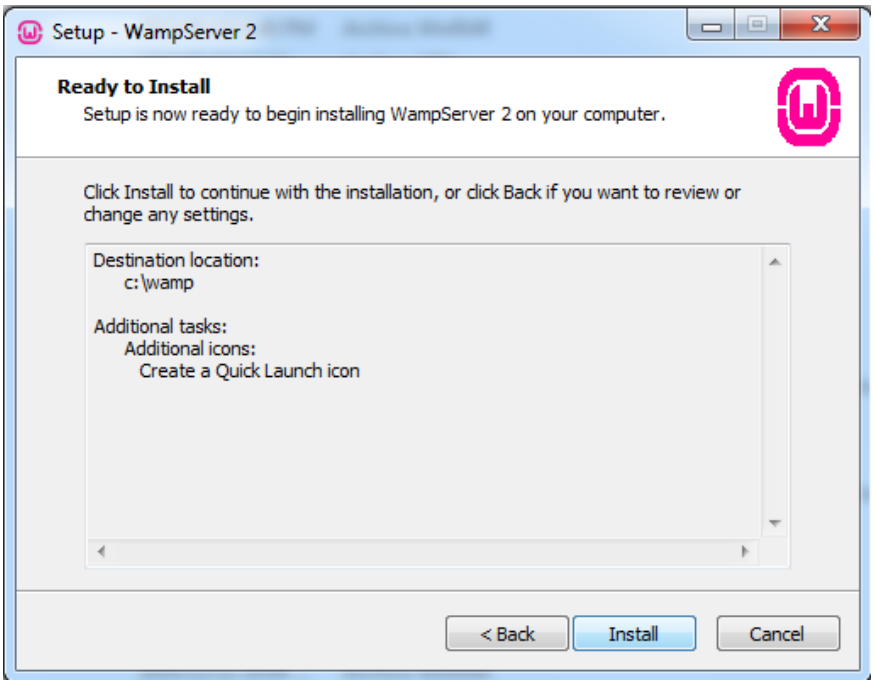


Figura 97. Ejecutamos la instalación.

g. Esperamos que proceda a instalarse.

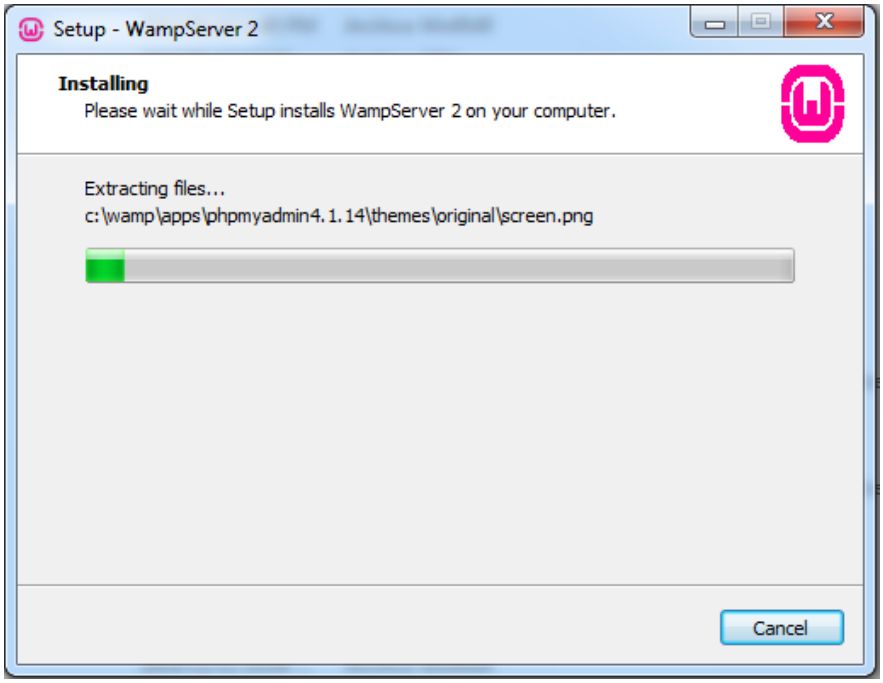


Figura 98. Instalación en ejecución.

h. En esta venta a detectado que tengo instalado Firefox, pregunta si deseamos dejar el navegador como predeterminado de WampServer.

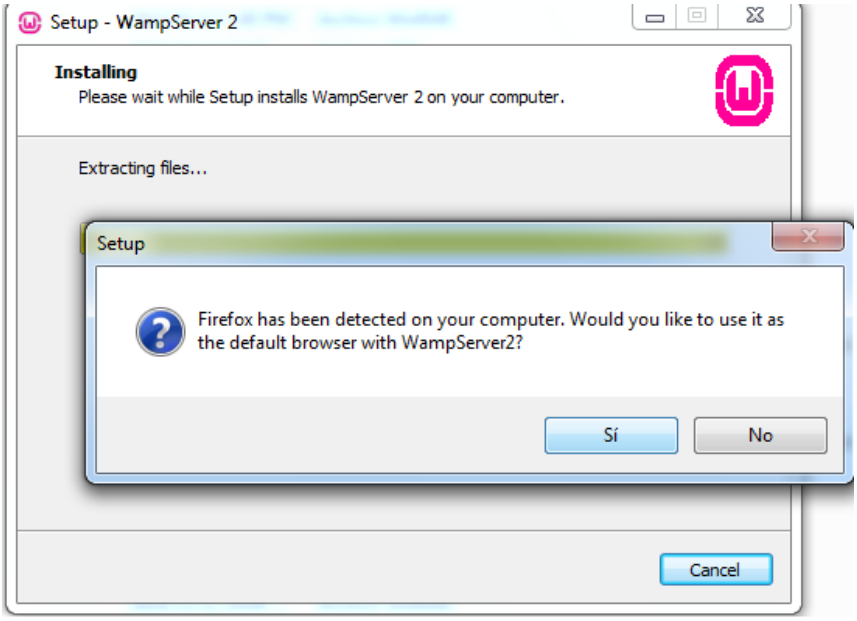


Figura 99. Elegimos que navegador utilizar.

i. En esta opción se nos pregunta si queremos configurar el SMTP, si no le dejamos como nos indica el instalador.

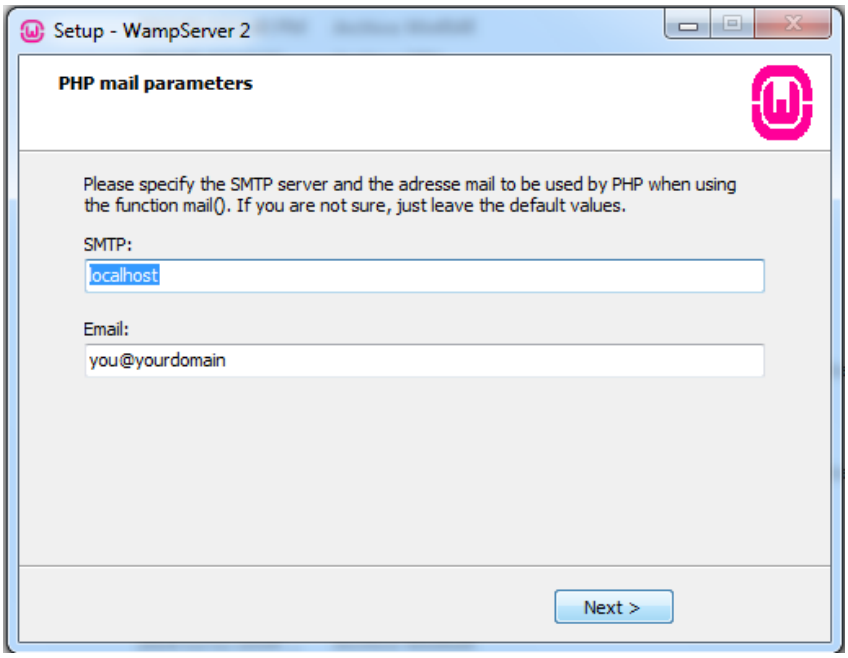


Figura 100. Configuración SMTP.

j. El proceso de instalación ha terminado, si deseas ejecutar la aplicación dejar marcado y dar finalizar.

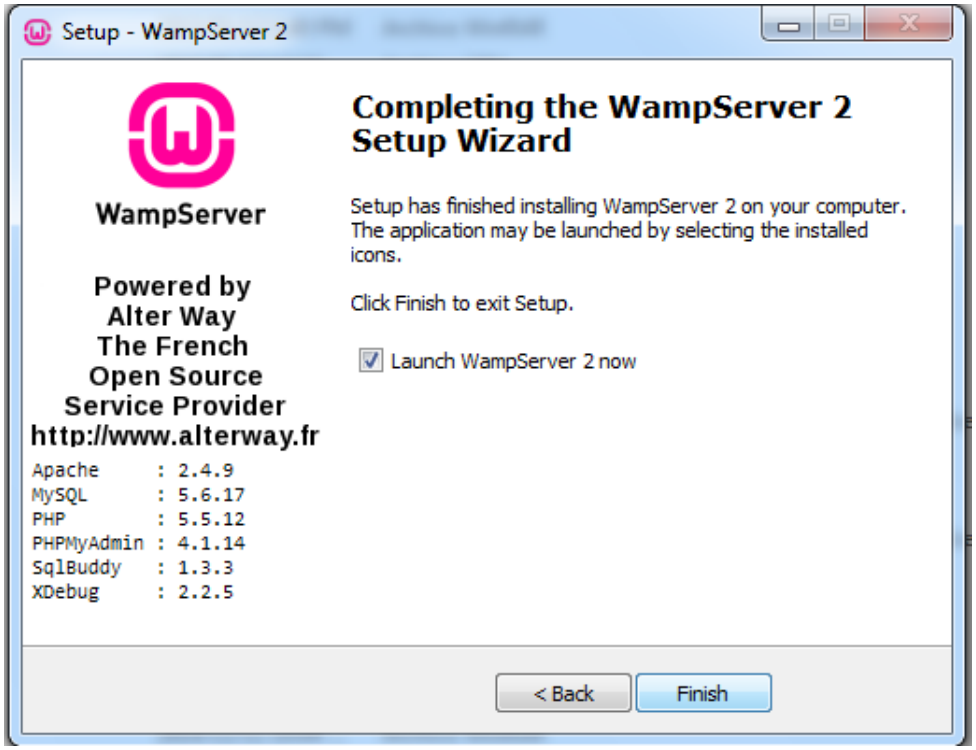


Figura 101. Proceso de instalación finalizado.

i. WampServer se ejecutará en segundo plano en la barra de tareas y se tornará de un color verde.

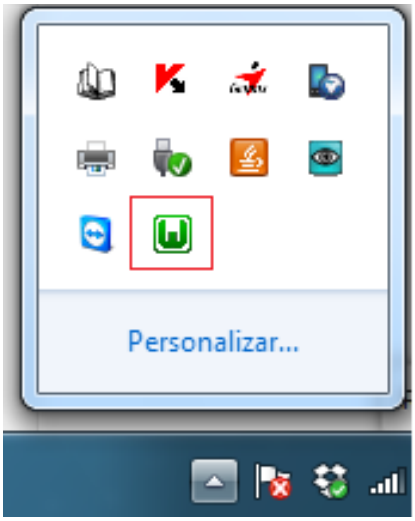


Figura 102. WampServer ejecutándose en segundo plano.

k. Ahora activaremos unos componentes necesarios de PHP, damos clic en el icono verde de WampServer como muestra la imagen arriba, esto desplegara un menú de opciones, seleccionamos PHP, luego Extensiones de PHP y activamos las siguientes con un clic (por cada extensión activada WampServer se reinicia): php_curl, php_imap, php_socket y php_openssl.

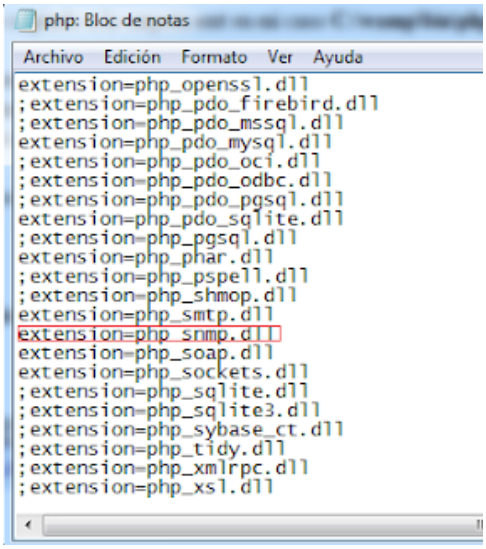


Figura 103. Activar componentes PHP.

l. Guarda los cambios y reiniciar WampServer, clic en el icono verde y reiniciar los servicios, después verificamos que la configuración se realizó correctamente abrimos el navegador, y escribimos "localhost" y obtendremos la pantalla para trabajar con el entorno de desarrollo.

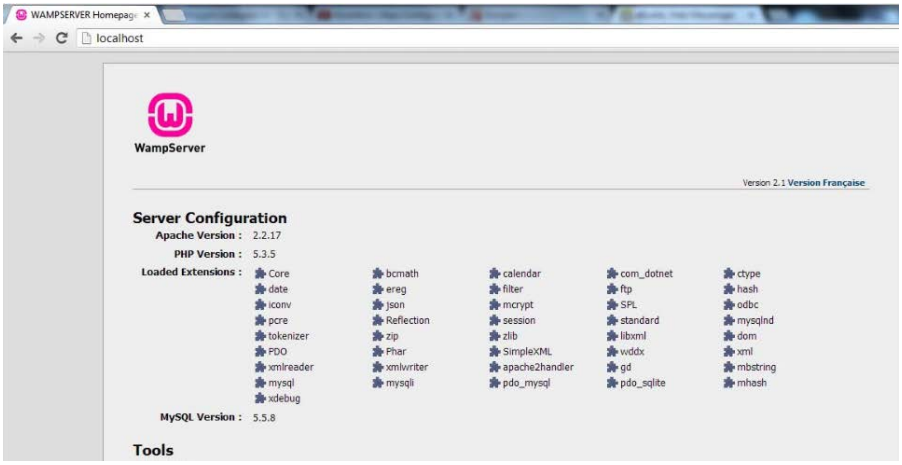


Figura 104. Apertura WampServer.

Después creamos el directorio de proyecto. La carpeta a la que Wamp puede acceder para visualizar las webs en el navegador se ubican en un directorio que se conoce con el nombre de “DocumentRoot”. Por defecto, está en “c:/wamp/www“. Accedemos a este directorio y dentro creamos el directorio del proyecto.

3.11 Diseño de la red de comunicación.

En la universidad, este sistema de seguridad será instalado como un prototipo, de manera que se realizará el direccionamiento según las IP que nos asigne la universidad para pruebas.

3.11.1 Áreas de seguridad.

Como este sistema se lo implementa por seguridad se instala para conexión de varios usuarios, este sistema realiza monitoreos en horarios no laborables de manera que vigile las instalaciones de la universidad.

Tabla 20.
Usuarios posibles para conectarse.

Área	Número de usuarios
Laboratorio 466	10 o más
Laboratorio 464	10 o más
Laboratorio 461	10 o más

3.11.2 Direccionamiento para los equipos de red.

Vamos a definir las IPs con las cuales van a trabajar cada uno de los equipos de la red interna, es decir, cámaras, biométrico, access point y página Web con el fin de tener claro cómo se va a realizar la conexión interna.

Tabla 21.

Direccionamiento de equipos de red.

Equipo	Descripción	IP
Laboratorio 466	Cam360º	10.90.135.107
Laboratorio 466	Página Web	10.170.1.81
Laboratorio 466	Máquina virtual	10.170.1.229
Laboratorio 466	Access point	10.90.135.110
Laboratorio 464	Cámara	10.90.135.105
Laboratorio 461	Sistema biométrico	10.90.135.108
Laboratorio 461	Cámara	10.90.135.106

Figura 105. Diagrama de instalación de los equipos de red.

3.11.2.1 Diseño físico de la red.

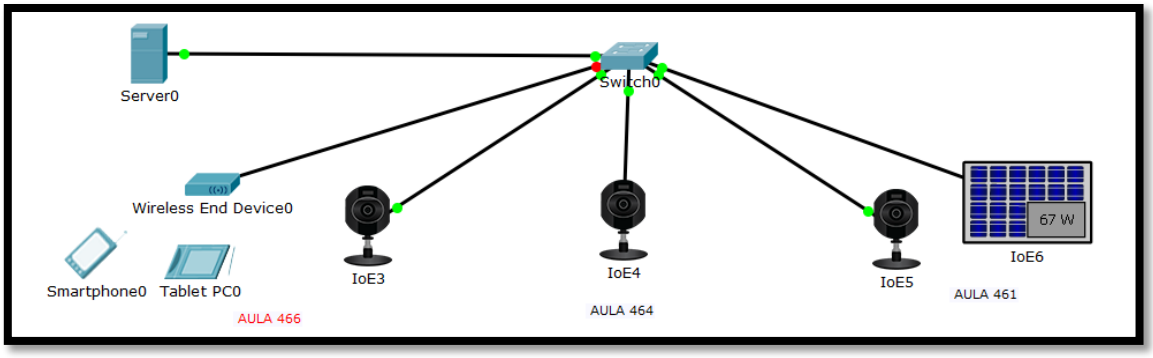


Figura 106. Diseño físico de la red.

3.11.2.2 Diseño lógico de la red.

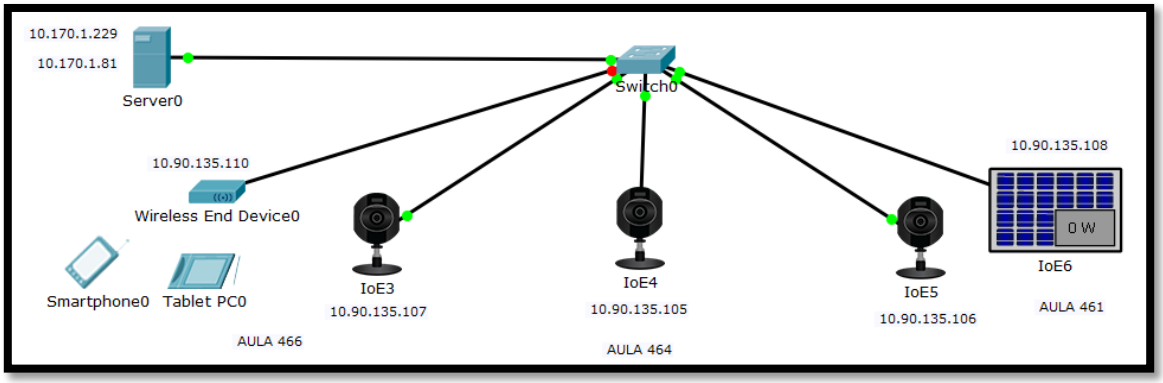


Figura 107. Diseño lógico de la red.

CAPITULO IV. PRUEBAS DEL SISTEMA.

4. Pagina Implementada.

Este capítulo comprende las pruebas que se hicieron ya con la página web alojada en el Data center, y con los equipos ya conectados.

- La siguiente figura 108, comprende la interfaz de login de la página web realizada.

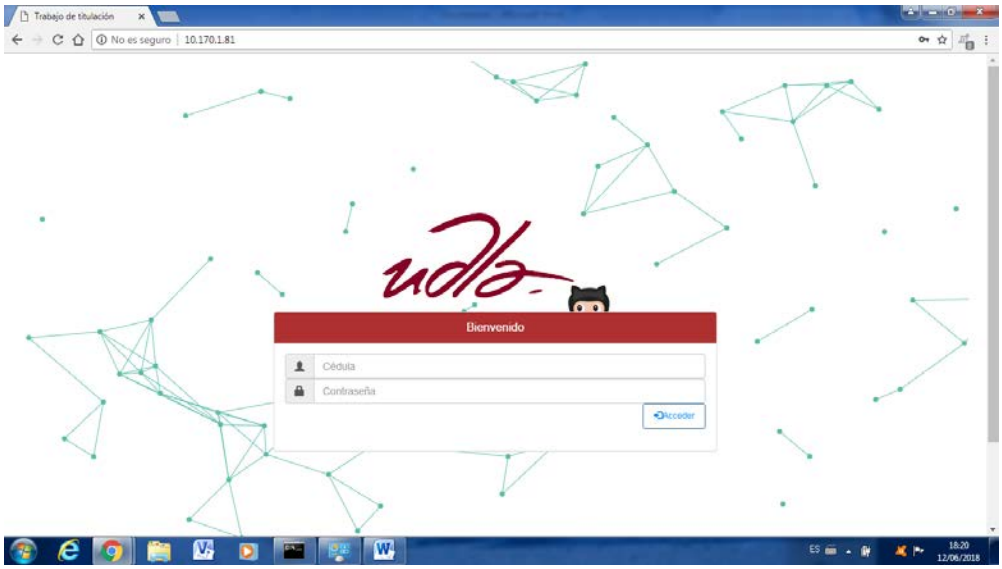


Figura 108. Login página web

- En la siguiente figura 109 verificamos que la contraseña se encuentra encriptada para mayos seguridad.

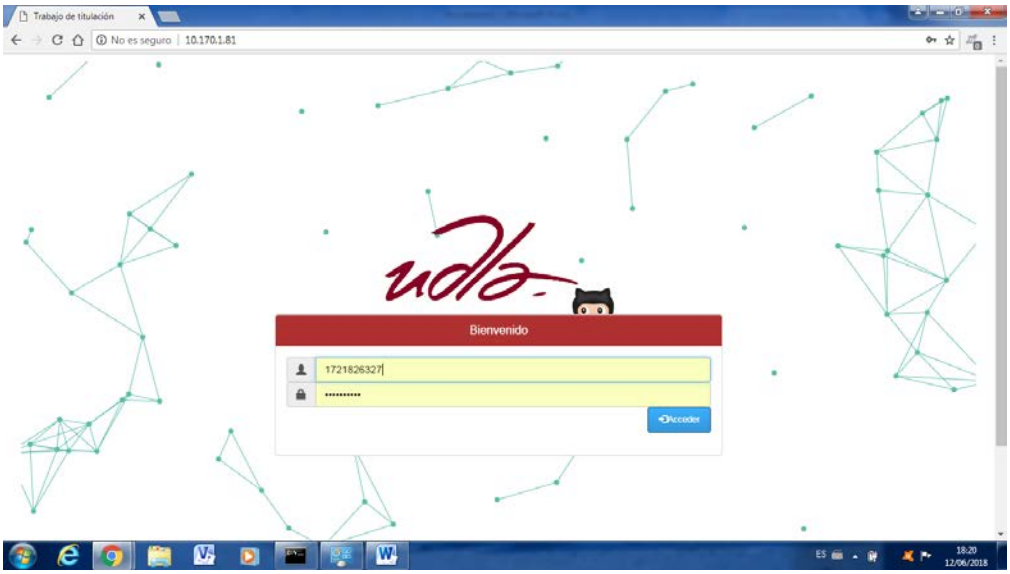


Figura 109. Contraseña encriptada.

- Una vez ingresado con el usuario root, verificamos que se pueden crear usuarios para ingresar a la página dependiendo los permisos, además que en la figura 110, se divisa la interfaz con todas las opciones.

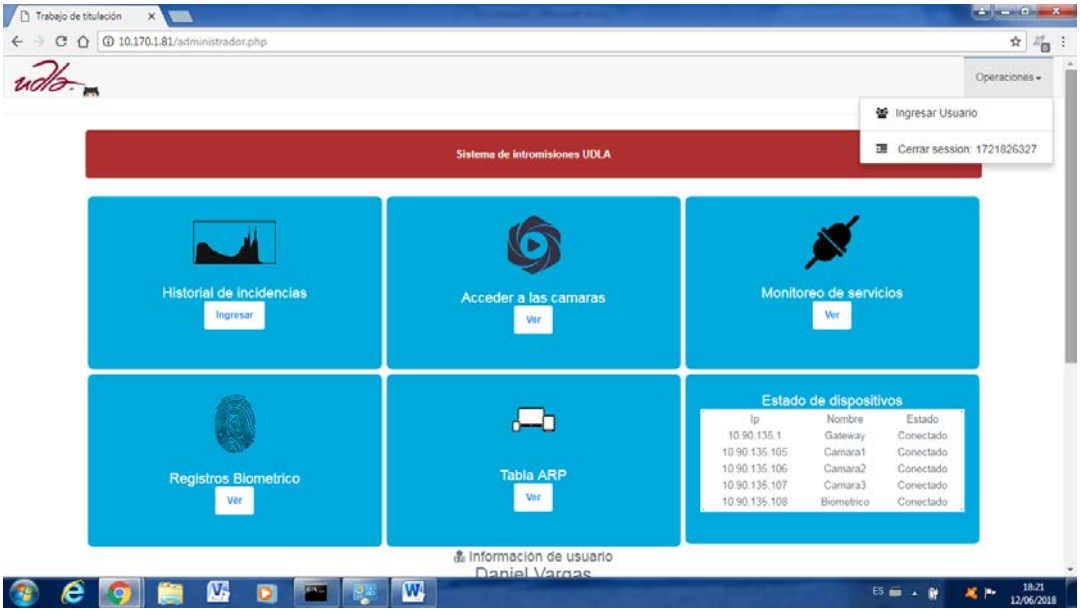


Figura 110. Interfaz de la página web.

- Si el usuario root (Administrador) ingresa a la opción de “ingresar usuarios”, verificamos que se despliega el formulario de usuarios.

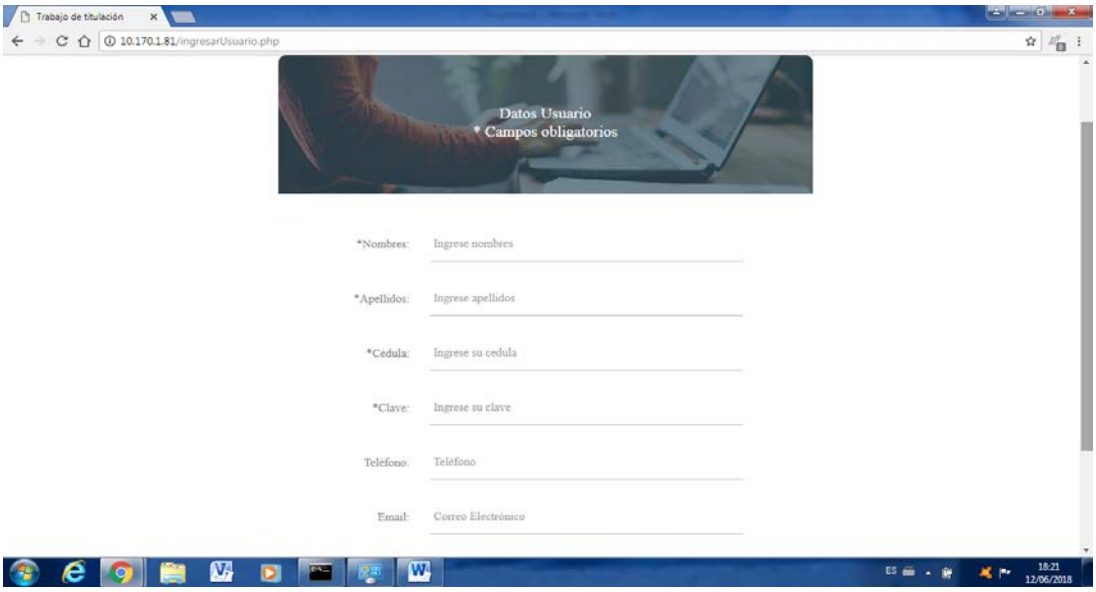


Figura 111. Formulario de usuarios.

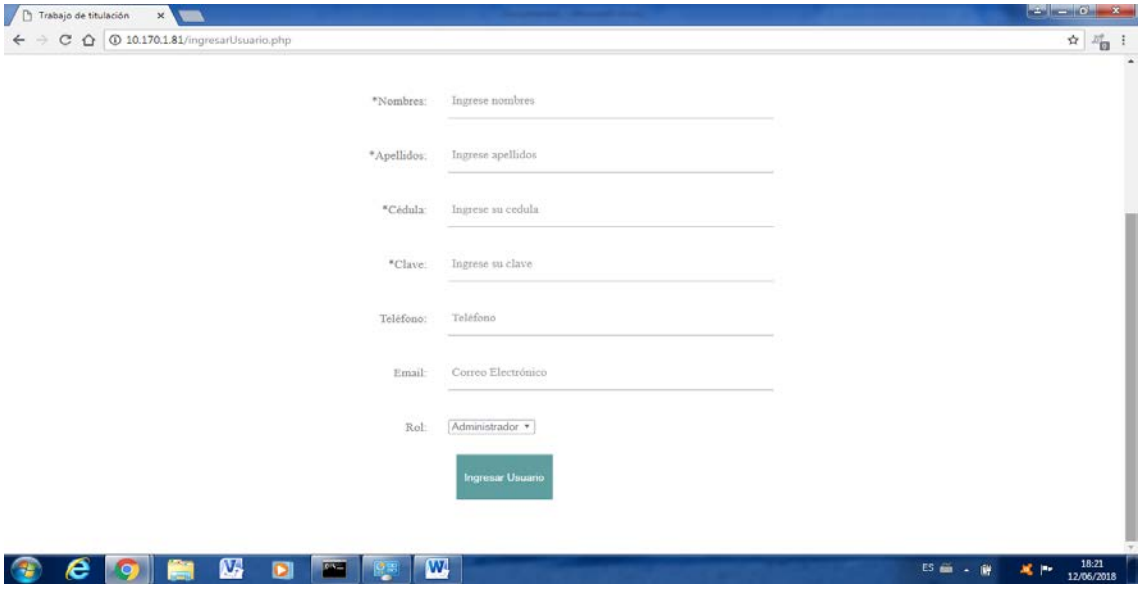


Figura 112. Formulario de usuarios con todos los campos.

- Comenzamos con la primera opción de registro de incidencias, donde nos indica si las cámaras detectaron algún movimiento y se censa en la siguiente figura 113.

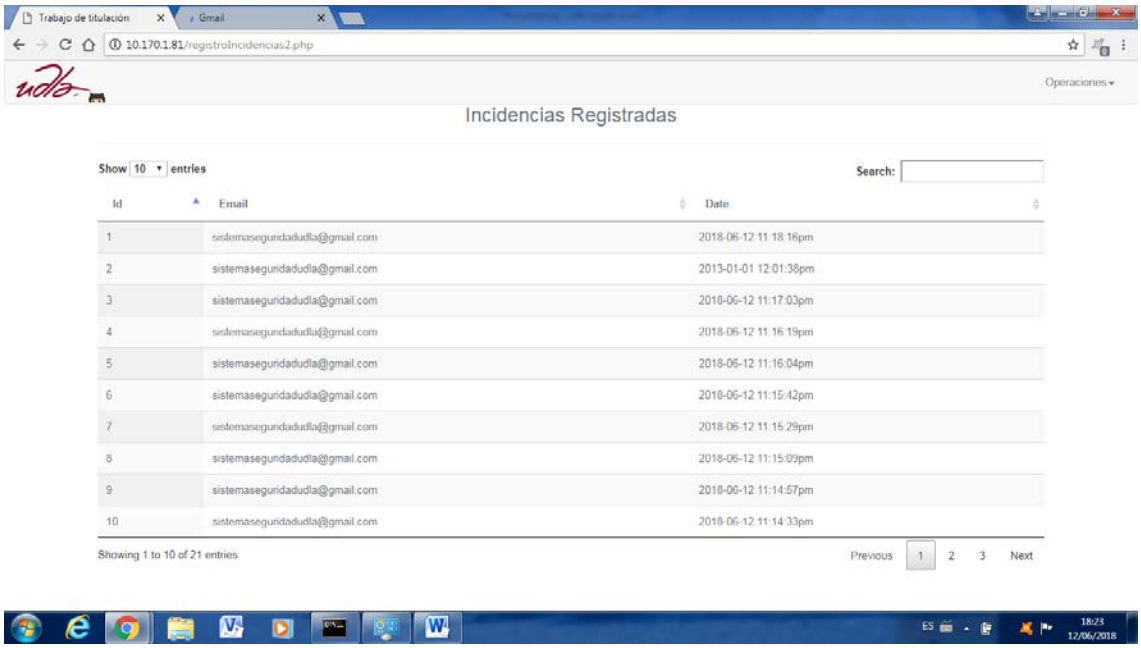


Figura 113. Registro de Incidencias.

- En la siguiente figura 114 verificamos el correo del administrador, donde también se pueden verificar las cámaras si detectaron el movimiento.

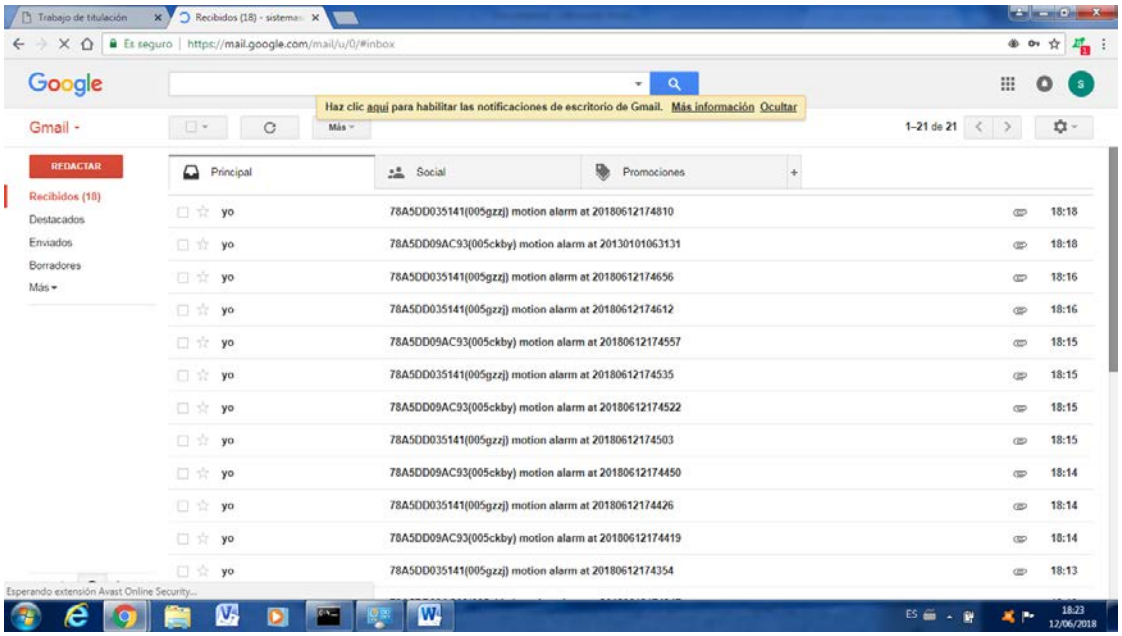


Figura 114. Correo de alertas de las cámaras.

- En la siguiente captura se puede verificar la alerta de movimiento que detecto desde el correo.

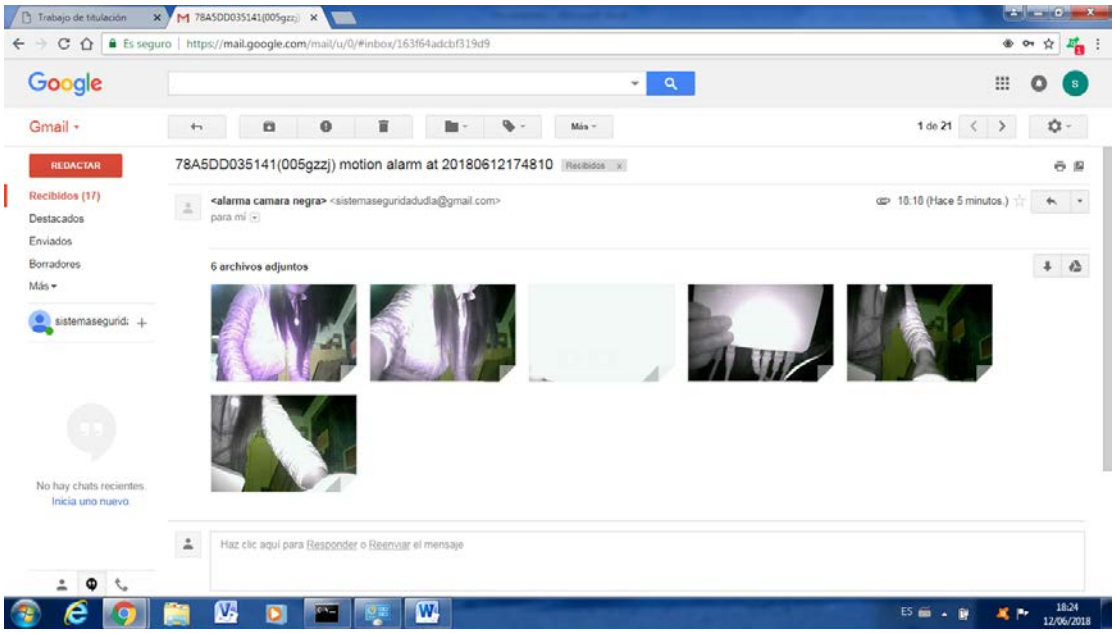


Figura 115. Correo con imágenes de las cámaras.

- En la siguiente figura 116 tenemos la pestaña de las cámaras, donde dando clic en las pestañas podemos ingresar a cada una de las cámaras detectadas.

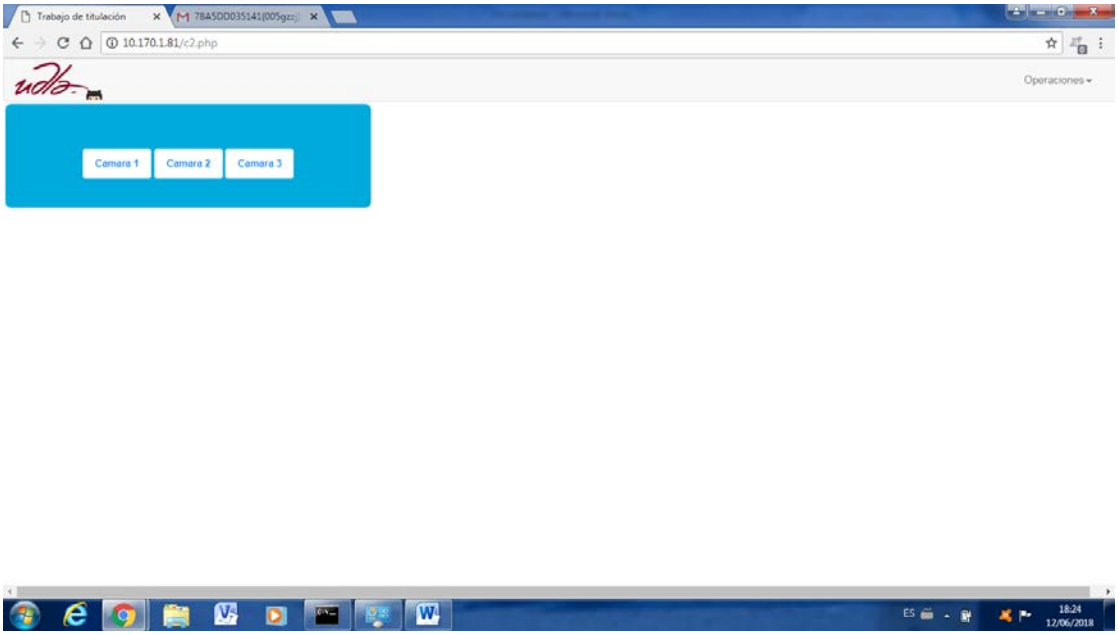


Figura 116. Estatus cámaras.

- Cámara 1.

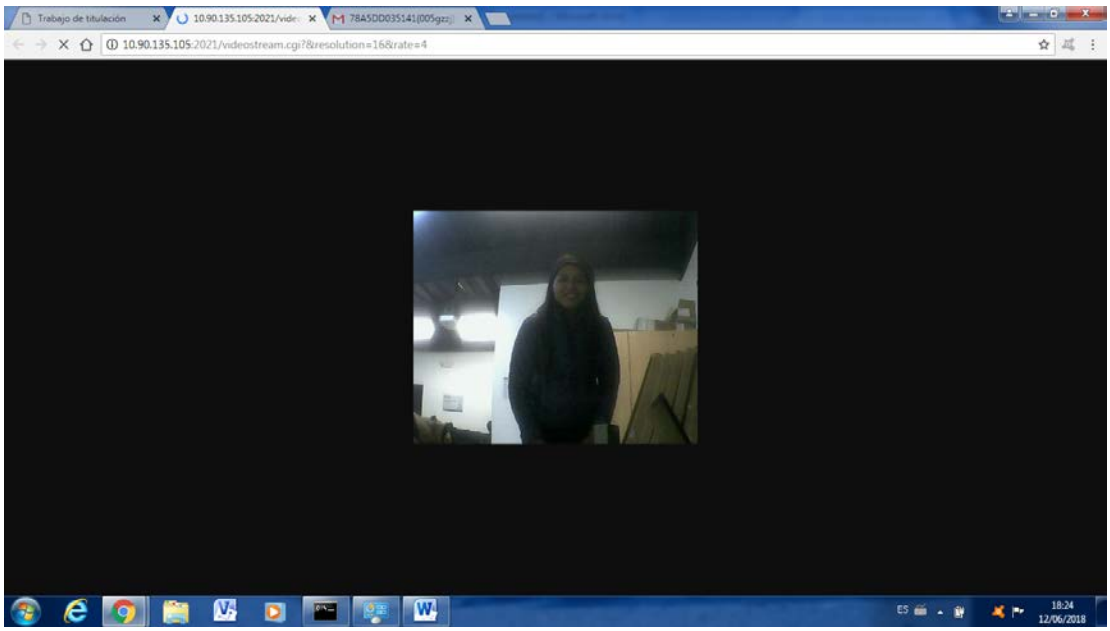


Figura 117. Figura cámara 1

- Cámara 2.

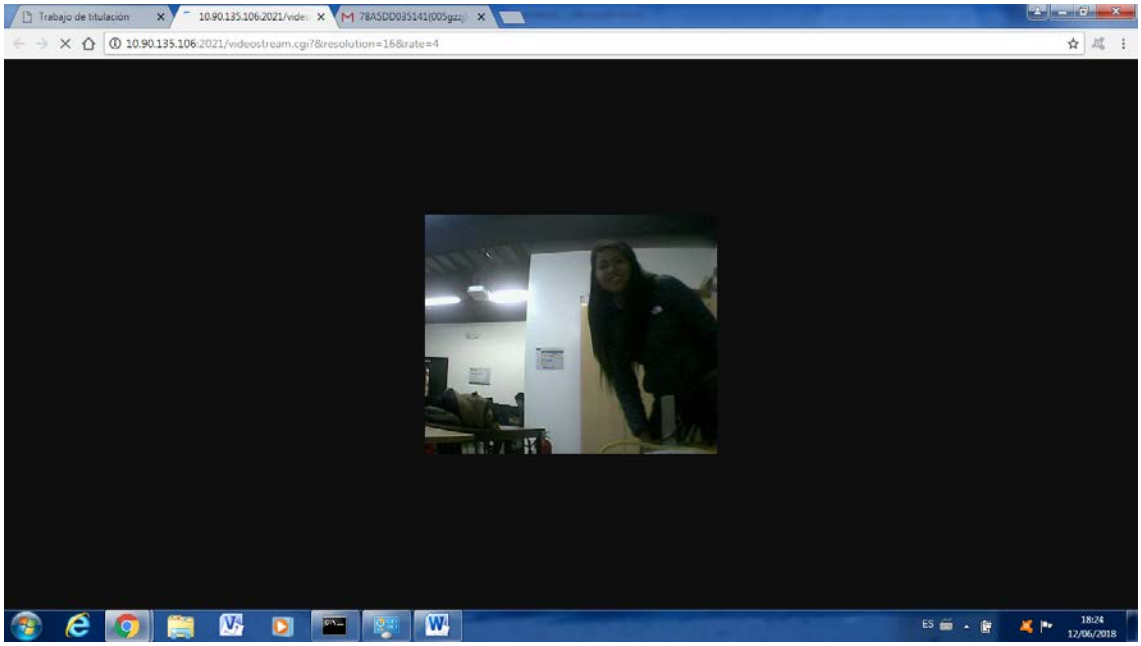


Figura 118. Cámara 2.

- Cámara 3.

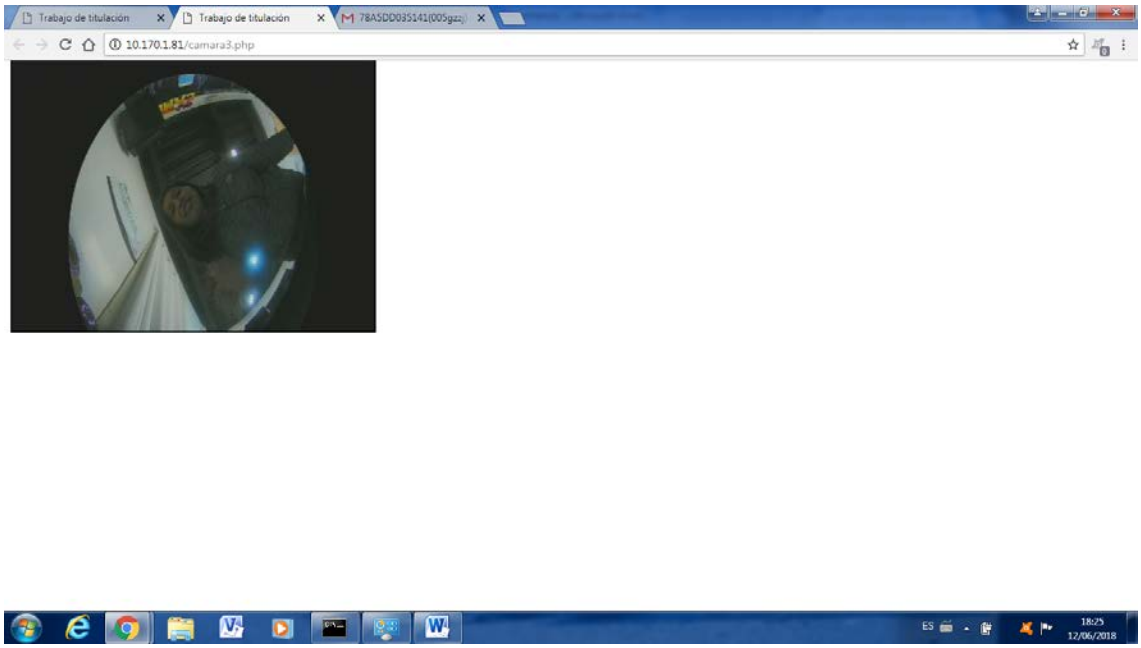


Figura 119. Cámara 3.

- En la siguiente figura 120 tenemos en registro de los sistemas, donde si un equipo se desconecta podremos verificar la hora de desconexión.

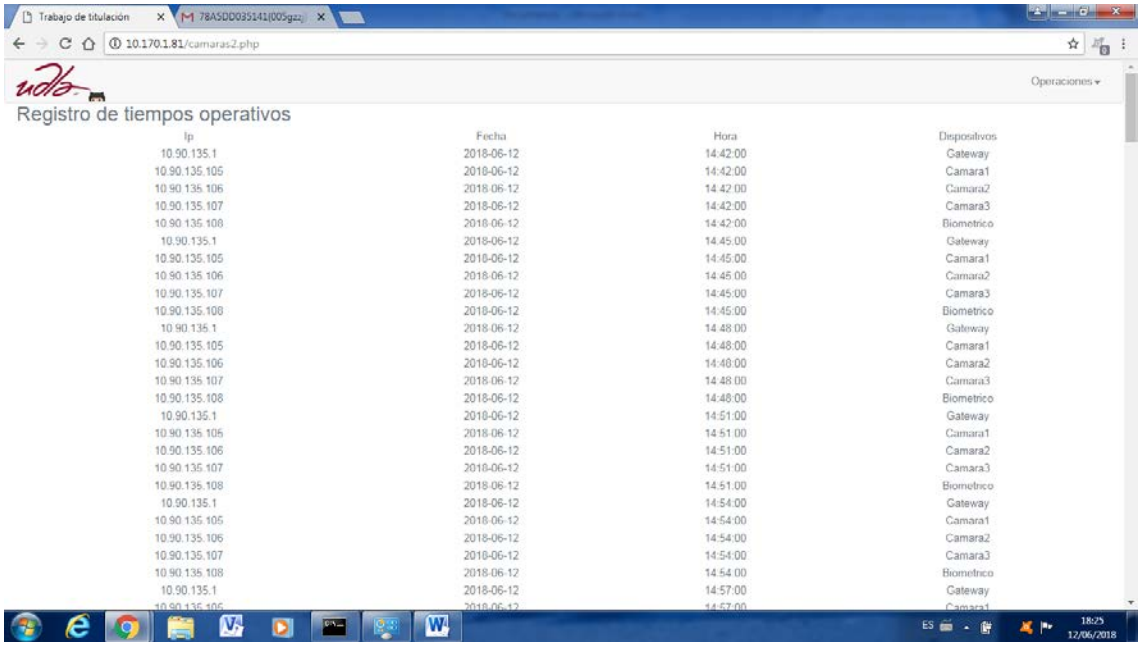


Figura 120. Registro de tiempos operativos.

- En la siguiente figura 121 tenemos los datos registrados por el biométrico de las personas que entraron al Data Center Académico.

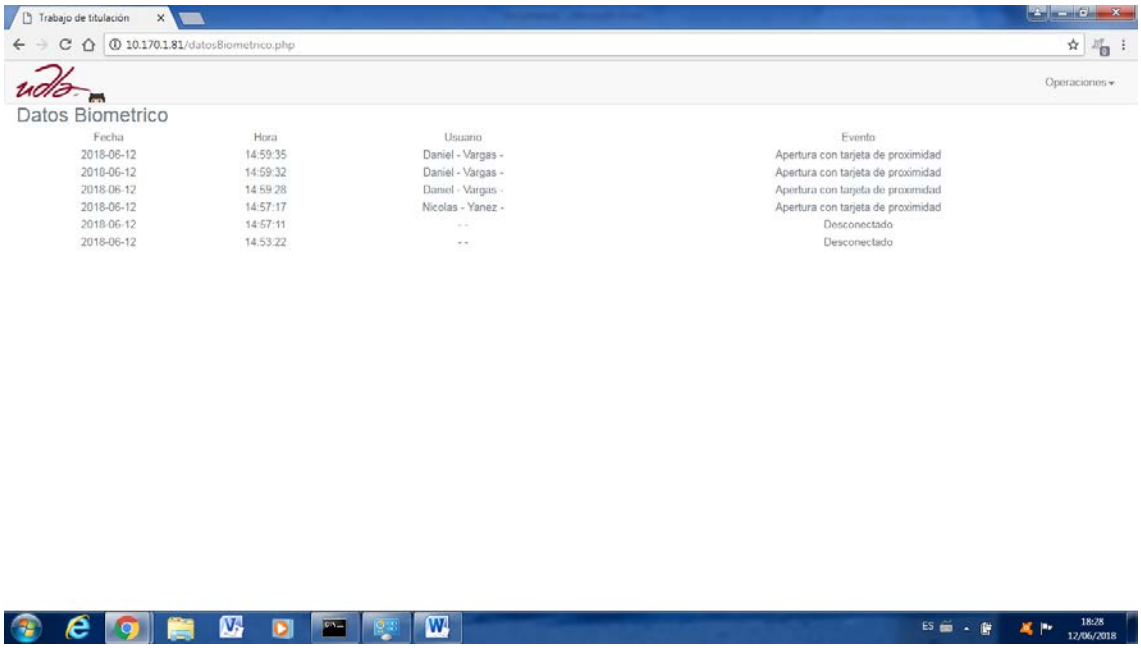


Figura 121. Datos de Biométrico.

- Control de los dispositivos captados por el AP.

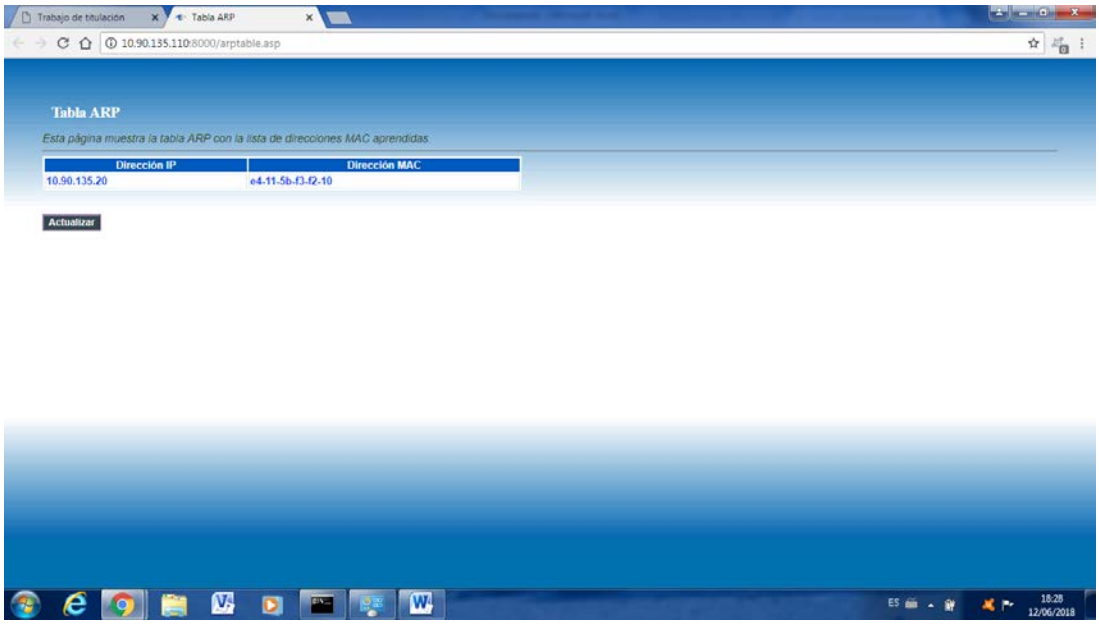


Figura 122. Tabla ARP del AP.

- Estados dispositivos en la página principal, con nombre de ID del usuario.

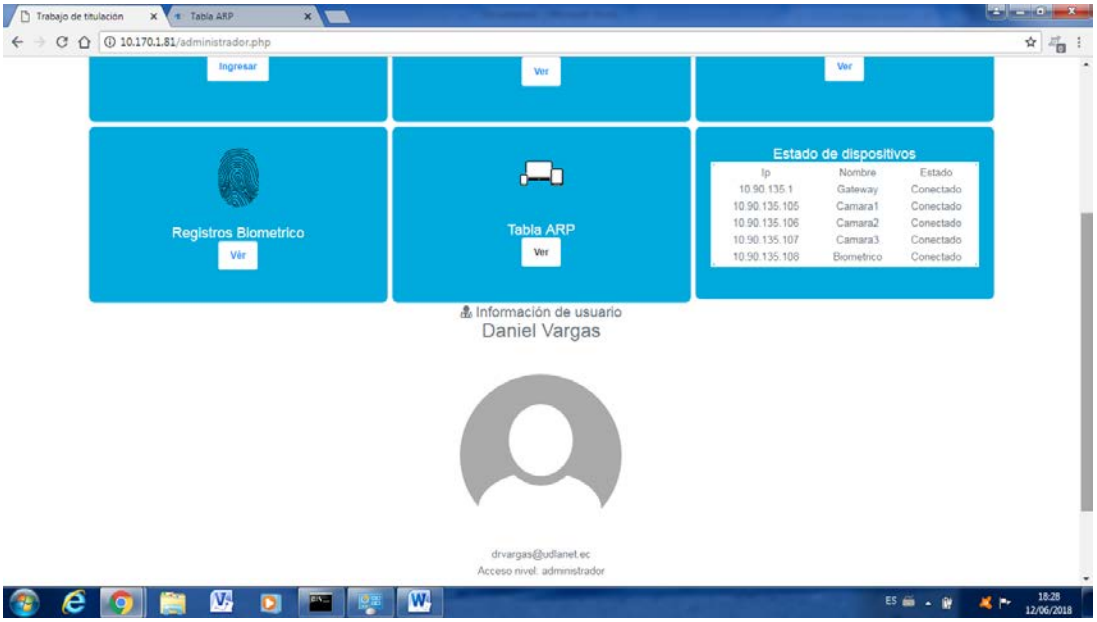


Figura 123. Estados dispositivos.

5. CONCLUSIONES Y RECOMENDACIONES.

5.1 Conclusiones.

La implementación de este sistema de seguridad en el Data Center Académico Udla sede Queri nos permite comprender el funcionamiento de un sistema de seguridad física actual, en donde las empresas desean controlar sus negocios desde cualquier lugar, almacenar las grabaciones de las cámaras de seguridad en un Cloud, sin necesidad de tener gastos monetarios en equipos adicionales y sin limitante de espacio de almacenamiento

Este sistema de seguridad instalado se complementa con lo anteriormente dicho con una página web, cuyo servicio está alojado en el Data Center Académico, donde convergen todos los sistemas convencionales y no convencionales de seguridad implementados, además un sistema proactivo de seguridad.

Los dispositivos que fueron utilizados para este sistema de seguridad llegaron a ser adquiridos siguiendo un estudio de compatibilidad con equipos que pueden ser configurados desde un entorno web, para extraer los datos de más importancia y llevarlo a lenguaje de programación PHP.

Utilizamos un diseño web en PHP antes de ASP o ASP.NET por su código, ya que PHP se lo puede abordar de manera gratuita y como sabemos es accesible para todos y recibe actualizaciones contantemente, además podríamos indicar que al ser un código abierto existen publicaciones, manuales inclusive librerías y recursos que crean las comunidades PHP, para poder utilizar el código libremente y cubrir necesidades que se desea.

Respecto a la base de datos PHP se puede utilizar tipos diferentes de base de datos con compatibilidad con Windows en nuestro sistema utilizamos MYSQL en las que su principales ventajas tenemos que es Open Source, mejor rendimiento, facilidad de configuraciones e instalación, además de tener una baja probabilidad de corromper datos y tener bajos costos en requerimientos para la elaboración de base de datos, tenemos que tener presente que su conectividad, velocidad,

seguridad es apropiado para que se pueda acceder desde una base de datos en Internet.

Este sistema de seguridad física aborda un sistema de comunicación Cliente-Servidor en la cual vinculamos varios dispositivos IP, a través de la red. Además de ser escalable en donde aprovecharemos mejor los recursos tanto de hardware o software también de una fácil administración. Contando con recursos y la integridad de los datos en el servidor la cual facilita las tareas, también el mantenimiento y actualizaciones en el servidor que en nuestro caso es el Data Center Académico.

El Data Center Académico nos ofrece servicios IaaS (Software como Infraestructura), nos ofrece infraestructura para poder instalar, configurar y administrar nuestro propio sistema operativo. El mantenimiento, actualizaciones y copias de seguridad serán responsabilidad del administrador de Data Center. Este modelo tiene las ventajas de tener reducción de tiempos puesto que el software en nuestro caso la página web se encuentra en una máquina virtual en Windows.

La instalación de sistema biométrico planteada como sistema de control de acceso hace referencia a un mecanismo que en función de una identificación mediante huella o carnet pueda acceder al área del Data Center Académico que controla una puerta con cerradura magnética. El biométrico adquirido funciona autónomamente a nuestro sistema de seguridad que converge en la página WEB, es decir, aunque no se tenga acceso a la página web, el biométrico lleva un registro de las personas que ingresaron con la fecha y la hora

La calidad del monitoreo mediante las cámaras web dependerá de las características específicas con la que se configure la cámara de seguridad, que en todos los escenarios debe ser optima, las cámaras incluyen un sistema de sensor de movimiento donde están programadas para que informen si alguien fuera de la hora de clases se encuentra cerca del Data Center Académico o los laboratorios que están con este sistema de seguridad.

El presente proyecto de titulación contemplaba la instalación de este sistema de seguridad en los laboratorios 466, 464 y 461. El prototipo funcionaba para esas tres áreas, pero por políticas y términos legales de la UDLA (Universidad de las Américas). Se logro llegar a un acuerdo de proceder con la instalación permanente solo en el laboratorio 466 con todos los índices de componentes que comprenden cámara IP, sistema biométrico, AP y pagina Web.

5.2 Recomendaciones.

Este sistema de seguridad comprende varias etapas que puede ser escalables para tener un sistema de seguridad física que cumpla con muchas más exigencias y adoptando nuevas tecnologías y técnicas.

El sistema de control de acceso por biométrico es un dispositivo que cumple con las expectativas de seguridad, pero se podría configurar con nuevos biométricos cuya configuración es mediante la web y se puede tener una aplicación móvil para un mayor manejo de registro de empleados. Estos biométricos avanzados son costosos, pero mediante estas nuevas tecnologías se podría conectar directamente a la página web que desarrollamos ahorrándonos la generación de archivo en Excel mediante software.

Las cámaras de seguridad fueron configuradas en resolución de imagen baja, ya que al tratarse de un demo de presentación para un proyecto de titulación no se necesita tener una imagen óptima. Pero se recomienda que para cualquier tipo de seguridad sea configurada con la mejor resolución de la cámara de video vigilancia.

En cuanto a los sistemas de seguridad mediante las cámaras IP, se recomienda verificar la calidad de las cámaras ya que muchas del mercado ofrecen configuración IP, pero al momento de realizar pruebas se verifica que es lenta la comunicación de respuesta del equipo, además que varias de ellas nos ofrecen la calidad de video baja. Por lo que es recomendable verificar en revistas o a través de la web, la reputación de las cámaras adquirir. Las cámaras IP que se adquirió para el Data Center Académico cuentan con un sensor de movimiento que para una aérea pequeña que va a censar no existe problema, pero si se

cambiaría a un área más grande, al equipo se le puede adaptar un sensor de movimiento extra, además de una sirena de seguridad.

Verificando las características del biométrico adquirido, se lo puede conectar un teclado externo para ofrecer más flexibilidad en las operaciones mediante puerto USB, dicho puerto también nos puede servir para descargar información a una memoria USB, el biométrico cuenta con comunicación TCP/IP además que tiene otros protocolos de comunicación como RS485.

El sistema de control por access point es un sistema proactivo que como indicamos anteriormente guarda la tabla ARP de los equipos que se conectan al AP, y se puede tener un sistema de seguridad más alto, para esto se recomienda que el AP, cuente con la configuración de actualización a cada minuto, para tener una mejor lectura de los equipos conectados, además de verificar la velocidad de comunicación mediante Ethernet o WiFi.

REFERENCIAS

Acevedo, J. F. (2015). *Rincon AVC.* Recuperado el 19 de marzo de 2018 de http://elrincondeacv2.blogspot.com/2015/04/uptime-institute-la-certificacion-tier.html

Admin. (2018). *Standards Informant*. Recuperado el 19 de marzo de 2018 de http://blog.siemon.com/standards/tia-942-a-distributed-data-center-topology

Aldama, M. (2013). *BICSI*. Recuperado el 12 de marzo de 2018 de https://www.bicsi.org/uploadedFiles/BICSI_Website/Global_Community/Presentations_and_Photos/Caribbean/2012_Fall/2.0%20Siemon%20ANSI-TIA%20942A%20ISO-IEC%2024764.pdf

Andino, G. C. (2014). *Cables y componentes para comunicaciones*. Recuperado el 17 de junio de 2018 de https://www.c3comunicaciones.es/data-center-el-estandar-tia-942/

Anixter. (2011). *The Four Layers of Data Center Physical Security for a Comprehensive*. Recuperado el 19 de marzo de 2018 de https://www.anixter.com/content/dam/Anixter/White%20Papers/12F0010X00-Four-Layers-Data-Center-Security-WP-EN-US.pdf

Anlorenro. (2016). *DAS, NAS Y SAN.* Recuperado el 20 de marzo de 2018 de https://anlorenro.wordpress.com/2016/04/18/das-nas-y-san/

ANSI. (2018). *American National Standards Institute*. Recuperado el 25 de amrzo del 2018 de https://www.ansi.org/

Azure, M. (2018). *Qué es la nube pública, privada e híbrida.* Recuperado el 26 de marzo de 2018 de https://azure.microsoft.com/es-es/overview/what-are-private-public-hybrid-clouds/

BISCI. (2015). *Protecting datacenters & mission critical facilities*. Recuperado 29 de marzo de 2018 de https://www.bicsi.org/uploadedfiles/PDFs/Conferences/Asia_11_11/2.6%20Protecting%20Mission-Critical%20Facilities%20-%20Anixter.pdf

Bitec. (2017). *Infraestructura de Sistemas.* Recuperado el 14 de abril de 2018 de https://www.itec.es/el-blog-de-bitec/adoptando-la-nube-nube-hibrida-privada-iaas-paas-o-saas.html

Cardoso, M. (2015). *Interside*. Recuperado el 30 de abril del 2018 de http://www.interside.org/es/2015/06/acesso-remoto-via-software-de.html

Center, A. e. (2014). *Revista Mundo HVACR*. Recuperado el 12 de marzo de 2018 de https://www.mundohvacr.com.mx/2011/10/ahorro-energetico-en-sistemas-de-data-center/

Cisco. (2018). *Soporte Tecnológico.* Recuperado el 7 de abril del 2018 de https://www.cisco.com/c/en/us/tech/lan-switching/ethernet/index.html

Cisco-firewall. (2018). *¿Qué es un firewall?* Recuperado el 26 de marzo de 2018 de https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

Commission, I. E. (2018). *IEC*. Recuperado el 7 de marzo de 2018 de http://www.iec.ch/

Cruz, G. (2013). *SlideShare*. Recuperado el 1 de junio de 2018 de https://es.slideshare.net/german_cruz/sistemas-de-seguridad-16443711

CyberSeguridad. (2014). *Seguridad, redes, programacion.* Recuperado el 21 de abril de 2018 de https://cyberseguridad.net/index.php/280-que-es-infiniband

Dahua. (2018). *Dahua Tecnology*. Recuperado el 29 de abril de 2018 de https://www.dahuasecurity.com/

DCD. (2017). *Isidro Ramos*. Recuperado el 16 de abril de 2018 de https://www.dcd.media/opinion/los-nuevos-est%C3%A1ndares-de-centros-de-datos-tier-5/

Editronix. (2018). *Editronix*. Recuperado el 14 de abril de 2018 de Editronix: https://www.youtube.com/watch?v=S38js8mGvKE

Electan. (2018). *Electan Electrónica y Robótica*. Recuperado el 30 de marzo de 2018 de Electan Electrónica y Robótica: https://www.electan.com/sensor-vibracion-piezoelectrico-p-3380.html

Electrónica, T. (2018). *TodoElectrónica*. Recuperado el 26 de marzo del 2018 de https://www.todoelectronica.com/es/25873-focos-infrarrojos

Electronics, H. (2018). *Hobby Electronics*. Recuperado el 6 de mayo del 2018 de http://www.hobbytronics.co.uk/passive-poe-cable-set

Epcom. (2018). *epcom syscom*. Recuperado el 31 de marzo de 2018 de https://epcom.net/

EvaluandoCloud.com. (2016). *Clasificacion de un sitio WEB*. Recuperado el 17 de abril de 2018 de http://evaluandocloud.com/clasificacion-de-datacenter/

Ferro, G. (2013). *NETWORKING.* Recuperado el 5 de mayo del 2018 de https://www.networkcomputing.com/networking/innovation-and-merchant-silicon-not-oxymoron/1590457170

Fibraopticahoy. (2014). *Sistema de cableado MPO y LC*. Recuperado el 14 de marzo de 2018 de https://www.fibraopticahoy.com/sistema-de-cableado-con-conectores-mpo/

FireOS. (2018). *FireOS*. Recuperado el 21 de mayo de 2018 de https://fireosoft.com.co/blogs/las-camaras-ip-y-la-videovigilancia/

Gartner. (2018). *It glosary.* Recuperado el 18 de abril de 2018 de https://www.gartner.com/it-glossary/data-center/

Good, B. (2018). *Band Good.com*. Recuperado el 22 de abril del 2018 de https://www.banggood.com/es/2m-Blue-Cat5-65FT-RJ45-Ethernet-Cable-For-Cat5e-Cat5-RJ45-Internet-Network-LAN-Cable-Connector-p-1116356.html?cur_warehouse=CN

Huawei. (2011). *Unificado con cable e inalámbrico.* Recuperado el 28 de abril de 2018 de http://www.huawei.com/minisite/gigabit_en/wired_wireless.html

IEC. (2018). *International Electrotechnical Commission*. Recuperado el 14 de abril de 2018 de International Electrotechnical Commission: http://www.iec.ch/

IEEE. (2018). *IEEE Advancing Technology for Humanity*. Recuperado el 28 de abril de 2018 de https://www.ieee.org/

Infoweek. (2017). *INFONEWS*. Recuperado el 24 de marzo de 2018 de https://www.infoweek.biz/la/2017/06/la-auspiciosa-relacion-energias-renovables-datacenter/

Idecnet. (2018). *Soluciones tecnologicas a medida*. Recuperado el 29 de abril de 2018 de https://www.idecnet.com/blog/item/41-tia-942

Institute, A. N. (2018). *ANSI*. Recuperado el 16 de marzo de 2018 de https://www.ansi.org/

IT, D. (2013). *Estándares en el DataCenter*. Recuperado el 28 de junio del 2018 de http://blog.aodbc.es/2013/02/23/estandares-en-el-datacenter/

Itreseller. (2017). *Convergencia o hiperconvergencia.* Recuperado el 30 de marzo de 2018 de http://www.itreseller.es/distribucion/2017/03/convergencia-o-hiperconvergencia-elige-la-mejor-opcion-para-tu-cliente

ITU. (2018). *Unión Internacional de Telecomunicaciones*. Recuperado el 4 de junio de 2018 de https://www.itu.int/es/Pages/default.aspx

Jiménez, J. A. (2017). *Planificación y Administración de Redes*. Recuperado el 12 de marzo de 2018 http://planificacionadministracionredes.readthedocs.io/es/latest/Tema02/Teoria.html

Kan, R. (2012). *Data Center Network.* Recuperado el 8 de abril de 2018 de http://www.excitingip.com/2802/data-center-network-top-of-rack-tor-vs-end-of-row-eor-design/

LineMark. (2018). *LineMark*. Recuperado el 21 de marzo de 2018 de http://www.linemak.com/ve/listado-camaras-de-seguridad/camaras-ocultas

Martínez, E. (2015). *Eveliux*. Recuperado el 13 de abril de 2018 de http://www.eveliux.com/mx/Estandares.html

Muñoz, D. (2016). *FayerWayer*. Recuperado el 16 de abril de 2018 de https://www.fayerwayer.com/2016/02/project-natick-el-plan-de-microsoft-para-instalar-centros-de-datos-en-el-mar/

Murcia, U. d. (2018). *Universidad de Murcia*. Recuperado el 17 de junio de 2018 de http://www.um.es/web/dis/

Niesteszeck2. (2012). *Observatorio Tecnológico*. Recuperado el 24 de marzo de 2018 de http://recursostic.educacion.es/observatorio/web/eu/cajon-de-sastre/38-cajon-de-sastre/1045-sistemas-fisicos-y-biometricos-de-seguridad

Oriente, A. (2012). *agenciaoriente*. Recuperado el 27 de marzo de 2018 de https://agenciaorigen.wordpress.com/galeria/huella/

Panssertechnology. (2018). *panssertechnology*. Recuperado el 8 de mayo de 2018 de http://www.panssertechnology.cl/producto/sensor-perimetral-infrarrojo-inalambrico-de-dos-2-ases-area-100-metros-lineales/

Powernet. (2016). *DISTRIBUCIÓN ELÉCTRICA DE UN DATA CENTER*. Recuperado el 17 de marzo de 2018 de http://powernet.es/web/blog/cpd/distribucion-electrica-de-un-data-center/

Renci. (2016). *From Data Center 1.0 to 3.0.* Recuperado el 16 de abril de 2018 de http://renci.org/wp-content/uploads/2016/12/RENCI-WP-2016_DatCenter3.0-FINAL-12.9.16.pdf

Saltillo, A. (2018). *Tienda Arduinos y Sensores en Saltillo*. Recuperado el 16 de junio de 2018 de http://www.arduinosaltillo.denivel.com/

Security, D. (2018). *Digital Security Magazine.com*. Recuperado el 31 de marzo de 2018 de https://www.digitalsecuritymagazine.com/2015/05/29/pelco-presenta-en-espana-su-plataforma-de-gestion-de-videovigilancia-videoxpert/

Seguridad, C. (2018). *Proteja el centro de datos virtualizado.* Recuperado el 18 de abril de 2018 de https://www.cisco.com/c/es_mx/solutions/data-center/security.html

ServiLuz. (2018). *ServiLuz*. Recuperado el 21 de marzo de 2018 de https://www.serviluz.com/detectores-de-movimiento-pir-c-56/mi-detector-de-movimiento-microondas-radar-para-luz-iluminacion-p-576.html

Siemon. (2014). *Data Center*. Recuperado el 1 de junio de 2018 de http://www.siemon.com/la/company.asp

Sony. (2018). *Sony*. Recuperado el 15 de junio de 2018 de https://pro.sony/ls_gt/products/video-security-housings/yt-ld124s

Sosio, N. (2013). *S.O.S Seguridad*. Recuperado el 12 de marzo de 2018 de http://www.seguridadsos.com.ar/dvr/

Spera, C. (2012). *Tendencia en los Data Center 3.0.* Recuperado el 13 de marzo de 2018 de https://es.slideshare.net/LogicalisLatam/presentacin-data-center-chile-logicalis-14206026

Store, X. S. (2018). *AliExpress*. Recuperado el 25 de marzo de 2018 de https://es.aliexpress.com/store/2924020

Taringa. (2018). *Taringa*. Recuperado el 21 de abril de 2018 de https://www.taringa.net/posts/info/12412496/Como-funciona-un-detector-de-movimiento.html

Telecomunicaciones, U. I. (2018). *ITU*. Recuperado el 1 de abril de 2018 de https://www.itu.int/es/Pages/default.aspx

Terdiman, D. (2016). *Fast Company*. Recuperado el 17 de abril de 2018 de https://www.fastcompany.com/3066288/how-facebooks-home-grown-data-centers-serve-billions-of-users-now-and-in-the-f

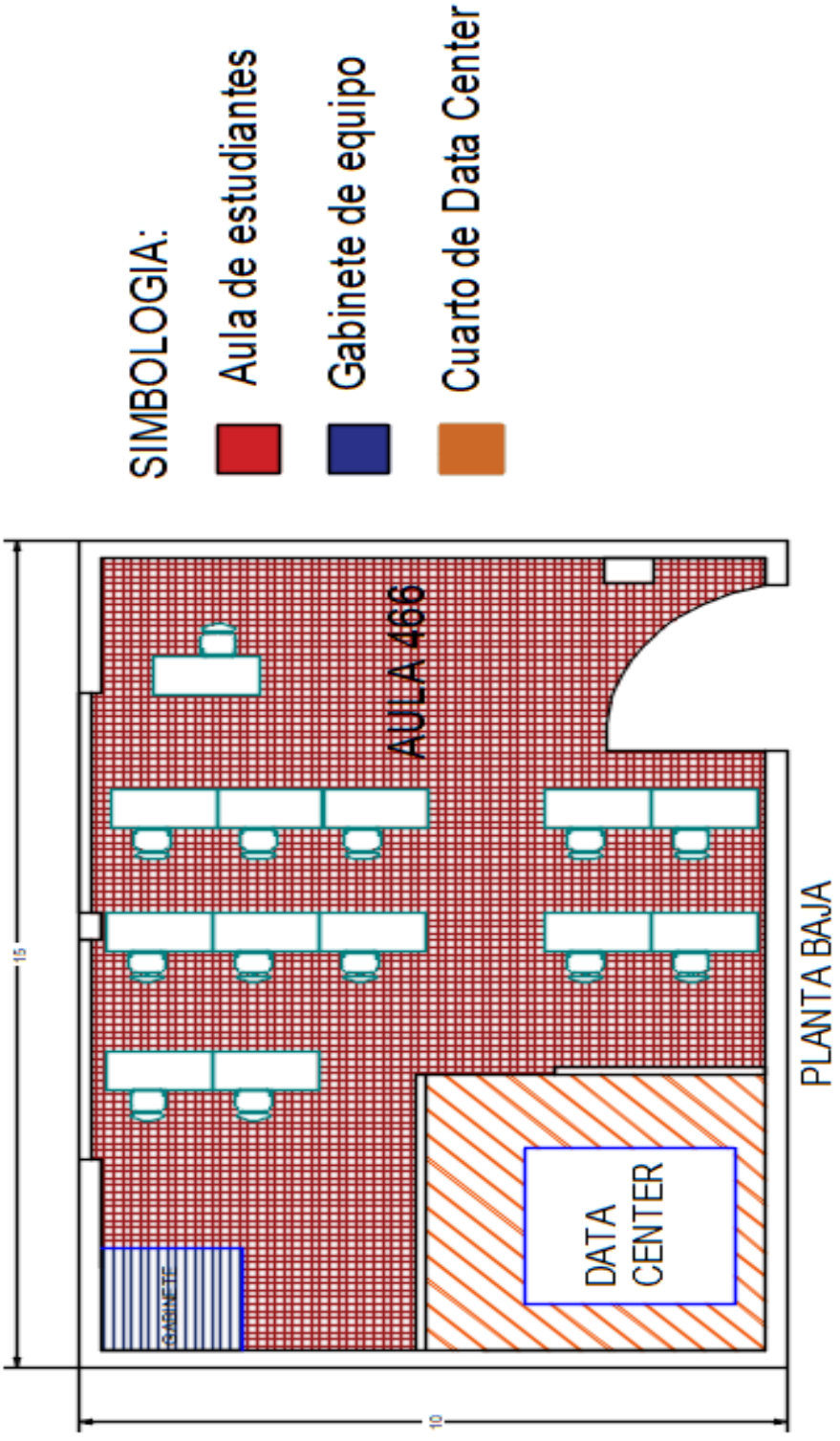
Vende, C. (2018). *Cordoba Vende*. Recuperado el 29 de abril de 2018 de http://m.cordobavende.com/productos/ficha/6729252

Vmware. (2018). *Virtualización.* Recuperado el 15 de abril de 2018 de https://www.vmware.com/co/solutions/virtualization.html

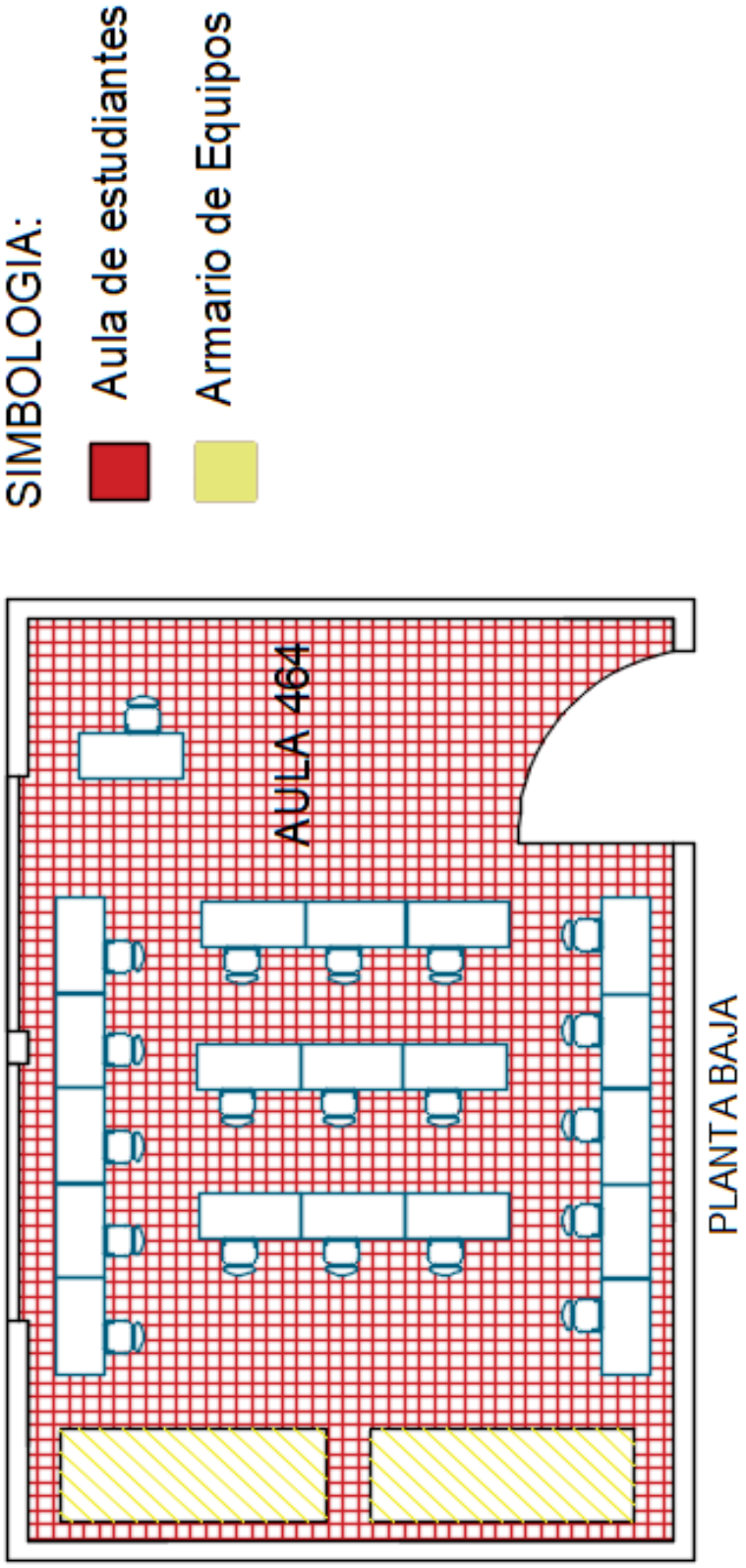
Zeichick, A. (2010). *Virtualización 3.0.* Recuperado el 16 de marzo de 2018 de http://alanzeichick.com/2008/05/what-heck-is-virtualization-30.html

ANEXOS

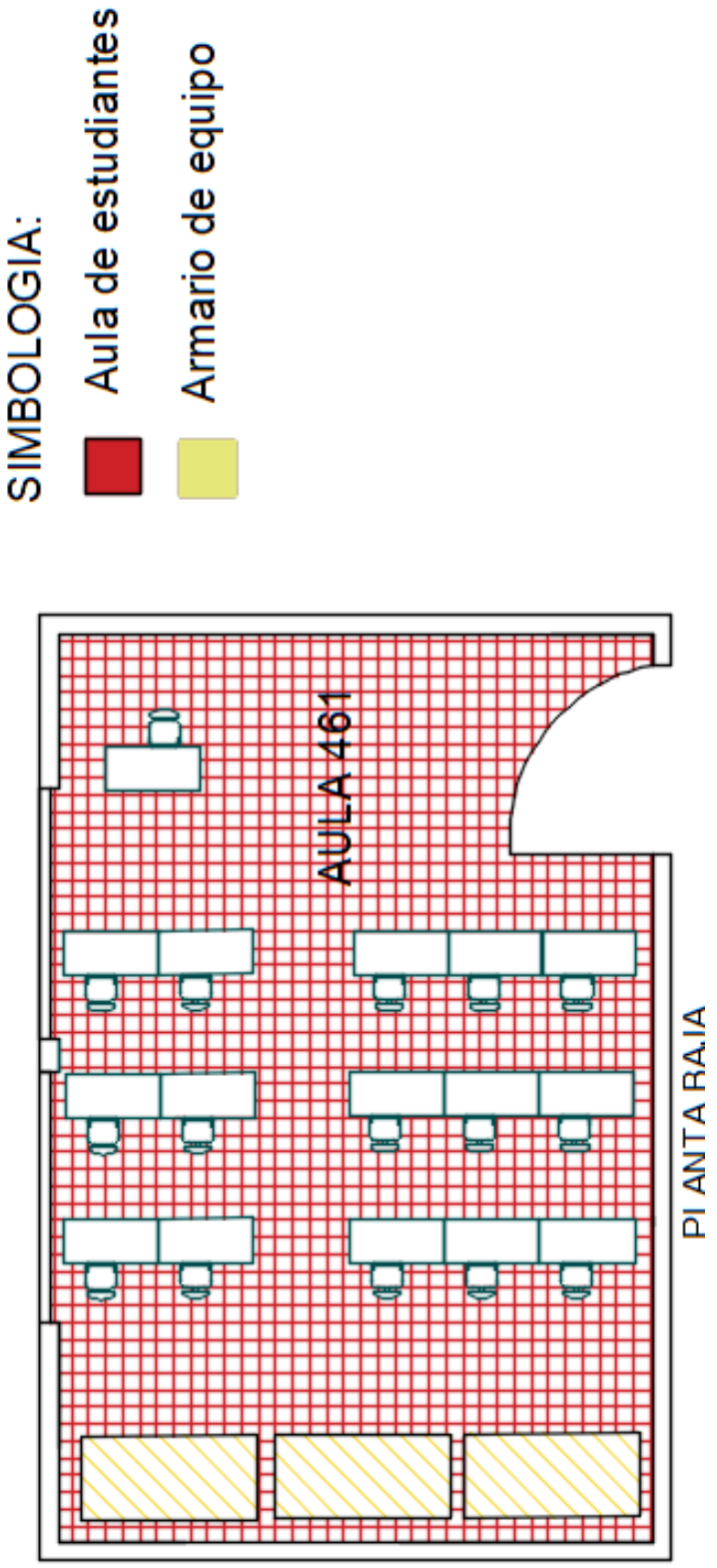
Anexo 1. Diagrama laboratorio 466 Bloque Número 4 Planta baja.



Anexo 2. Diagrama laboratorio 464 Bloque Número 4 Planta baja.



Anexo 3. Diagrama laboratorio 461 Bloque Número 4 Planta Baja.



Anexo 4. Data Sheet Cámara Web.

Item	Sub Item	Description
Image Capture	Sensor	1/4" CMOS sensor
	Pixels	300k
	Minimum Illumination	IR on, 0 Lux
	Lens	f=4.5mm, F=2.0, Fixed Iris
Pan/Tilt	Pan Coverage	270°
	Tilt Coverage	120°
IR Illumination	Lighting Control	10pcs 850nm Infrared LEDs, 5m range
	Lighting	Auto control
Video and Audio	Resolution	640*480(VGA)/320*240(QVGA)/160*120(QQVGA)
	Compression	MJPEG
	Frame Rate	30fps
	Bit Rate	128kbps ~ 5Mbps
	Image Rotation	Mirror /Up-side down
	OSD	Supported
	Audio Compression	ADPCM
Network	Basic Protocols	TCP/IP, UDP/IP, HTTP, SMTP, FTP, DHCP, DDNS, UPNP, NTP, PPPOE
	Other Protocols	802.11b/g
Other Features	Video Control	Supported
	Dual way audio	Supported
	Motion Detection	Supported
	Triggered Actions	Email/FTP/external alarm/send message to alarm Server
	User Settings	Three Level
	Date/ Time Setting	Supported
	Upgrade	Upgrade from network
	DDNS	A free DDNS provided by manufacturer
Hardware Interface	Ethernet	10Base-T/100base-TX
	Alarm In	1 way
	Alarm Out	1 way
	Audio In	Internal Mic
	Audio Out	Audio Line-out interface x 1
	Weight	245g

Physical Index	Main body	100mm(L)*99mm(W)*118mm(H)
	Power	DC 5V
	Power consumption	<6W
	Operating Temperature	0℃~ 45℃
	Operating Temperature	10% ~ 80% non-condensing
Software(PC Side)	OS Supported	Microsoft Windows 98/2000/XP/Vista
	Browser	Internet Explorer6.0 and Above or Compatible Browser, Firefox, Safari etc.
	Application Software	IPCMonitor.exe

Anexo 5. Datasheet de Biométrico.

Specifications

Capacity

Fingerprint Capacity	1500
ID Card Capacity	10000
Log Capacity	100000

Hardware

Sensor	ZEM710
CPU	32 bit ZK6001 microprocessor 400MHz
Memory	32M RAM, 256M Flash
Sensor	ZK Optical Sensor
Proximity	ID card
Relay contacts	Lock control, Alarm, Sensor, Exit Button

Display

LED Indicator	Green / Red

Environment

Oper. Temp	-10°-60°C
Oper. Humidity	20%-80%
IP Rating	IP54

Power

Power	12V, DC 3A

Communication

Comm. Port	TCP/IP, RS485
Pen drive	USB Host
Wiegand	Output and Input

Fingerprint Algorithm

Type	ZK Finger 10.0
Identification	<= 2 seconds
Verification	< 1 second
FRR	< 1%
FAR	<= 0.0001%

Languages

Available	All European languages
Maximum	1
Voices	Allowed

Dimensions

Dimensions	73 x 148 x 34.5 mm (L x W x D)
Weight	1.15 kg

Firmware

OS	Linux
Applications	AC (groups and TZ)
SDK	Standard SDK

Anexo 6. Datasheet de AP.

Características técnicas del Router ADSL

Estandar ADSL

- ITU-T G.992.1 (G.dmt).
- ANSI T1.413 Issue 2.
- G.992.2 (G.lite).
- G.994.1 (G.hs).
- Auto-negociación de adaptación de velocidad.
- ADSL2 G.dmt.bis (G.992.3).
- ADSL2 G.lite.bis (G.992.4).
- ADSL2+ (G.992.5).

Características Software

- RFC-1483/2684 LLC/VC-Mux bridged/routed.
- RFC-1577 Clásico IP sobre ATM.
- RFC-2516 PPPoE.
- RFC-2364 PPPoA.
- ITU-T 1.610 F4/F5 OAM loopback enviar y recibir.
- Protocolo 802.1d Spanning-Tree.
- DHCP Cliente/Servidor/Relay.
- NAT.
- RIP v1/v2.
- Agente DNS Relay.
- Soporte de DMZ.
- IGMP Proxy/Snooping.
- Inspección de Paquetes Stateful.
- Protección contra ataques de Denegación de Servicio.
- Filtrado de Paquetes IP.
- QoS.
- DNS Dinámico.
- Soporte de UPnP.
- Soporte de IPV6.

Gestión

- Configuración Web.
- Menú guiado de Intérprete de línea de comandos.
- SNMP v1/v2/Trap.
- Actualización de Firmware por FTP, TFTP y HTTP.
- Copia/restablecimiento de configuración.
- Herramientas de Diagnóstico.
- Soporte de TR069.

Estandar Wifi

- Cumplimiento de IEEE 802.11n (MIMO 1T1R).
- Compatible hacia atrás con 802.11b/g.
- Soporte de pulsador de encendido/apagado Wifi.
- Soporte de pulsador Wifi WPS.
- Soporte de 802.11n (MIMO 1T1R): hasta 150Mbps
- Soporte de 802.11g con tasas de datos de hasta 54 Mbps con ajuste automático hacia atrás a 48, 36, 24,18, 12, 9, y 6 Mbps.
- Soporte de 802.11b con tasas de datos de hasta 11 Mbps con ajuste automático hacia atrás a 5.5, 2, y Mbps.
- Soporte de modos de preámbulo corto y largo
- Cumplimiento de precisión de transmisión de modulación y transmisión de densidad espectral de potencia.
- IEEE 802.11i Soporte de seguridad 64/128-bits WEP, WPA, WPA2, WPS y WDS.
- Filtrado de Direcciones MAC.
- SSID Múltiple.
- IEEE 802.11e realce de QoS (WMM).

Canales/Frecuencias de operación

- USA (FCC) 11 canales: 2.412GHz ~ 2.462GHz
- Europa (ETSI) 13 canales: 2.412GHz ~ 2.472GHz.
- Japón 14 canales: 2.412GHz ~ 2.484GHz.

Interfaz Ethernet

- Soporte de 1 interfaz Ethernet 10/100 Mbps con auto selección, que cumple con los estándar IEEE 802.3x.
- Soporte Ethernet de configuración de transceptor automático MDI/MDI-X.

Interfaz Hardware

- 1 Conector de alimentación.
- 1 Pulsador de encendido/apagado del router.
- 1 Pulsador Reset para restablecimiento a valores de fábrica.
- 1 Conector telefónico RJ11 para la conexión ADSL.
- 1 Conector Ethernet para conexión del Puerto LAN.
- 1 Antena Interna.

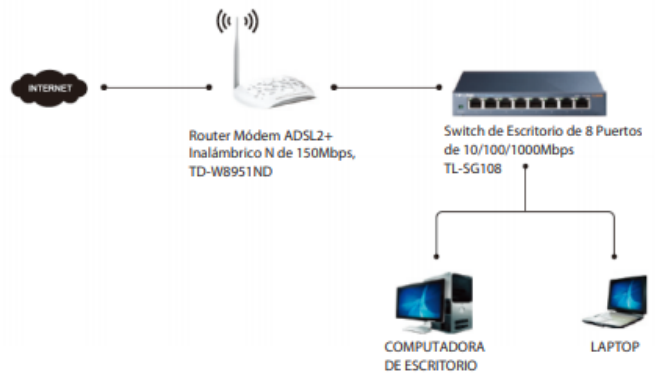
Anexo7. Datasheet de swith tp-link.

Especificaciones:

Interfaz	8 Puertos de 10/100/1000Mbps, Auto-Negociación, Auto-MDI/MDIX
Estándares de IEEE	IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3x
Protocolo	CSMA/CD
Características de Conmutación	Dúplex total y Semi-dúplex Aprendizaje de direcciones MAC Banda Ancha / Tarjeta madre posterior de 16Gbps IEEE 802.1P QoS
Velocidades de Reenvío	10BASE-T: 14880pps/puerto; 100BASE-TX: 148800pps/puerto 1000BASE-T: 1488000pps/puerto
Velocidad de transferencia datos	10/100/1000Mbps en Semi Dúplex 20/200/2000Mbps en Dúplex Total
LEDs	Encendido, Puertos Ethernet (1, 2, 3, 4, 5, 6, 7, 8)
Método de Transferencia	Almacenamiento y Envío
Suministro de Energía	9V 0.85A
Certificaciones	CE, FCC, RoHS
Dimensiones (Largo x Ancho x Alto)	6.2 x 4.0 x 1.0 pulg. (158 x 100.7 x 25.4 mm)
Condiciones Ambientales	Temperatura de Operación: 0°C~40°C (32°F~104°F) Temperatura de Almacenamiento: -40°C~70°C (-40°F~158°F) Humedad de Funcionamiento: 10%~90% sin condensación Humedad de Almacenamiento: 5%~90% sin condensación

Diagrama:

CONFIGURACIÓN TÍPICA DE LA RED



Paquete:

- Switch de Escritorio de 8 Puertos de 10/100/1000Mbps TL-SG108
- Guía del Usuario
- Adaptador de Corriente

Productos Relacionados:

- Router Módem ADSL2+ Inalámbrico N de 150Mbps, TD-W8951ND