



UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD CCTV Y
VIRTUALIZACIÓN DE SERVIDORES FIREWALL – PROXY,
CORREO Y WEB PARA LA UNIDAD EDUCATIVA
ESNUALSA

PROYECTO DE TITULACIÓN

Previo a la obtención del título de:

INGENIERO EN NETWORKING Y TELECOMUNICACIONES

AUTORES:

Wilson Andrés Del Pozo Espín
Johanna Alejandrina Hernández Páramo

TUTOR:

Ing. Ángel Ochoa

GUAYAQUIL – ECUADOR

2016



Presidencia
de la República
del Ecuador



Plan Nacional
de Ciencia, Tecnología,
Innovación y Saberes



SENESCYT
Secretaría Nacional de Educación Superior,
Ciencia, Tecnología e Innovación

REPOSITORIO NACIONAL EN CIENCIAS Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS

"IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD CCTV Y VIRTUALIZACIÓN DE SERVIDORES FIREWALL – PROXY, CORREO Y WEB PARA LA UNIDAD EDUCATIVA ESNUALSA"

REVISORES:

INSTITUCIÓN: Universidad de Guayaquil

FACULTAD: Ciencias Matemáticas y Físicas

CARRERA: Ingeniería en Networking y Telecomunicaciones

FECHA DE PUBLICACIÓN:

N° DE PÁGS.: 82

ÁREA TEMÁTICA: Implementación de Sistemas

PALABRAS CLAVES: CCTV, servidores, firewall, proxy, sitio web, correo institucional, dominio, DNS.

RESUMEN: ESNUALSA S.A. es una comunidad educativa que en los últimos años ha estado inmersa en cambios de nivel tecnológico, por lo que necesitan una solución del mismo tipo a los problemas que actualmente presentan. Mediante el levantamiento de información que se realizó en las instalaciones de la institución, se propuso que la solución más adecuada y viable es la de mejorar el sistema de seguridad y vigilancia que poseen, cambiando tanto los equipos de monitoreo como el cableado, ya que las cámaras se encontraban en buenas condiciones, además adicionar 3 nuevas cámaras para enfocar ciertas áreas que son necesarias. En cuanto a los inconvenientes que poseían con el internet, se decidió crear un servidor firewall que permita segmentar el ancho de banda dando prioridad de uso al personal administrativo, a su vez instalar un proxy que restrinja el acceso a ciertas páginas de internet para los estudiantes. Además se propuso la creación de un servidor de correo institucional para que todo el personal docente y administrativo posea una cuenta que sirva como medio de comunicación oficial tanto interno como externo, para esto se adquirió un dominio por el lapso de 5 años y a su vez se creará un tercer servidor cuya función será la de mantener activo un sitio web oficial en donde se publicará información sobre las instituciones que conforman ESNUALSA S.A., proyectando así la calidad educativa que brindan a sus estudiantes.

N° DE REGISTRO

N° DE CLASIFICACIÓN:

N°

DIRECCIÓN URL:

ADJUNTO PDF

☒ X

SÍ

☐ NO

CONTACTO CON AUTORES:

Wilson Andrés Del Pozo Espín

Johanna Alejandrina Hernández Páramo

TELÉFONO:

0997754109

0985676614

E-MAIL:

adydel@hotmail.es

aleja456-16@hotmail.com

CONTACTO DE LA INSTITUCIÓN:

Alborada Décima Etapa, Calle Isidro Ayora, Intersección
Benjamín Carrión, Manzana 46, Solar 1-10

www.esnualsa.edu.ec

NOMBRE: Coordinadora Académica

Dra. Consuelo Chafla Jarama

TELÉFONO: (04) 2174087

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de investigación **“IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD CCTV Y VIRTUALIZACIÓN DE SERVIDORES FIREWALL – PROXY, CORREO Y WEB PARA LA UNIDAD EDUCATIVA ESNUALSA”** elaborado por el **Sr. Wilson Andrés Del Pozo Espín y la Srta. Johanna Alejandrina Hernández Páramo** Alumnos no titulados de la Carrera de Ingeniería en Networking y Telecomunicaciones de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil, previo a la obtención del Título de Ingeniero en Networking y Telecomunicaciones, me permito declarar que luego de haber orientado, estudiado y revisado, la Apruebo en todas sus partes.

Atentamente

Ing. Ángel Ochoa Flores

TUTOR

DEDICATORIA

Dedico este proyecto a mis dos madres Nancy y Rosario, que me han ayudado a cumplir todas mis metas, a mi abuelo que lamentablemente nos dejó a inicios de este 2016 y no se pudo cumplir el deseo de verme como Ingeniero, aunque para él Yo ya lo era y finalmente a mi novia Johanna por ser mi compañera de vida.

Wilson Andrés Del Pozo Espín

La realización de este proyecto está dedicado a mi familia, principalmente a mi madre Elizabeth Páramo y mi hermana Carolina Hernández quienes han sido mis grandes compañeras, gracias por todo su amor y cariño. A mi compañero de tesis y novio Andrés Del Pozo quien desde el inicio de esta larga etapa siempre estuvo a mi lado. Y por último a mis alumnos del 7mo año de la Escuela San Gabriel quienes me hicieron sonreír en los momentos difíciles que se presentaron en este proyecto. Gracias por formar parte de este momento.

Johanna Alejandrina Hernández Páramo

AGRADECIMIENTO

Agradezco a mi familia en especial a mi madre Nancy Espín por darme la vida, a mi tía Rosario Espín que es como mi segunda madre por acogerme en su hogar durante todos estos años, ustedes han sido el pilar fundamental para convertirme en un ser humano de bien e ir por buen camino. Agradezco también a mi compañera y novia Johanna Hernández que ha estado conmigo durante esta trayectoria universitaria y en el desarrollo de este proyecto, brindándome su amor y el apoyo cuando más lo he necesitado.

Wilson Andrés Del Pozo Espín

Agradezco a Dios porque ha estado conmigo en cada paso que he dado, cuidándome en todo momento. A mis padres en especial a Elizabeth Páramo que han sido un pilar fundamental a lo largo de mi vida. A mi compañero de tesis Andrés Del Pozo, quien me brindó siempre su apoyo y me animaba a seguir adelante. A mi tutor de tesis Ing. Ángel Ochoa y revisores Ing. José Maridueña e Ing. Jorge Crespo quienes compartieron su conocimiento con nosotros y por último a las autoridades de la Escuela San Gabriel, Dra. Consuela Chafía y Msc. Paola Alvarado quienes estuvieron siempre dispuestas a ayudarnos en todo lo que necesitamos para este proyecto.

Johanna Alejandrina Hernández Páramo

TRIBUNAL PROYECTO DE TITULACIÓN

Ing. Eduardo Santos Baquerizo, M.Sc.
DECANO DE LA FACULTAD
CIENCIAS MATEMÁTICAS Y
FÍSICAS

Ing. Harry Luna Aveiga, M.Sc.
DIRECTOR
CINT

Ing. José Maridueña, M.Sc.
PROFESOR REVISOR DEL ÁREA -
TRIBUNAL

Ing. Jorge Crespo, M.Sc.
PROFESOR REVISOR DEL ÁREA -
TRIBUNAL

Ing. Ángel Ochoa, M.Sc.
PROFESOR DIRECTOR DEL PROYECTO
DE TITULACIÓN

Ab. Juan Chávez A.
SECRETARIO

DECLARACIÓN EXPRESA

“La responsabilidad del contenido de este Proyecto de Titulación, me corresponden exclusivamente; y el patrimonio intelectual de la misma a la UNIVERSIDAD DE GUAYAQUIL”

Wilson Andrés Del Pozo Espín

Johanna Alejandrina Hernández Páramo



UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD CCTV Y
VIRTUALIZACIÓN DE SERVIDORES FIREWALL – PROXY,
CORREO Y WEB PARA LA UNIDAD EDUCATIVA
ESNUALSA

Proyecto de Titulación que se presenta como requisito para optar por el título de
INGENIERO en NETWORKING Y TELECOMUNICACIONES

Autor: Wilson Andrés Del Pozo Espín

C.I.: 0930748918

Tutor: Ing. Ángel Ochoa

Guayaquil, Septiembre del 2016



UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD CCTV Y
VIRTUALIZACIÓN DE SERVIDORES FIREWALL – PROXY,
CORREO Y WEB PARA LA UNIDAD EDUCATIVA
ESNUALSA

Proyecto de Titulación que se presenta como requisito para optar por el título de
INGENIERO en NETWORKING Y TELECOMUNICACIONES

Autor: Johanna Alejandrina Hernández Páramo

C.I.: 0928617802

Tutor: Ing. Ángel Ochoa

Guayaquil, Septiembre del 2016

CERTIFICADO DE ACEPTACIÓN DEL TUTOR

En mi calidad de Tutor del proyecto de titulación, nombrado por el Consejo Directivo de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil.

CERTIFICO:

Que he analizado el Proyecto de Titulación presentado por el egresado **Wilson Andrés Del Pozo Espín** como requisito previo para optar por el título de Ingeniero en Networking y Telecomunicaciones cuyo problema es:

IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD CCTV Y VIRTUALIZACIÓN DE SERVIDORES FIREWALL – PROXY, CORREO Y WEB PARA LA UNIDAD EDUCATIVA ESNUALSA

Considero aprobado el trabajo en su totalidad.

Presentado por:

Wilson Andrés Del Pozo Espín

Apellidos y Nombres Completos

0930748918

Cédula de ciudadanía N°

Tutor: Ing. Ángel Ochoa

Guayaquil, Septiembre del 2016

CERTIFICADO DE ACEPTACIÓN DEL TUTOR

En mi calidad de Tutor del proyecto de titulación, nombrado por el Consejo Directivo de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil.

CERTIFICO:

Que he analizado el Proyecto de Titulación presentado por la egresada **Johanna Alejandrina Hernández Páramo** como requisito previo para optar por el título de Ingeniero en Networking y Telecomunicaciones cuyo problema es:

IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD CCTV Y VIRTUALIZACIÓN DE SERVIDORES FIREWALL – PROXY, CORREO Y WEB PARA LA UNIDAD EDUCATIVA ESNUALSA

Considero aprobado el trabajo en su totalidad.

Presentado por:

Johanna Alejandrina Hernández Páramo

Apellidos y Nombres Completos

0928617802

Cédula de ciudadanía N°

Tutor: Ing. Ángel Ochoa

Guayaquil, Septiembre del 2016



UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

Autorización para Publicación de Proyecto de Titulación en Formato Digital

1. Identificación del Proyecto de Titulación

| | |
|--|--|
| Nombre de Alumnos: Wilson Andrés Del Pozo Espín Johanna Alejandrina Hernández Páramo | |
| Dirección: Sauces IX | |
| Teléfono: 0997754109 0985676614 | E-mail: adydel@hotmail.es aleja456-16@hotmail.com |

| |
|---|
| Facultad: Ciencias Matemáticas y Físicas |
| Carrera: Ingeniería en Networking y Telecomunicaciones |
| Título al que opta: Ingeniero en Networking y Telecomunicaciones |
| Profesor guía: Ing. Ángel Ochoa |

| |
|--|
| Título del Proyecto de Titulación: Implementación de un Sistema de Seguridad CCTV y Virtualización de Servidores Firewall – Proxy, Correo y Web para la Unidad Educativa Esnualsa |
|--|

| |
|--|
| Tema del Proyecto de Titulación: Implementación de sistemas y servidores virtuales |
|--|

2. Autorización de Publicación de Versión Electrónica del Proyecto de Titulación
A través de este medio autorizo a la Biblioteca de la Universidad de Guayaquil y a la Facultad de Ciencias Matemáticas y Físicas a publicar la versión electrónica de este Proyecto de titulación.

Publicación electrónica

| | | | |
|-----------|--------------------------|------------------|-------------------------------------|
| Inmediata | <input type="checkbox"/> | Después de 1 año | <input checked="" type="checkbox"/> |
|-----------|--------------------------|------------------|-------------------------------------|

Firma Alumnos: Wilson Andrés Del Pozo Espín
Johanna Alejandrina Hernández Páramo

3. Forma de envío

El texto del proyecto de titulación debe ser enviado en formato Word, como archivo .Doc. O .RTF y .Puf para PC. Las imágenes que la acompañen pueden ser: .gif, .jpg o .TIFF.

| | | | |
|--------|-------------------------------------|-------|--------------------------|
| DVDROM | <input checked="" type="checkbox"/> | CDROM | <input type="checkbox"/> |
|--------|-------------------------------------|-------|--------------------------|

ÍNDICE GENERAL

| | |
|---|-----------|
| CARTA DE APROBACIÓN DEL TUTOR | II |
| DEDICATORIA | III |
| AGRADECIMIENTO | IV |
| TRIBUNAL DE PROYECTO DE TITULACIÓN | V |
| DECLARACIÓN EXPRESA | VI |
| AUTORÍA | VII |
| CERTIFICADO DE ACEPTACIÓN DEL TUTOR | IX |
| AUTORIZACIÓN PARA PUBLICACIÓN | XI |
| ÍNDICE GENERAL | XII |
| ABREVIATURAS | XVI |
| ÍNDICE DE CUADROS Y TABLAS | XVII |
| ÍNDICE DE GRÁFICOS | XIX |
| RESUMEN | XXI |
| ABSTRACT | XXII |
| INTRODUCCIÓN | 1 |
| CAPÍTULO I | 4 |
| EL PROBLEMA | 4 |
| PLANTEAMIENTO DEL PROBLEMA | 4 |
| -Ubicación del problema en un contexto | 4 |
| -Situación conflicto. Nudos críticos | 5 |
| -Causas y consecuencias del problema | 5 |
| -Delimitación del problema | 6 |
| -Formulación del problema | 7 |
| -Evaluación del problema | 8 |
| -Alcances del problema | 9 |
| OBJETIVOS DE LA INVESTIGACIÓN | 12 |
| -Objetivo General | 12 |
| -Objetivos Específicos | 12 |
| JUSTIFICACIÓN E IMPORTANCIA DE LA INVESTIGACIÓN | 12 |
| CAPÍTULO II | 14 |
| MARCO TEÓRICO | 14 |
| ANTECEDENTES DEL ESTUDIO | 14 |
| -Fundamentación Teórica | 15 |
| Seguridad | 15 |
| Sistema de seguridad | 15 |
| Características de un sistema de seguridad | 15 |
| Sistema de Circuito Cerrado de TV o CCTV utilizando DVR | 17 |
| Beneficios de un Sistema de seguridad de CCTV | 18 |
| Cámaras de seguridad | 18 |
| Cámaras Analógicas | 18 |
| Cámaras Digitales | 18 |
| Cámaras de Red o IP | 18 |
| Cámaras PTZ | 19 |
| DVR | 19 |
| Servidor | 19 |
| Virtualización | 20 |
| Ventajas y desventajas de la virtualización | 22 |
| Ventajas | 22 |

| | |
|---|-----------|
| Desventajas | 23 |
| Tipos de Virtualización | 23 |
| Virtualización a nivel de Sistema Operativo | 23 |
| Paravirtualización | 23 |
| Virtualización Completa | 23 |
| VMware vSphere | 24 |
| ¿Cómo utilizar vSphere? | 24 |
| Principales servicios que ofrece vSphere | 24 |
| Servicios de aplicaciones | 25 |
| Sistema Operativo | 26 |
| Tipos de Sistemas Operativos | 27 |
| Sistemas Operativos Propietarios | 28 |
| Sistemas Operativos Libres | 28 |
| GNU/Linux | 28 |
| CentOS | 29 |
| Red LAN | 30 |
| Topología | 31 |
| Topología en Malla | 31 |
| Topología en Estrella | 32 |
| Topología Árbol | 33 |
| Topología en Bus | 33 |
| Topología en Anillo | 34 |
| Firewall | 35 |
| Tipos de Firewall | 35 |
| Filtrados del Firewall | 36 |
| Proxy | 37 |
| Webmin | 37 |
| Correo Electrónico | 38 |
| Zimbra | 38 |
| Sitio Web | 40 |
| Características | 40 |
| Wordpress | 41 |
| Temas | 42 |
| Plugins | 42 |
| Widgets | 42 |
| Dominio de internet | 42 |
| -Fundamentación Social | 44 |
| -Fundamentación Legal | 45 |
| -Hipótesis | 46 |
| -Variable | 47 |
| -Definiciones Conceptuales | 48 |
| CAPITULO III | 50 |
| METODOLOGÍA DE LA INVESTIGACIÓN | 50 |
| DISEÑO DE LA INVESTIGACIÓN | 50 |
| -Modalidad de la Investigación | 50 |
| -Tipo de investigación | 50 |
| -Población y muestra | 51 |
| Población | 52 |

| | |
|--|-----------|
| Muestra | 52 |
| -Instrumentos de recolección de datos | 52 |
| Técnica de investigación | 52 |
| Encuesta | 52 |
| Instrumento de investigación | 53 |
| -Recolección de la información | 53 |
| -Procesamiento y análisis | 53 |
| -Validación de hipótesis | 63 |
| CAPÍTULO IV | 64 |
| PROPUESTA TECNOLÓGICA | 64 |
| Sistema CCTV | 64 |
| Cableado Estructurado | 64 |
| Servidores virtualizados | 65 |
| -Análisis de factibilidad | 65 |
| Factibilidad Operacional | 65 |
| Factibilidad Técnica | 66 |
| -Propuesta tecnológica y solución | 66 |
| -Tecnología disponible | 66 |
| Hardware CCTV | 67 |
| Hardware – Servidor | 68 |
| Software – Servidor | 70 |
| -Conocimientos técnicos | 71 |
| -Factibilidad Legal | 71 |
| -Factibilidad Económica | 71 |
| -Etapas de la metodología del Proyecto | 72 |
| Fase de planificación | 72 |
| Fase de iniciación | 72 |
| Fase de ejecución | 73 |
| Fase de Entrega o puesta en marcha | 75 |
| Fase de Control | 75 |
| -Entregables del proyecto | 76 |
| Manual Técnico | 76 |
| - Manual Técnico del sistema CCTV | 76 |
| - Manual técnico sobre | 76 |
| -Hypervisor | 76 |
| -Servidor Firewall – Proxy | 76 |
| -Servidor de Correo | 76 |
| -Servidor Web | 76 |
| Manual de Usuario | 76 |
| - Manual de Usuario del Sistema CCTV | 76 |
| - Manual de Usuario sobre | 76 |
| -Servidor de Correo | 76 |
| -Sitio Web | 77 |
| -Webmin | 77 |
| -Criterios de validación de la propuesta | 77 |
| -Criterios de aceptación del Producto o Servicio | 77 |
| Mejoras del sistema de CCTV | 77 |
| Segmentación del Ancho de Banda | 77 |

| | |
|--------------------------------|-----------|
| Restricción a Internet | 77 |
| Acceso al sitio web | 78 |
| Correo institucional | 78 |
| CAPÍTULO V | 79 |
| CONCLUSIONES Y RECOMENDACIONES | 79 |
| -Conclusiones | 79 |
| -Recomendaciones | 80 |
| BIBLIOGRAFÍA | 81 |
| ANEXOS | 83 |

ABREVIATURAS

| | |
|-------------|---|
| DVR | Digital Video Recorder |
| s.f | Sin fecha |
| CCTV | Circuito cerrado de televisión |
| TIC | Tecnología de la información y comunicación |
| EGB | Educación General Básica |
| UTP | Unshielded twisted pair o par trenzado sin blindaje |
| CD | Disco compacto |
| DVD | Disco Versátil Digital |
| LAN | Local Area Network o Red de área Local |
| UPS | Sistema de alimentación Ininterrumpida |
| VCR | Videograbadora |
| IP | Protocolo de Internet |
| SO | Sistema Operativo |
| TI | Tecnología de la información |
| ADSL | Línea de abonado digital asimétrica |
| TCP | Protocolo de Control de Transmisión |
| UDP | Protocolo de datagrama de usuario |
| BSD | Distribución de software Berkeley |
| URL | Localizador de recursos uniforme |
| CMS | Sistema de gestión de contenidos |

ÍNDICE DE CUADROS

| | |
|--|----|
| CUADRO N° 1 | |
| Causas y consecuencias del problema..... | 5 |
| CUADRO N° 2 | |
| Delimitación del problema..... | 7 |
| CUADRO N° 3 | |
| Variables..... | 47 |
| CUADRO N° 4 | |
| Población..... | 52 |
| CUADRO N° 5 | |
| Frecuencia de pregunta N° 1..... | 54 |
| CUADRO N° 6 | |
| Frecuencia de pregunta N° 2..... | 55 |
| CUADRO N° 7 | |
| Frecuencia de pregunta N° 3..... | 56 |
| CUADRO N° 8 | |
| Frecuencia de pregunta N° 4..... | 57 |
| CUADRO N° 9 | |
| Frecuencia de pregunta N° 5..... | 58 |
| CUADRO N° 10 | |
| Frecuencia de pregunta N° 6..... | 59 |
| CUADRO N° 11 | |
| Frecuencia de pregunta N° 7..... | 60 |
| CUADRO N° 12 | |
| Frecuencia de pregunta N° 8..... | 61 |
| CUADRO N° 13 | |
| Frecuencia de pregunta N° 9..... | 62 |
| CUADRO N° 14 | |
| Hardware CCTV..... | 67 |
| CUADRO N° 15 | |
| Hardware Servidor..... | 68 |

| | |
|------------------------|----|
| CUADRO N° 16 | |
| Software Servidor..... | 70 |

ÍNDICE DE GRÁFICOS

| | |
|-------------------------------------|----|
| GRÁFICO Nº 1 | |
| Tipos de Sistemas de seguridad..... | 16 |
| GRÁFICO Nº 2 | |
| Sistema de seguridad con DVR..... | 17 |
| GRÁFICO Nº 3 | |
| Virtualización..... | 22 |
| GRÁFICO Nº 4 | |
| VMware..... | 26 |
| GRÁFICO Nº 5 | |
| Cliente – Servidor..... | 30 |
| GRÁFICO Nº 6 | |
| Punto – Punto..... | 31 |
| GRÁFICO Nº 7 | |
| Topología en Malla..... | 32 |
| GRÁFICO Nº 8 | |
| Topología Estrella..... | 32 |
| GRÁFICO Nº 9 | |
| Topología en Árbol..... | 33 |
| GRÁFICO Nº 10 | |
| Topología en Bus..... | 34 |
| GRÁFICO Nº 11 | |
| Topología Anillo..... | 34 |
| GRÁFICO Nº 12 | |
| Firewall..... | 35 |
| GRÁFICO Nº 13 | |
| Webmin..... | 38 |
| GRÁFICO Nº 14 | |
| Wordpress..... | 41 |
| GRÁFICO Nº 15 | |
| Dominio e internet..... | 43 |

| | |
|--------------------|----|
| GRÁFICO Nº 16 | |
| Pregunta Nº 1..... | 54 |
| GRÁFICO Nº 17 | |
| Pregunta Nº 2..... | 55 |
| GRÁFICO Nº 18 | |
| Pregunta Nº 3..... | 56 |
| GRÁFICO Nº 19 | |
| Pregunta Nº 4..... | 57 |
| GRÁFICO Nº 20 | |
| Pregunta Nº 5..... | 58 |
| GRÁFICO Nº 21 | |
| Pregunta Nº 6..... | 59 |
| GRÁFICO Nº 22 | |
| Pregunta Nº 7..... | 60 |
| GRÁFICO Nº 23 | |
| Pregunta Nº 8..... | 61 |
| GRÁFICO Nº 24 | |
| Pregunta Nº 9..... | 62 |



UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

**IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD CCTV Y
VIRTUALIZACIÓN DE SERVIDORES FIREWALL – PROXY,
CORREO Y WEB PARA LA UNIDAD EDUCATIVA
ESNUALSA**

Autores: Wilson Andrés Del Pozo Espín
Johanna Alejandrina Hernández Páramo
Tutor: Ing. Ángel Ochoa

RESUMEN

ESNUALSA S.A. es una comunidad educativa la misma que en los últimos años ha estado inmersa a cambios de nivel tecnológico, por lo que necesitan una solución del mismo tipo a los problemas que actualmente presentan. Mediante el levantamiento de información que se realizó en las instalaciones de la institución, se propuso que la solución más adecuada y viable es la de mejorar el sistema de seguridad y vigilancia que poseen, cambiando tanto los equipos como el cableado ya que las cámaras se encontraban en buenas condiciones, además adicionar 3 nuevas cámaras para enfocar ciertas áreas que son necesarias. En cuanto a los inconvenientes que poseían con el internet, se decidió crear un servidor firewall que permita segmentar el ancho de banda dando prioridad de uso al personal administrativo, a su vez instalar un proxy que restrinja el acceso a ciertas páginas de internet para los estudiantes. Además se propuso la creación de un servidor de correo institucional para que todo el personal docente y administrativo posea una cuenta que sirva como medio de comunicación oficial tanto interno como externo, para esto se adquirió un dominio por el lapso de 5 años y a su vez se creará un tercer servidor cuya función será la de mantener activo un sitio web oficial en donde se publicará información sobre las instituciones que conforman ESNUALSA S.A. proyectando así la calidad educativa que brindan a sus estudiantes.



UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

**IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD CCTV Y
VIRTUALIZACIÓN DE SERVIDORES FIREWALL – PROXY,
CORREO Y WEB PARA LA UNIDAD EDUCATIVA
ESNUALSA**

Autores: Wilson Andrés Del Pozo Espín
Johanna Alejandrina Hernández Páramo
Tutor: Ing. Ángel Ochoa

ABSTRACT

ESNUALSA S.A. Is an educative community that in the last years has been involved in technological changes, that's why they need a solution in the same kind to the problems that they have nowadays. Throughout the data mining that took place in the institutions, there was proposed that the most adequate and viable solution is to improve the security and vigilance system that they have, changing the equipment and the cable because the cameras they had were in good conditions, in addition add 3 new cameras to focus several areas that are necessities. About the issues they had with the internet, it was decided to create a firewall sever that permits segment the bandwidth with priority to the use of management employers, at the same time to install a proxy that restricts the access to several internet web pages for the students.

Moreover it was proposed to create a sever of institutional mail so that the teachers and management employers could have an account that server an official communication media, external and internal for that was purchased a domain for five years and at the same time it will be created a third sever whose function will be to keeping active the official web site where it will be published the information of the institutions that conform ESNUALSA S.A. proyecting in that way the educative quality they offer to the students.

INTRODUCCIÓN

En la actualidad se puede observar que la mayoría de Instituciones Educativas han realizado mejoras conforme la tecnología avanza. Hoy en día se aprecia que tanto instituciones públicas como privadas, cuyas actividades están orientadas a diferentes ámbitos, hacen uso de la tecnología para ofrecer un ambiente más seguro a los usuarios utilizando diferentes sistemas de seguridad.

Actualmente la adquisición de correos propios por parte de empresas, instituciones y demás organizaciones, para el manejo de su información en sus actividades diarias, es algo evidente que se ha dado gracias a la evolución tecnológica, dejando atrás el uso de servicios gratuitos de correo como son los tradicionales Hotmail, Gmail, Yahoo, etc. ya que representan en cierto aspecto un riesgo para las instituciones.

El uso de sitios web en nuestros días, representa un beneficio tanto para las instituciones propietarias del portal como para los usuarios, ya que es una forma fácil y rápida de proporcionar - obtener información requerida por ambas partes, sea esta información sobre servicios prestados, ubicación para ponerse en contacto o realizar consultas, sugerencias y otros.

Haciendo referencia al ámbito educativo, si bien es cierto que el uso del internet constituye una herramienta práctica y eficiente para los estudiantes en la elaboración de sus tareas, el libre acceso al mismo en horas de clase también simboliza en cierta forma una distracción, ya que direccionan su interés en ingresar a paginas poco adecuadas como son las redes sociales, juegos en línea y otros. Esto repercute no solo en su aprendizaje, también ocasionan molestias para el personal que labora dentro de las instituciones ya que la mayoría de actividades laborales se verán afectadas debido a que hacen mal uso de este recurso por la falta de control sobre el mismo.

En la Comunidad Educativa ESNUALSA al realizar un análisis se percibe la necesidad de mejorar en todos los puntos anteriormente descritos, planteando así

una propuesta en la cual se expone hacer uso de diferentes herramientas que a su vez conducen a la actualización tecnológica de la misma.

Con la implementación de un Sistema de Seguridad se puede tener un mejor control sobre los posibles sucesos que se den dentro de las instalaciones y el ingreso/salida de personas externas. La adquisición de un correo propio ayudará que la información se maneje con más eficiencia y organización. La creación de un sitio web oficial será de gran utilidad para la emisión de información que debe ser de conocimiento de padres de familia y de personas en general como son actividades curriculares, enlaces a redes sociales, multimedia (galería de fotos y videos) etc.

La utilización de un servidor Firewall – Proxy, es considerado actualmente, una de las herramientas más eficaces para brindar mayor seguridad informática a las instituciones, indistinto de la actividad que se realice, a su vez que permite también limitar el acceso a los diferentes sitios web aplicando políticas de restricción. Por lo tanto se considera como la solución más factible para controlar el uso del internet dentro la Comunidad Educativa ESNUALSA.

La tecnología va evolucionando día a día, por ende las instituciones principalmente las educativas deben ir mejorando en conjunto con dichos cambios, debido a que actualmente la mayoría de personas buscan escuelas y/o colegios donde se hagan uso de herramientas tecnológicas modernas que brinden una enseñanza de calidad.

Este proyecto consiste en la implementación de un Sistema de Vigilancia y Monitoreo con cámaras de seguridad, utilizando un Digital Video Recorder (DVR) como equipo de almacenamiento, el cual permite guardar y reproducir videos pasados, instalación de servidores Firewall-Proxy, Correo y Web dentro de un mismo equipo físico, utilizando como principal herramienta la virtualización.

En el desarrollo del presente proyecto, se encontrará mayor información relacionada netamente al tema descrito en párrafos anteriores, el cual consta de cinco capítulos estructurados con diferentes puntos concernientes al tema central como los objetivos tanto generales como específicos, alcance del proyecto, delimitación y formulación del mismo, fundamentación teórica en la que se basa,

fundamentación legal en la cual se apoya el desarrollo del proyecto, el tipo de investigación que se realizó y las técnicas aplicadas con sus respectivos instrumentos de recolección de información, la selección de la población y de la muestra en caso de requerirse, el procesamiento y análisis de los datos obtenidos, así como también las conclusiones establecidas con sus respectivas recomendaciones y las fuentes de donde se tomó parte de la información contenida en este proyecto.

CAPÍTULO I

EL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

Ubicación del problema en un contexto

La empresa “ESNUALSA S.A.”, lugar donde se desarrolla el presente proyecto educativo, está ubicada en la ciudad de Guayaquil, provincia del Guayas en la que actualmente laboran dos instituciones educativas en dos jordanas distintas:

- Jornada matutina: Escuela Particular Mixta N° 542 “Nueva Alborada”
- Jornada vespertina: Escuela Particular Mixta N° 224 “San Gabriel”

Cuenta con un sistema de CCTV obsoleto, sin utilizarse durante varios años y actualmente existe la necesidad de su utilización debido a acontecimientos que se han dado, muchos de estos vinculados con la seguridad de los estudiantes en el perímetro de las instalaciones.

Un factor importante para que este sistema haya llegado a un estado de inutilización es la falta de conocimiento sobre el manejo del mismo por parte del personal administrativo que ha ido cambiando con el transcurso del tiempo.

Con el avance de la tecnología y la utilización de las TIC, en este ámbito educativo existe la necesidad de contar con un correo institucional y un sitio web que servirán como medio oficial de comunicación por internet entre todo el personal docente y administrativo de dichas instituciones.

El libre acceso a internet a temprana edad, representa en los estudiantes una distracción y esto repercute en horas de clase, específicamente en las horas de práctica en el laboratorio de informática donde direccionan su interés a páginas de redes sociales, juegos en línea y portales no adecuados, lo que evidencia la falta de control en la utilización de la web y que a su vez genera inconvenientes en las labores administrativas por la saturación del ancho de banda.

Situación Conflicto Nudos Críticos

Han existido casos de comportamiento agresivo, accidentes y daños dentro de las instalaciones por parte de los estudiantes y la falta de evidencia dificulta realizar el respectivo seguimiento.

Se requiere evitar posibles casos de desaparición de estudiantes por secuestros que puedan darse en la parte exterior de las instalaciones, personas inescrupulosas que tengan la insolencia de acercarse a retirar a estudiantes ajenos dando los nombres y apellidos.

La información institucional que es enviada por personal administrativo, autoridades y docentes se lo hace a través de correos personales sin tener la certeza de que la misma es recibida, mal utilizada o enviada a terceros.

Los comunicados dirigidos a padres de familia se envían de forma escrita por medio del diario escolar, el cual casi nunca es revisado por el representante y muchas veces no existe una comunicación directa entre ambas partes.

Al contar con un servicio corporativo de internet, no se le está dando el uso adecuado, el ancho de banda es saturado en su mayoría por los estudiantes al momento de recibir las prácticas en el laboratorio de computación.

Causas y Consecuencias del Problema

Causas y Consecuencias del Problema
Cuadro Nº 1

| CAUSAS | CONSECUENCIAS |
|--|---|
| No existe una persona que se haga responsable del control de ingreso y salida ni cámaras que enfoquen las puertas de las instalaciones | Fácil acceso de personas no autorizadas a las instalaciones |
| El cableado del CCTV está en mal estado | No se pueda visualizar de manera eficiente las cámaras instaladas |
| Falta de vigilancia dentro de las aulas de la institución. | Posibles sucesos entre estudiantes sin evidencias que dificulte realizar el respectivo seguimiento. |
| Envío de comunicados de forma escrita o papeles grapados al diario. | Posibles extravíos de comunicados físicos y que no lleguen a los representantes |

| | |
|--|---|
| Envío inseguro de información por medio de cuentas de correo electrónico personales | Posible desvío de información a terceros al digitar incorrectamente la cuenta de correo |
| Cuentas de correo personales con nombres no apropiados para representar a una institución educativa | Receptor pase desapercibido el correo al no saber que este proviene de una institución educativa |
| Falta de control en el uso del internet por parte de los estudiantes | Los estudiantes no prestan atención a la clase y se entretienen navegando en internet |
| Consumo de la mayor parte del ancho de banda al utilizar el laboratorio de computación en forma no apropiada | Malestar del personal administrativo al momento de realizar sus actividades diarias debido a la lentitud del internet |

Fuente: Datos de la investigación

Elaboración: Andrés Del Pozo Espín – Johanna Hernández Páramo

Delimitación del problema

En la actualidad, con el desarrollo de la tecnología, nace la necesidad en las instituciones de contar con un sistema de seguridad para tener un buen control en las mismas, y con mayor razón las instituciones educativas no deben estar exentas ya que está bajo su responsabilidad asegurar la integridad física y moral de los estudiantes donde los padres han depositado su total confianza.

Con la existencia de planes corporativos de internet y la contratación de los mismos por parte de las empresas, es de vital importancia que se implementen servidores para mayor rendimiento y productividad aprovechándolos al máximo buscando siempre los mejores beneficios.

Es por eso que este proyecto propone como medio de solución la implementación de un sistema actualizado de CCTV funcional al 100% y dotar de tres servidores, uno como servidor de correo institucional, otro como servidor de firewall – proxy y el último como servidor web. En base a los recursos que se tienen, se analizó y se llegó a la conclusión de que la mejor alternativa es virtualizar los servidores utilizando herramientas gratuitas y sistemas operativos Open Source, todo dentro de un mismo equipo físico robusto.

Delimitación del problema
Cuadro N° 2

| | |
|----------------|---|
| CAMPO | Tecnológico |
| AREA | Tecnologías de la Información y las comunicaciones |
| ASPECTO | Propuesta para la implementación de un sistema de seguridad, correo institucional, servidor web y la gestión del tráfico entrante y saliente generado por internet. |
| TEMA | Implementación de un Sistema de Seguridad CCTV y virtualización de servidores Firewall-Proxy, Correo y Web para la unidad educativa ESNUALSA |

Fuente: Datos de la investigación

Elaboración: Andrés Del Pozo Espín – Johanna Hernández Páramo

Formulación del Problema

¿Cómo influye la implementación de un sistema CCTV y la creación de servidores de correo, web y firewall - proxy en la comunidad educativa de ESNUALSA S.A. en el año 2016?

En la comunidad educativa ESNUALSA S.A. se aprecia la no utilización del sistema obsoleto de seguridad, la necesidad de un correo institucional, un sitio web y la falta de control sobre el internet corporativo que posee.

Al realizar el estudio de estas problemáticas se propone:

- Actualizar el sistema de seguridad con la finalidad de tener un mayor control de las instalaciones y a su vez sea de fácil manejo.
- Crear servicio de correo institucional para dejar de usar cuentas personales como medio de envío/recepción de información institucional.
- Crear un sitio web como medio informativo para el público en general.
- Controlar el acceso a internet y segmentarlo por medio de la creación de un servidor firewall – proxy.

Evaluación del Problema

Delimitado: La comunidad educativa ESNUALSA S.A. hoy en día evidencia un problema y este es la incorrecta utilización de los recursos tecnológicos disponibles, que pueden ser para beneficio del personal administrativo, docente, estudiantes y padres de familia.

Claro: Los recursos tecnológicos que tienen no son aprovechados por falta de conocimiento.

Evidente: Los diversos sucesos negativos que han acontecido entre los estudiantes muchas veces carecen de evidencias, la incorrecta utilización del internet y la inseguridad del envío de información son temas pendientes a resolver.

Relevante: La implementación de este proyecto permitirá brindar mayor seguridad para la comunidad educativa, se tendrá un control de quienes ingresan y salen de las instalaciones, se tendrá evidencia en caso de que exista algún inconveniente con los estudiantes, el personal administrativo trabajará con normalidad cuando utilicen el internet sin presentar problemas de saturación y el correo institucional al igual que el sitio web permitirán ser ya un medios oficiales de comunicación y de gran ayuda para los representantes que cuya jornada laboral la realizan en oficina, donde pueden recibir novedades sobre sus hijos.

Original: La empresa cuenta con un sistema de seguridad obsoleto que solo permite visualizar una cámara a la vez, nuestra propuesta mejora la forma de visualización usando todas las cámaras a la vez y permitiendo grabar lo que acontece durante todo el día teniendo evidencia cuando se suscite algún inconveniente. En cuanto a los servidores se aplicará los conocimientos adquiridos sobre virtualización para aprovechar más los recursos de la máquina que se tiene.

Factible: El proyecto no requiere de una fuerte inversión económica ni de mucho tiempo de desarrollo, se encaminará más por la virtualización para aminorar notablemente los costos.

Alcances del Problema

Implementación de un Sistema de Seguridad CCTV y virtualización de servidores Firewall – Proxy, Correo y Web para la unidad educativa ESNUALSA

CCTV

La empresa cuenta con cámaras en las siguientes aulas:

- Inicial 1 “A”
- Inicial 2 “A”
- Inicial 1 (Matutino)
- Primero “A”
- Tercero EGB (Matutino)
- Segundo EGB
- Tercero EGB
- Cuarto EGB
- Quinto EGB
- Sexto EGB
- Séptimo EGB
- Laboratorio de Inglés

Se realizó una inspección y se determinó que de las 12 cámaras solo 6 emiten video y las restantes funcionan pero tienen problemas en el cableado.

Los equipos de recepción de video que actualmente posee la comunidad educativa solo permiten visualizar una cámara y no proporcionan un respaldo, si se desea ver otras cámaras se lo debe hacer manualmente.

La conexión de las cámaras con los equipos de recepción es por medio de cable coaxial, el cual en varios tramos se encuentra deteriorado.

En base a esto se cambiarán los 2 equipos de recepción por un DVR de 16 canales, y se reemplazará el cableado con cable UTP categoría 6, adicionalmente se instalará 3 cámaras nuevas en dirección a los siguientes puntos:

- 1 cámara enfocando a la puerta de ingreso principal.
- 1 cámara en el pasillo del baño de varones.
- 1 cámara en el laboratorio de computación.

Se crearán políticas para la grabación, las cuales permitan almacenar video durante la jornada laboral, de esta manera nos aseguramos que el disco duro no se llene y se sobrescriba de inmediato, además se capacitará a la persona que se

encargará del manejo del DVR la misma que determinará el tiempo de respaldo de video, creando así respaldos físicos en CD o DVD en cuanto se produzcan novedades y eliminando las horas de grabación inservible.

SERVIDORES

Se ensamblará una máquina que posea las características idóneas cumpliendo el papel de un servidor ya que es mucho más factible económicamente que adquirir servidores reales que son mucho más costosos.

Se procederá a instalar el sistema de virtualización el cual nos permita crear nuestros servidores aprovechando al máximo los recursos de nuestro equipo físico.

Una vez listo el sistema de virtualización se procede a crear las máquinas virtuales, asignándole a cada uno los recursos adecuados a la función que van a cumplir.

El sistema operativo que tendrán las máquinas virtuales es Open Source, y el más idóneo para el desarrollo de este proyecto es CentOS 7. Los servidores a instalarse son:

- Firewall – Proxy
- Correo
- Web

Un firewall nos permite gestionar, filtrar y/o bloquear el tráfico entrante o saliente que se genera entre dos redes según la configuración que contenga. Es importante tener un servidor firewall más aún si se van a instalar servidores de correo y web, ya que este impide ataques informáticos, bloqueando acceso a redes, direcciones o puertos desde o hacia una red determinada.

Dentro del servidor de firewall se configurará el Squid quien se encarga de reducir el ancho de banda mejorando los tiempos de respuesta y rendimiento de las conexiones de empresas y particulares a internet permitiendo reutilizar las páginas web solicitadas con frecuencia.

Otra de las funciones que realizará el servidor firewall es el control de ancho de banda, el cual va a permitir repartir de forma eficiente el ancho de banda de internet para un usuario, grupo de usuarios o servicios determinados.

Es necesario la creación de iptables, que no es más que las políticas de filtrado del tráfico que circula por la red.

Se creará una LAN la cual nos facilitará la identificación de los equipos conectados a la red cuyo tráfico pasará por el firewall permitiendo monitorear y encontrar vulnerabilidades en caso de existir.

Para el servidor de correo se instalara la última versión de Zimbra que actualmente es la 8.7.0, se escogió este servicio por su ambiente gráfico que es amigable con el usuario final para su fácil utilización, ya que proporciona una experiencia basada en navegador permitiendo conectarse de forma segura y sin problemas a sus cuentas.

Tanto al personal administrativo como docente se le crearan cuentas de correo, y debido a que hay dos jornadas laborales, se procederá a agrupar las cuentas con la finalidad de que sea más fácil identificar a que institución pertenece.

Con un correo institucional se estandarizará en cuanto a los nombres de las cuentas eliminando así el uso de correos personales que muchas veces tienen nombres no adecuados como medio de comunicación oficial de esta empresa.

Una de las ventajas del servidor de correo es que actualmente muchos de los padres de familia trabajan en oficina y diariamente revisan su correo electrónico, es por eso que los docentes y personal administrativo tendrán la facilidad de enviar comunicados y obtener una pronta respuesta de los mismos.

El sitio web permitirá informar sobre la comunidad educativa y publicar comunicados generales que requieran ser de conocimiento por los padres de familia.

Para permitir el acceso desde cualquier parte hacia el correo institucional y el sitio web se va a contratar un dominio durante 5 años, pasado de ese tiempo la empresa decidirá si renovar o no el contrato del mismo.

Todos los equipos involucrados en este proyecto se conectarán a un UPS, el cual generará un tiempo de respaldo en caso de que haya cortes imprevistos de energía.

OBJETIVOS DE LA INVESTIGACIÓN

OBJETIVO GENERAL

Analizar y proponer soluciones a los problemas que existen actualmente en la comunidad educativa ESNUALSA S. A.; en el área de acceso a internet, correo, comunicación electrónica y actualización del sistema CCTV.

OBJETIVOS ESPECÍFICOS

- Actualizar el sistema de CCTV, reemplazando el cableado, cámaras dañadas e incluyendo nuevas.
- Implementar un servidor firewall que permita segmentar el ancho de banda disponible para los diversos usos.
- Aplicar las políticas de filtrado de tráfico que permitan restringir páginas no adecuadas durante la jornada educativa.
- Implementar un servidor de correo institucional que brinde mayor seguridad al momento de recibir o enviar información importante de las instituciones.
- Diseñar un sitio web que sirva como medio informativo.
- Contratar un dominio que permita acceder al correo institucional y al sitio web.
- Adecuar un espacio físico para la ubicación de los equipos de telecomunicaciones.

JUSTIFICACIÓN E IMPORTANCIA

Este proyecto tiene como finalidad corregir y mejorar todos aquellos problemas que se han evidenciado durante la realización de una investigación previa en las instalaciones de la comunidad educativa ESNUALSA S.A.

Mejorar el grado de seguridad dentro de las instalaciones, es una de las problemáticas a la que se dará solución ya que actualmente la seguridad constituye una parte fundamental sobre todo en las instituciones educativas.

La implementación de un sistema de cámaras de vigilancia, hoy en día es uno de los métodos de uso más frecuente que ayuda a realizar el respectivo monitoreo y control, no solo de sucesos que se den entre estudiantes dentro de la comunidad

educativa sino también cuidar las instalaciones de la misma y así transmitir un ambiente de confiabilidad a padres de familia.

El envío/recepción de información relevante a través de la web debe ser realizada por un medio propio y seguro, el cual permita identificar fácilmente al emisor/receptor de un correo.

Con la implementación de un servidor de correo institucional, el manejo de la información será más organizado al momento de transmitirla ya que las cuentas para todo el personal administrativo y docente se crearan bajo una estandarización en cuanto a nombres.

El avance de la tecnología y la introducción de medios de comunicación digital a nuestro entorno, ha permitido a la sociedad tener acceso a la información de forma rápida a través de sitios web.

Los medios digitales, hoy en día son los más utilizados para transmitir información gracias al fácil acceso que se tiene al internet y las instituciones educativas también hacen uso de este recurso, ya que es más factible que los padres de familia tengan conocimiento por este modo sobre las actividades próximas a realizarse dentro del establecimiento que un comunicado físico enviado en el diario escolar.

Dentro de una institución la organización de los equipos de cómputo es indispensable para lo cual la mejor manera de lograrlo es mediante el diseño de una red LAN.

Mantener el control de las actividades de un equipo es tarea de los servidores, y más aún cuando se cuenta con internet, medio que muchas veces es mal utilizado y es ahí donde actúa un servidor firewall, controlando el ancho de banda para los usuarios o servicios determinados y a su vez protegiendo de ataques informáticos provenientes del exterior.

CAPÍTULO II

MARCO TEÓRICO

ANTECEDENTES DEL ESTUDIO

ESNUALSA S.A ubicada en la Alborada 11ava etapa mz. 11 - 46 del 1 al 10, en las calles Isidro Ayora y Benjamín Carrión, es una comunidad educativa cuya labor es formar estudiantes.

Hace mucho tiempo ESNUALSA ha venido presentando problemas en ciertos puntos que son:

- Sistema de seguridad
- Uso del internet
- Emisión de comunicados

Cuya solución está relacionada con la tecnología, se ha realizado investigaciones previas sobre casos similares, las cuales sirvieron de guía para la implementación de este proyecto.

En el 2014 en la Carrera de Ingeniería en Sistemas y Networking de la universidad de Guayaquil, se llevó a cabo un proyecto que consistía en el diseño e implementación de un sistema de seguridad y monitoreo, debido a diversos inconvenientes que se presentaron muchos de ellos relacionados a los robos.

Este proyecto permitió tener un mayor control de las instalaciones, permitiendo monitorear inclusive áreas que se consideraban puntos ciegos, se utilizó la tecnología IP de las cámaras para que estas puedan ser visualizadas desde los equipos móviles.

Basándose en un proyecto de investigación que se realizó en la ciudad de Quito en el año 2012 sobre la implementación de un servidor virtualizado de correo electrónico utilizando ZIMBRA, se propuso implementar en esta comunidad de ESNUALSA además de un servidor de correo, un servidor web donde se podrá

publicar información que se considere importante para los representantes de los alumnos y puedan visualizarla desde cualquier dispositivo conectado a internet.

Según el levantamiento de información previo se pudo constatar que el equipo encargado de realizar la segmentación del ancho de banda no era el adecuado, y en base a esto se propone la implementación de un servidor firewall – proxy de manera que se pueda aprovechar de mejor manera el internet.

FUNDAMENTACIÓN TEÓRICA

SEGURIDAD

Proviene latín securitas, y este a su vez se deriva del verbo securus (sin precaución, sin cuidado, sin temor), y significa libre de cualquier tipo de daño o peligro.

La seguridad como término se la emplea en múltiples ámbitos y en este proyecto se enfoca en la seguridad electrónica la misma que hace referencia a sistemas de monitoreo, alarmas, softwares de seguridad para ser utilizados a fin de preservar y proteger la comunidad educativa.

SISTEMA DE SEGURIDAD

Es una herramienta compuesta por varios recursos que trabajan de manera conjunta para alcanzar un objetivo específico como es el de brindar la protección a personas, bienes materiales y propiedades sean estas públicas o privadas.

Con el paso del tiempo los sistemas de seguridad han mejorado en conjunto con la tecnología de tal manera que el mercado nos ofrece una gran diversidad de alternativas y según la necesidad existente permite escoger el más idóneo.

Características de un sistema de seguridad

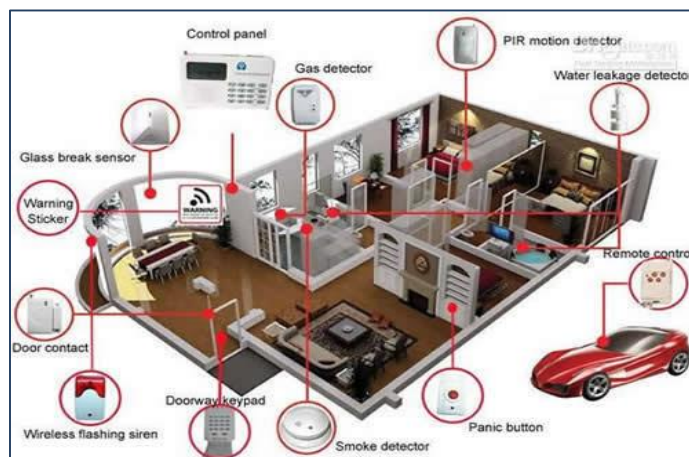
Para que un sistema pueda considerarse como seguro debe cumplir con las siguientes características:

- **Integridad:** hace referencia al estado de los datos, estos deben ser originales, toda la información captada por las cámaras y almacenada en el receptor correspondiente no podrá, bajo ningún contexto, ser modificada o alterada.

- **Confidencialidad:** el acceso a la información recopilada por los sistemas de seguridad, debe ser restringido, es decir serán datos secretos para el personal no autorizado.
- **Disponibilidad:** hace referencia al tiempo que un sistema debe estar disponible para su funcionamiento, al tratarse de un sistema de seguridad, la disponibilidad debe ser completa, ya que los sucesos pueden darse a cualquier hora del día y en cualquier segmento de todo el sector que abarca el sistema.

Tipos de sistema de seguridad

Gráfico N°1



Fuente: <http://www.inh.com.co>

Elaborado por: INH Technologies

Actualmente la mayoría de estos sistemas de seguridad hacen uso de cámaras para realizar el respectivo monitoreo, equipos para su debida configuración y almacenamiento de estos datos captados en forma de imagen o video.

Con el pasar del tiempo y el avance de la tecnología, estos sistemas han ido mejorando en conjunto con los equipos y componentes que los conforman, de tal manera que podemos encontrar en el mercado diferentes opciones.

- ✓ Sistemas de circuito cerrado de TV con VCR
- ✓ Sistemas de circuito cerrado de TV con DVR
- ✓ Sistemas de circuito cerrado de TV con DVR de red

- ✓ Sistemas de vídeo IP con servidores de vídeo

Para el presente proyecto, se hará la implementación de un Sistema CCTV con DVR.

Sistema de Circuito Cerrado de TV o CCTV utilizando DVR

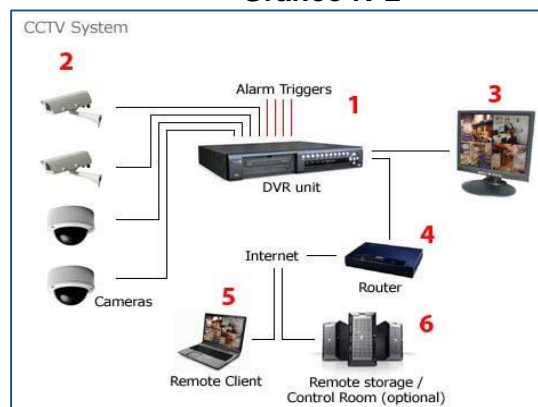
Sus siglas en inglés significan Closed Circuit Televisión que traducido al español es Circuito Cerrado de Televisión, y no es más que un conjunto de cámaras conectadas a un receptor en este caso un DVR, cuyas imágenes van a ser visualizadas a través de televisores o monitores.

El CCTV se compone de:

- Cámaras de Video
- Lentes
- Monitores
- Grabadores análogos y/o digitales
- Joystick
- Software de Gestión
- Cableado de video
- Cableado eléctrico
- Receptor (DVR)

Sistema de seguridad con DVR

Gráfico N°2



Fuente: www.ideasparapymes.com

Elaborado por: Ideas para PYMES

Beneficios de un Sistema de seguridad de CCTV

- ✓ Incrementa la seguridad de las personas que se encuentran dentro del perímetro monitoreado por el Sistema de CCTV.
- ✓ Disminuye considerablemente la realización de acciones que vayan en contra de las leyes como lo son crímenes, hurtos y daños a la propiedad privada.
- ✓ Representan una herramienta muy útil y necesaria para generar posibles evidencias para realizar un seguimiento de algún suceso dado.

CÁMARAS DE SEGURIDAD

Una cámara de seguridad o video vigilancia es una herramienta vital en cualquier instalación ya que se encarga de captar toda la actividad que ocurra en los perímetros donde se encuentra instalada.

Actualmente existen diversos tipos de cámaras, y según la tecnología utilizada se las puede clasificar en:

- **Cámaras Analógicas**

La imagen se obtiene de su lente y la señal de salida de video que emite es analógica, la cual se transmite a un equipo receptor de imágenes (DVR) en el cual se puede visualizar y realizar el monitoreo respectivo, además este equipo convierte la imagen analógica en digital con la finalidad de que se pueda visualizar desde otros dispositivos remotos siempre y cuando esté conectado a internet.

- **Cámaras Digitales**

Son aquellas cámaras que se encuentran unidas a la tecnología informática, necesitan de un computador para poder reproducir las imágenes y tener la facultad de transmitir las hacia el internet para que otros dispositivos puedan visualizarlas.

- **Cámaras de Red o IP**

Poseen un conmutador miniatura incluido permitiendo que los videos se puedan almacenar y emitir por si mismos además de la posibilidad de conectarse a internet o a una red LAN.

- **Cámaras PTZ**

PTZ proviene del acrónimo *pan-tilt-zoom* Son cámaras móviles, rotan alrededor de dos ejes, uno vertical y otro horizontal, a su vez permite enfocar un objeto o área determinada mediante el zoom.

DVR

Significa Digital Video Recorder traducido al español es Grabadora de vídeo digital. Este equipo permite capturar lo que visualiza la cámara y lo envía en formato digital al disco duro comprimiéndolo para almacenar la mayor cantidad posible de imágenes en un día.

Salvador (2014) “**DVR desde 4, 8, 16,32 canales de vídeo también cuentan con canales de entrada de audio y/o alarma también podemos controlar una cámara PTZ como también tiene salidas de vídeo (VGA, HDMI, BNC)**” (párr.2)

SERVIDOR

Es un componente informático ubicado dentro de una red y su función es la de proveer servicios a los equipos clientes. Un servidor puede ser:

- **Software:** Capaz de atender las diferentes peticiones de los clientes mediante una aplicación que se pueda ejecutar en cualquier tipo de computadora.
- **Hardware:** Es el equipo físico en donde se alojarán los distintos servicios que se requieran en un determinado lugar.

Existen algunos tipos de servidores que cumplen una función determinada, entre estos se pueden mencionar los siguientes:

- **Servidores de archivos:** Se encargan de almacenar toda clase de archivos, los mismos que van a ser utilizados en cualquier momento por los usuarios que se encuentren conectados a la red.
- **Servidores de correo:** Son aquellos que se encargan de prestar servicios de correo electrónico ya sea interno o también externo.

- **Servidor de impresión:** Es aquel equipo en el que se conectan las impresoras para que funcionen en red, y se pueda mantener un control de las impresiones que realizan los distintos usuarios. A través de este servidor se trabaja con cualquier impresora como si estuviese conectada directamente a la computadora del usuario final.
- **Servidor de base de datos:** Es considerado el más importante ya que contiene toda la base de datos que una empresa necesita para poder utilizar su sistema interno.
- **Servidor web:** Este servidor se encarga de almacenar toda la información que contienen los sitios web a los cuales se puede acceder mediante internet.
- **Servidor de fax:** En la actualidad de muy poco uso ya que fueron desplazados por los servidores de correo, pero su función es la de realizar todas las actividades necesarias para el envío, recepción y almacenamiento de los faxes.
- **Servidor del acceso remoto:** Este se encarga de permitir que se pueda administrar la red o alguno equipo conectada a la misma mediante el uso de internet desde cualquier lugar externo.
- **Central Telefónica:** Este servidor permite crear extensiones telefónicas para una comunicación interna, y también poseen configuración para comunicarse con el exterior.

VIRTUALIZACIÓN

Es una tecnología que permite crear versiones virtuales de algún recurso tecnológico como es el caso de los software, aprovechando los recursos de un equipo físico que permite ejecutar varias aplicaciones y sistemas operativos de manera simultánea.

La virtualización simula mediante un software la presencia de un hardware.

InformationWeek (s.f.) Dice: **“Es una opción simple para los departamentos de TI que desean implementar las herramientas más sofisticadas de administración y migración de máquinas virtuales. Es VMware.”** (párr. 1)

La virtualización genera ahorros significantes en cuanto a costos, al mismo tiempo que aumenta la agilidad, flexibilidad y escalabilidad de TI.

IBM fue quien empezó a implementar la virtualización, como una forma lógica de particionar computadores centrales en máquinas virtuales totalmente independientes.

En la década de los 80 la virtualización fue abandonada ya que se encontraron ciertas limitaciones como las siguientes:

- Bajo uso de la infraestructura.
- Incremento en cuanto a costo de las infraestructuras físicas.
- Insuficiencia en cuanto a protección ante desastres y fallas.
- Mantenimiento elevado de los escritorios del usuario final.

Otros autores manifiestan que:

El objetivo de la virtualización es tener uno a varios sistemas operativos sobre uno ya existente, permaneciendo este sin verse afectado y pudiendo arrancarlos de manera independiente a diferencia de la instalación en el mismo equipo gracias a una capa de software llamada Virtual Machine Monitor o VMM que crea una capa de abstracción entre el equipo físico o host y el software del sistema operativo de la máquina virtual o guest

(Guerrero, 2011, p.11)

Virtualización Gráfico N°3



Fuente: www.niux.com.ar

Elaborado por: NiuX Servicios Informáticos

Cuando se utiliza la virtualización se deben considerar los siguientes factores: la reducción considerable de costos, las inversiones de las TI mejoran, mayor flexibilidad en cuanto al uso del hardware, reducción de los gastos operativos, el consumo de energía también se reduce, se tiene una mayor eficiencia en cuanto a los recursos informáticos, de manera más ágil y centralizada se puede gestionar y administrar los recursos, la capacidad de los servidores aumentarán entre un 16 y 80 por ciento dependiendo de las características físicas que estos tengan.

Ventajas y desventajas de la virtualización

Ventajas

- Fácil incorporación de recursos de hardware nuevos para las máquinas virtuales.
- Reducción en cuanto a costos de mantenimiento y consumo eléctrico.
- Aislamiento, si una máquina virtual tiene problemas esta no afecta al resto.
- Administración global centralizada y simplificada.
- Mejora en cuanto a reducción del costo total de propiedad y retorno de inversión.
- Mejora en cuanto a procesos de clonación y copia de sistemas.
- Rápida incorporación de recursos nuevos para máquinas virtualizadas.

- Proporciona un consumo homogéneo de recursos para ser óptimo en toda la infraestructura.

Desventajas

- El rendimiento no es el mismo comprándolo con un equipo físico.
- En caso de fallo del disco duro se perderán las máquinas virtuales.
- En caso de robo del equipo físico donde se almacenan las máquinas virtuales, se perderán las mismas.

Tipos de virtualización

Existen los siguientes tipos de virtualización:

- **Virtualización a nivel de Sistema Operativo**

Este tipo de virtualización permite abstraer los servicios del Sistema Operativo, para proveer de un entorno virtualizado a las aplicaciones nativas.

Para permitir crear múltiples instancias virtualizadas, este tipo de virtualización se provee por el kernel de un único sistema operativo.

- **Paravirtualización**

Esta técnica consiste virtualizar diferentes sistemas operativos por software, como si fuesen un equipo independiente, las mismas que deben ser soportadas por un sistema operativo que actúa como hypervisor.

- **Virtualización completa**

Algunos autores manifiestan que:

Es conocida como virtualización completa. En esta virtualización el host emula lo suficientemente bien el hardware como para que los guests puedan ser ejecutados de forma nativa, es decir, sin cambios en el kernel y además de forma completamente aislada. Se pueden ejecutar varios guests en la misma máquina y compartir eficientemente sus recursos. (Ayoví, 2013, p.34)

VMware vSphere

Es una plataforma de virtualización que permite a los administradores de IT mantener un control mejorado sobre los ambientes virtuales en comparación con otras plataformas.

En el documento de “VMware vSphere” (s.f.) dice: **“VMware vSphere es la plataforma de virtualización líder del sector para construir infraestructuras en la cloud. Permite a los usuarios ejecutar aplicaciones críticas para el negocio con confianza y responder con mayor rapidez a las necesidades empresariales.”**(párr.1)

¿Cómo utilizar vSphere?

Consolidar y optimizar el hardware de TI: Permite consolidar en máquinas virtuales costosos proyectos de expansión de los centros de datos, en un solo servidor físico.

Mejorar la continuidad del negocio: Reduce los costos y la complejidad en la que se encuentre el negocio, una de sus funciones es estar disponible para la recuperación ante desastres.

Simplifica las operaciones de TI: Permite reducir drásticamente las sobrecargas operativas que existan por entornos de desarrollo de TI en producción.

Proporciona cloud computing: Esto se refiere a que vSphere siendo una plataforma de virtualización, permite a los usuarios disfrutar de servicios por medio de la red sin que su utilización represente un riesgo para los mismos.

Principales servicios que ofrece vSphere

- **vSphere Storage API:** ofrece una aplicación de almacenamiento que combina las diferentes tecnologías actuales para la protección de datos siempre y cuando estos sean compatibles con la plataforma de virtualización vSphere.

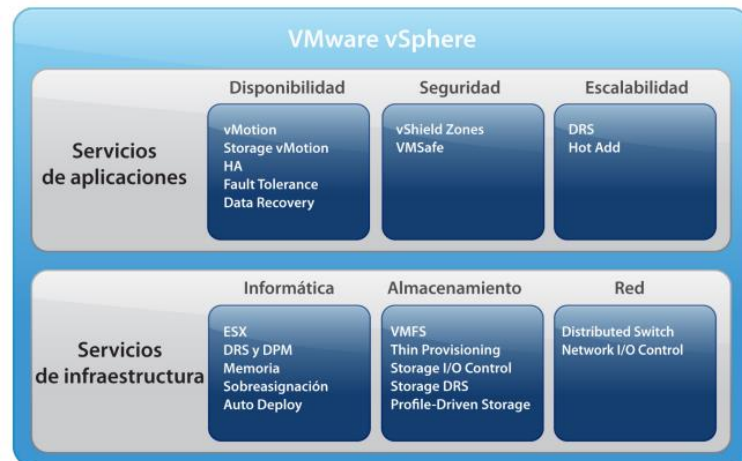
- **La arquitectura de hipervisor VMware vSphere ESXi™:** ofrece a sus clientes el servicio de virtualización con alto rendimiento permitiendo que varias máquinas virtuales hagan uso de los recursos de hardware al mismo tiempo y que su productividad sea igual o superior al nativo.
- **vSphere Storage Thin Provisioning:** asigna en forma dinámica la capacidad de almacenamiento, el cual es compartido entre las diversas máquinas virtuales creadas, lo que facilita a sus clientes implementar una estrategia de almacenamiento y reducir costos del mismo.
- **vSphere Storage Virtual Machine File System (VMFS) 5:** permite el acceso a los diferentes dispositivos de almacenamiento que se encuentran como compartidos para las diferentes máquinas virtuales.
- **El hardware virtual de VMware:** está apto para soportar 1 TB de RAM y gran variedad de hardware de próxima generación, como los procesadores de gráficos 3D o los dispositivos USB 3.0

Servicios de aplicaciones

- **VMware vSphere vMotion:** permite realizar la migración de las máquinas virtuales entre servidores sin pausar o interrumpir el funcionamiento de los mismos evitando molestias en el trabajo de los usuarios y evitando pérdidas de información o servicio.
- **VMware High Availability (HA)** en caso de que se dé un fallo de S.O. o hardware, vSphere realiza el reinicio de todas las aplicaciones automáticamente en el menor tiempo posible.
- **La conexión en caliente** permite realizar la conexión o desconexión de los diferentes dispositivos virtuales que sirve de almacenamiento o de red sin tener que establecer un tiempo de inactividad para realizar dicha conexión/desconexión, es decir se lo puedo realizar mientras el equipo está en funcionamiento.

- **La ampliación en caliente de discos virtuales:** al igual que los anteriores servicios, este permite agregar más almacenamiento virtual en pleno funcionamiento.

**VMware vSphere
Gráfico N°4**



Fuente: www.vmware.com

Elaborado por: VmWare

SISTEMA OPERATIVO

Es aquel software básico necesario que posee un dispositivo o equipo, que permiten la utilización de otros programas denominados aplicaciones.

El sistema operativo es el encargado de crear vínculos entre las aplicaciones, recursos y el usuario.

Entre sus principales características están:

- Fijar una interfaz para el usuario.
- Distribuir el hardware entre los usuarios.
- Compartición de datos entre usuarios.
- Facilitar de entrada/salida.

Fernández (2005) Dice: **“El SO debe estar pensado para manejar dispositivos que están limitados en hardware, es decir, aquellos sistemas con poca cantidad de RAM, flash, procesamiento, interfaces, entre otros.”** (p.19)

Tipos de Sistemas operativos

Los sistemas operativos se clasifican según:

- **El número de tareas:** Estos pueden ser Monotareas y Multitareas.
Monotarea: Son aquellos que permiten la ejecución de una sola aplicación o proceso en el sistema operativo, sin atender ningún otro hasta que el primer proceso finalice. Un ejemplo claro es el DOS o consola.
Multitarea: Permiten ejecutar varias aplicaciones o procesos en el mismo sistema operativo utilizando un algoritmo de planificación asignando una pequeña cantidad de tiempo a cada proceso.
- **El número de usuarios:** Se clasifican en Monousuarios y Multiusuarios.
Monousuario: Independiente de los procesos y números de procesadores que tenga, sistema operativo solo permite un usuario a la vez.
Multiusuario: Este tipo de sistema operativo permite interactuar a varios usuarios en una misma máquina.
- **El número de Procesadores:** Son Uniprocador y Multiprocador
Uniprocador: Permiten el uso de un solo procesador independiente de la cantidad de usuarios y tareas que se ejecuten.
Multiprocador: Permite la utilización de varios procesadores al mismo tiempo, sin importar cuantos procesos se ejecuten o el número de usuarios trabajando a la vez.
- **La Forma de ofrecer sus servicios:** Estos son Sistemas Operativos de red y Sistemas Operativos Distribuidos.
Sistemas Operativos de Red: Son aquellos que pueden interactuar con los demás sistemas operativos de otras máquinas utilizando cualquier medio de comunicación con la finalidad de compartir información.
Sistemas Operativos distribuidos: Son aquellos que permiten integrar los distintos recursos disponibles como, unidades de respaldo, impresoras, memorias, etc. en una sola máquina virtual, que será transparente para el usuario, y podrá hacer uso de estos como si estuviese utilizando un equipo local.

Sistemas Operativos Propietarios

Según la Fundación para el Software Libre (FSF) se aplica a todo aquel software cuyo uso, modificación o redistribución requiere un permiso por parte del titular del software, por lo tanto para su adquisición requieren de un costo.

Esparza (2013a) Dice: **“El software propietario, mala traducción de proprietary software, en inglés, también llamado privativo, privado, de código cerrado, cautivo o software no libre, es cualquier programa informático en el que el usuario tiene limitaciones para usarlo, modificarlo o redistribuirlo.”** (p.34)

Sistemas Operativos Libres

Son aquellos sistemas operativos que no buscan un lucro y se comparten libremente, su código es libre, es decir que cualquier persona puede colaborar con su aporte para su mejoramiento como es el caso de las distribuciones de Linux.

Esparza (2013b) Dice: **“Es la denominación del software que respeta la libertad de los usuarios sobre su producto adquirido y, por tanto, una vez obtenido puede ser usado, copiado, estudiado, modificado, y redistribuido libremente.”** (p.35)

GNU/Linux

Es un sistema operativo libre, basado en las distribuciones de UNIX, apareció en la década de los noventa y fue desarrollado por Linus Torvalds en la Universidad de Helsinki en Finlandia cuando aún era estudiante.

El núcleo de Linux fue inspirado en MINIX una distribución UNIX, y desde su primera versión oficial muchos programadores han contribuido a la construcción del sistema operativo funcional como lo es actualmente.

El principal objetivo es impulsar la distribución de un software libre junto a su código fuente para que cualquier persona pueda modificarlo a su antojo creando su propia distribución.

Miguez (2012a) Dice: **“Las distribuciones de Linux son paquetes de software que incluyen el Sistema Operativo Linux y unas aplicaciones, normalmente libres que permiten realizar prácticamente todas las tareas para las que está diseñado un ordenador.”** (p.6)

Sus principales características son:

- Libre: cuyo código fuente se encuentra disponible para su modificación
- Multiplataforma: Es posible su instalación en diversos dispositivos.
- Multiusuario: Varios usuarios pueden trabajar al mismo tiempo sobre él.
- Multitarea: Es capaz de realizar varias actividades.

CentOS

Cuyo significado es Comunnity Enterprise Operating System, es un sistema operativo open source basado en la distribución Red Hat Enterprise Linux, es diseñado como un software gratuito de clase empresarial al ser robusto, y fácil de utilizar e instalar.

Miguez (2012b) Dice: **“Típicamente los usuarios de CentOS son organizaciones e individuos que no necesitan el fuerte apoyo comercial para lograr el funcionamiento exitoso”** (p.8)

CentOS es un esfuerzo del software libre que se impulsa mediante una comunidad cuyo fin es centrarse en ofrecer un ecosistema de código abierto robusto.

A nivel de usuarios, CentOS ofrece una plataforma adaptable a una gran variedad de implementaciones.

A las comunidades que utilizan el código abierto, se les ofrece una base muy sólida para que junto a amplios recursos probar, lanzar y mantener su código.

Requisitos de hardware recomendado para operar:

- Sin entorno de escritorio
HDD: 1 – 2 GB Mínimo
Memoria RAM: 64MB Mínimo
- Con entorno de escritorio
HDD: 20GB mínimo – 40GB Recomendado
Memoria RAM: 1GB

En cuanto a procesador ambos entornos soportan las mismas arquitecturas:

- Intel x86-compatible (32 bit) (Intel Pentium I/II/III/IV/Celeron/Xeon, AMD K6/K7/K8, AMD Duron, Athlon/XP/MP).
- AMD64 (Athlon 64, etc.) e Intel EM64T (64 bit).

RED LAN

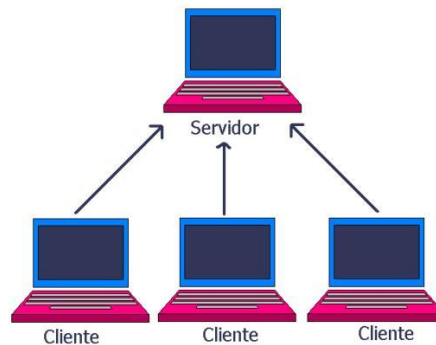
Cuyo significado Local Area Network, traducido al español es Red de Área Local, está conformada por la conexión de varios equipos informáticos entre sí, utilizando dispositivos físicos que permitan el transporte de información, en un área que no supere los 200m².

Las redes LAN se dividen en:

- **Cliente - Servidor:** se basan en conjunto de computadoras donde una será el servidor y el restante serán clientes, de tal manera que el servidor se encargará de ofrecer los distintos recursos utilizados por los clientes.

Cliente – Servidor

Gráfico N° 5

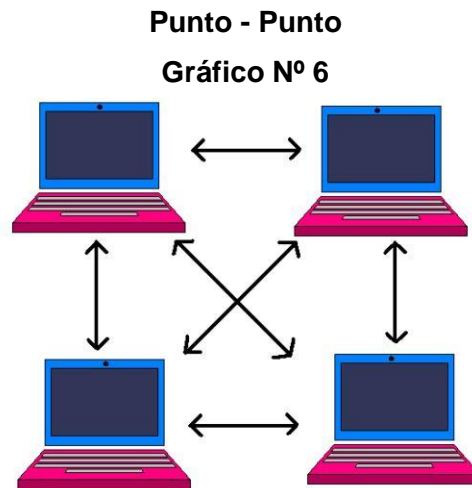


Fuente: <http://41dc.wikispaces.com>

Elaborado por: Wiki

- **Punto a Punto:** también denominadas redes igualitarias, se función es permitir que todas las computadoras hagan de cliente o de servidor no dedicado de tal manera que todas puedan compartir recursos disponibles dentro de la red, son más flexibles y económicas que las Cliente - Servidor

en cuanto a alta disponibilidad ya que si una de las computadoras llega a sufrir un desperfecto, la red no se verá afectada.



Fuente: <http://41dc.wikispaces.com>

Elaborado por: Wiki

TOPOLOGÍA

Las computadoras conectadas a la red se las denomina nodo, y la topología se define como la forma de conexión de los nodos para comunicarse y puede ser mediante la topología física o la topología lógica, dependiendo de la ruta que utilicen los datos para viajar de un nodo a otro.

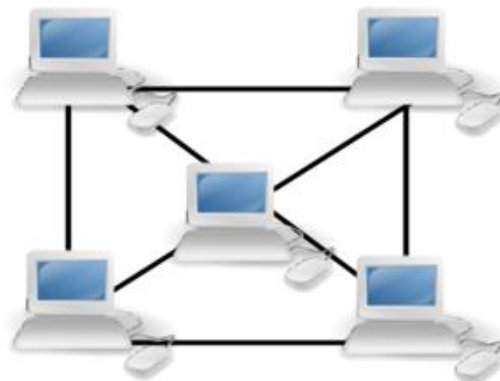
Existen cinco topologías posibles de red básicas o más comúnmente utilizadas que son:

- **Topología en Malla**

Se caracteriza por tener un enlace dedicado y punto a punto entre un dispositivo y otro, al usar este tipo de enlaces garantiza que solo transporte datos propios de los equipos conectado entre sí, eliminando inconvenientes surgidos por enlaces que se comparten por varios dispositivos. Es una topología robusta, en caso de que un enlace falle no se inhabilitará todo el sistema.

Topología en Malla

Gráfico N° 7



Fuente: <https://es.wikibooks.org/>

Elaborado por: Wikibooks

- Topología en Estrella

Los nodos se conectan mediante un enlace punto a punto dedicado con el dispositivo central o servidor no poseen conexión directa entre nodos por lo que a diferencia de la topología anterior si se desea enviar datos de un nodo a otro, todo el tráfico debe pasar por el dispositivo central y este debe indicar la ruta para que lleguen a su destino final.

Topología estrella

Gráfico N° 8



Fuente: <https://es.wikibooks.org/>

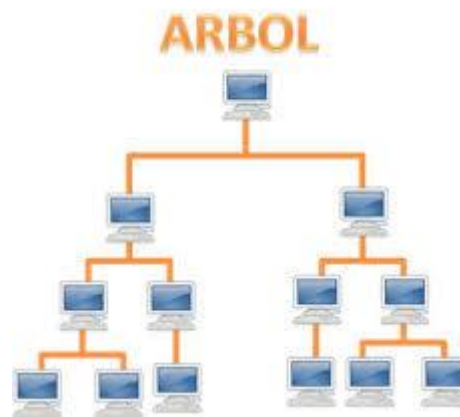
Elaborado por: Wikibooks

- **Topología en Árbol**

Es casi similar a la topología anterior, pero su variantes es que no todos los nodos se conectan al concentrador central directamente, la mayoría se conectan a un concentrador secundario y este a su vez tiene un enlace directo al concentrado central.

Topología en Árbol

Gráfico N° 9



Fuente: <https://redesinalambricasycableadas.wordpress.com>

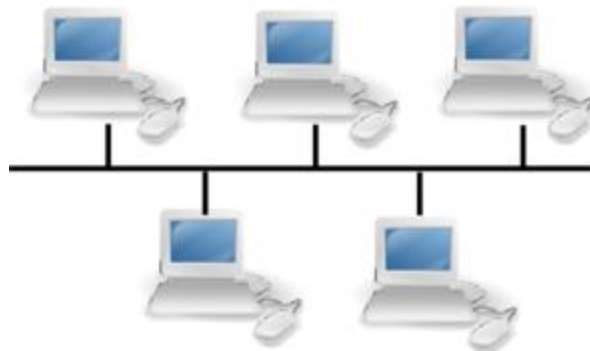
Elaborado por: Redes cableadas e inalámbricas

- **Topología en Bus**

Todos los nodos se unen en línea recta a un cable continuo o segmento, los datos se transmiten hacia todos los nodos conectados en esta red y por la forma de transmisión es que en los extremos debe existir un hardware que se denomina terminador el cual definirá el segmento actuando como límite. Entre más nodos hayan conectados la red será más lenta, este tipo de comunicación puede producir mucho ruido.

Topología en Bus

Gráfico N° 10



Fuente: <https://es.wikibooks.org/>

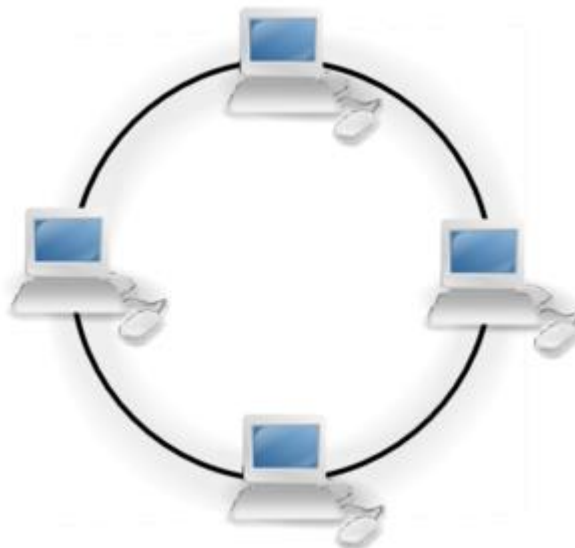
Elaborado por: Wikibooks

- Topología en Anillo

Los nodos se conectaban de forma circular con un cable, a diferencia de la topología anterior no existen terminaciones por lo que la señal viaja a través de cada equipo que hace las veces de repartidor de manera que la señal se amplifica y se envía al siguiente nodo

Topología en Anillo

Gráfico N° 11



Fuente: <https://es.wikibooks.org/>

Elaborado por: Wikibooks

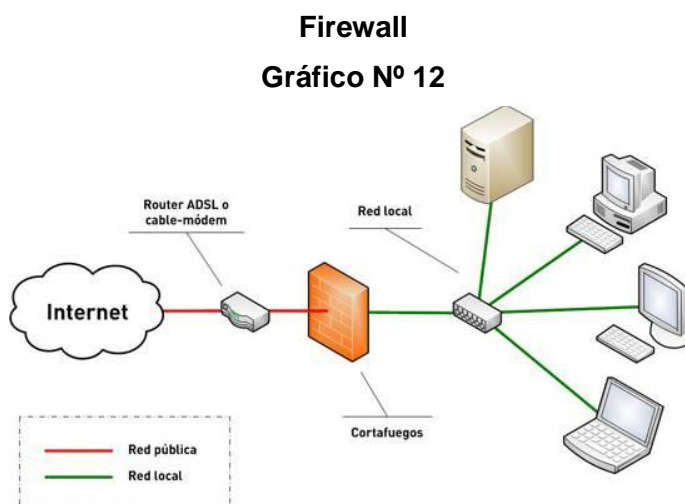
FIREWALL

Es aquel software o hardware que se encarga de proteger una red o un equipo, filtrando y/o bloqueando paquetes de datos que circulan por la red de intrusos o accesos no deseados que pueden sustraer información confidencial.

Normalmente el firewall se ubica en el punto de unión entre 2 redes la pública y la privada por lo tanto debe ser capaz de controlar todas las conexiones que se realizan a internet desde cualquier equipo, con el fin de evitar ataques informáticos.

Ciertos autores manifiestan que:

Un cortafuego es una máquina segura y confiable que se asienta entre una red privada y una red pública. La máquina cortafuegos se configura con un conjunto de reglas que determinan a que tráfico de red se le permitirá pasar y cuál será bloqueado o rechazado. (Esparza, 2013c, p.58)



Fuente: <http://geekland.eu/>

Elaborado por: Geekland

Tipos de Firewall

Tradicionalmente los firewall son hardware, en otras palabras un equipo físico instalado dentro de una red para protegerla del exterior, por lo general este tipo de firewall se lo utiliza en entornos profesionales, mientras que los cortafuegos

personales son a nivel de software, filtrando todo el tráfico entrante y saliente de la computadora.

Los cortafuegos presentan unas ventajas notorias como lo son:

- **Proteger de intrusos:** Permite el ingreso a la red solo a las personas autorizadas basándose en políticas configuradas.
- **Optimizar el acceso:** Permite identificar todos los elementos que se encuentran en la red interna, posibilitando a su vez optimizar la comunicación directa entre ellos.
- **Proteger la información privada:** Brinda accesos a los usuarios que posean privilegios a información de determinadas áreas o sectores de red.
- **Protección de virus:** Impide que la red se contamine de virus que intenten atacar.

Algunos autores manifiestan que:

Aunque el usuario medio pueda creer que los ataques no es algo que le pueda suceder en su casa a su computadora, el cortafuego se convierte en un elemento imprescindible si se utiliza el ordenador y se está conectado permanentemente mediante ADSL o cable. (Esparza, 2013d, p.60)

Filtrados del Firewall

A Nivel de paquetes: Este tipo de filtrado analiza la información que se encuentra en las cabeceras de los paquetes IP con la finalidad de decidir si rechazar o permitir el paso de las tramas que se reciben. Quienes conforman este tipo de filtrado son, las direcciones IP fuente y destino, el puerto destino TCP/UDP y el paquete que se va a transportar

A Nivel de Aplicaciones: Se caracteriza por el bloqueo total del tráfico IP entre el internet y la red interna, los usuario locales deben establecer una conexión hacia afuera pasando por el cortafuegos y el servidor proxy. Se ofrece un nivel de seguridad más alto

A nivel de conexión: Controla la conexión entre un cliente y el servidor, actuando de manera transparente.

PROXY

Es un servidor cuya función es la de ser intermediario entre las peticiones que realiza un determinado usuario desde un navegador y el internet.

Al ingresar hacia un determinado sitio web con frecuencia, se puede mejorar los tiempos de acceso, al guardarlos en la caché.

Otros autores expresan que:

Los servidores proxy se han convertido en una herramienta indispensable en casi todo entorno donde es necesario distribuir una conexión de internet para navegación y acelerar al mismo tiempo la velocidad de navegación de los clientes, así como para implementar el filtrado de acceso por varios criterios como: tiempos (horarios), URLs, direcciones, dominios, entre otras.

(León, 2012, p.11)

Webmin

Es una interfaz web que sirve para la administración de un sistema operativo Linux, eliminando la necesidad de editar manualmente todos aquellos archivos de configuración de Unix como, y permitiendo administrar un sistema de forma remota o desde consola.

Características:

- Programada en Perl.
- Permite añadir fácilmente funcionalidades nuevas.
- Permite la configuración de aspectos internos de muchos sistemas operativos, entre ellos los usuarios, espacio, servicios, etc.
- Posee licencia BSD

Webmin se construye a partir de módulos, que poseen una interfaz para configurar los archivos y el servidor, facilitando adicionar funcionalidades nuevas sin mayor esfuerzo. Permite mantener el control de varias máquinas por medio de una

interfaz simple, o iniciar la sesión en otros servidores iguales que se encuentren dentro de la misma red local.

Webmin
Gráfico N° 13



Fuente: <http://www.deacosta.com/>

Elaborado por: David E. Acosta

CORREO ELECTRÓNICO

Es uno de los tantos servicios que ofrece el internet de manera gratuita, por medio del cual se puede recibir y enviar mensajes con cualquier tipo de contenido.

El esquema de enlace que utiliza es asíncrono ya que no necesita una conexión previa entre el emisor y receptor para poder transmitir.

Su funcionamiento es similar al de un correo postal, ya que los dos permiten recibir y enviar mensajes, los mismos que llegan a destino por medio de una dirección.

Las direcciones de correo electrónico tienen la particularidad de que incorporan el arroba (@) con la finalidad de separar el nombre de usuario y el servidor al que pertenece, esto fue creado por el estadounidense Ray Tomlinson, cuya idea era la de usar un símbolo que se encuentre en todos los teclados pero que no sea parte de los nombres de la empresas o nombres propios de personas.

Zimbra

Es un sistema informático desarrollado en código libre que ofrece servicios integrados de mensajería, mostrando un servicio de correo electrónico de alto rendimiento y confiable.

Padilla (2012a) dice: **“Zimbra es la solución líder para correo electrónico y calendario de código abierto para empresas, proveedores de servicios, instituciones académicas y gubernamentales.”** (p.38)

Aporta con nuevos módulos que sirven para almacenar todo tipo de documentos, inclusive empezar una sesión de chat con otros contactos, permite también crear contenido dentro del calendario, tareas, contactos, etc.

Algunos autores manifiestan que:

En la actualidad Zimbra se ha convertido en una solución de código abierto líder a nivel para todo tipo de empresa como para proveedores de servicio, centros educativos y administraciones públicas. Su éxito se basa en el uso de tecnologías de código abierto y protocolos de comunicación e intercambio de datos estándares. (Padilla, 2012b, p.44)

Zimbra se creó a finales del 2003 orientado a ser un programa de correo electrónico, su primer prototipo fue desarrollado de manera rápida.

Mediante código libre disponible a través de toda la web, lograron ensamblar un sistema básico y en honor a una canción estadounidense del grupo Talking Heads lo bautizaron como Zimbra.

Al desarrollarse en código abierto fue publicado en internet para que varias personas lo vean, emitan sugerencias y colaboren con su aporte, gracias a esto el proyecto evolucionó, en 2005 se lanzó el producto comercialmente ofreciendo un descuento debido a que el mercado se encontraba dominado por Microsoft.

Zimbra utiliza los siguientes proyectos de código abierto:

- MySQL
- Postfix
- OpenLDAP
- Apache Tomcat
- Lucene
- Verity
- ClamAV
- SpamAssassin

- AMaViS y Amavisd-new
- DSPAM
- Aspell
- Apache James
- Sieve
- Perdition mail retrieval proxy
- nginx, desde la versión 5.0

Se basaron en SOAP para la interfaz de programación de aplicaciones, y también actúa como servidor POP3 e IMAP.

SITIO WEB

Es aquel espacio virtual alojado en internet, el cual se compone de un conjunto de páginas web a las que se puede acceder desde un dominio, y su función es la de ofrecer productos y/o servicios, vender y/o publicitar, informar, entretener, etc. con contenidos, al resto del mundo, muchos de estos lo muestran de manera gratuita y otros mediante una suscripción.

Siguencia (2012) Dice: **“Su objetivo es el de servir de puerta de entrada única para ofrecer al usuario, de manera fácil el acceso a múltiples servicios, recursos, aplicaciones desde un mismo lugar”** (p.22)

Características

En cuanto a la usabilidad los sitios web deben brindar a los usuarios las siguientes características:

- **Eficiente:** Todos los elementos que lo componen deben ser utilizados de manera correcta.
- **Rapidez:** El contenido no debe entorpecer la fluidez del sitio web.
- **Uso Fácil:** Su interfaz debe ser amigable con el usuario.
- **Utilidad:** Cada uno de los elementos que lo componen deben ser de uso, basándose en los objetivos que se plantean.

- **Intuitivo:** Los elementos que lo conforman se deben relacionar con la percepción del usuario final, para que este solo con visualizar sepa lo que debe hacer.

Wordpress

Ciertos autores expresan que:

WordPress es un software que puedes utilizar para crear fantásticas webs, blogs o aplicaciones. Nos gusta decir que WordPress es, al tiempo, gratis y de un precio incalculable. Dicho de forma sencilla, WordPress es el sistema que utilizas cuando deseas trabajar con tu herramienta de publicación en lugar de pelearte con ella. (Wordpress, s.f., párr.1)

Wordpress
Gráfico N° 14



Fuente: <https://wordpress.org>

Elaborado por: Wordpress

Wordpress es un CMS cuyo significado en inglés es Content Management System, traducido al español quiere decir Sistema de Administración de Contenidos, en sus inicios en el año 2003 comenzó siendo una plataforma de blogging y con el pasar de los años se ha convertido en una poderosa herramienta de fácil uso para crear páginas o blogs.

Es un software de código abierto y se encuentra disponible en su sitio web (WordPress.org) para ser descargado e instalado en cualquier dominio.

Wordpress es utilizado para lo siguiente:

- Tiendas virtuales
- Sitios web tradicionales
- Páginas corporativas
- Cartas de venta, etc.

Este software contiene 3 importantes componentes que lo convierten en una herramienta muy poderosa, estos son:

- Temas
- Plugins
- Widgets

Temas

No son más que plantillas con diseños modificables para mejorar la apariencia del sitio web, en la actualidad existen una infinidad de temas creados por usuarios que son gratuitos, mientras que otros son realizados por empresas y tienen un costo mínimo para su uso, estos son considerados “premium” ya que ofrecen más opciones de personalización y diseño.

Plugins

Son pequeños complementos que sirven para aumentar las capacidades de Wordpress, convirtiéndolo en un sistema flexible, al igual que las plantillas estos suelen ser en su mayoría gratuitos y otros tienen un costo.

Widgets

Son aquellos bloques en los que se pueden añadir información aprovechando los Sidebars (espacio en desuso), permitiendo que los usuarios tengan un mayor control sobre el contenido y el diseño del sitio web. La cantidad de estos dependen del tema que se haya escogido.

DOMINIO DE INTERNET

Es un nombre único que se proporciona a una empresa, organización, persona, etc. de manera que el ser digitado mediante un navegador, en su mayoría muestra todo el contenido de un sitio web.

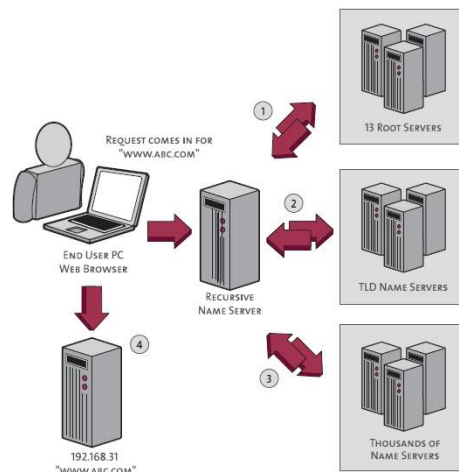
Al ser único se relaciona con una dirección IP, esta debe ser pública y es asignada por el proveedor de internet.

La principal función de un dominio es la traducción de direcciones IP de los nodos activos en la red, en términos que se puedan memorizar y sean muy fáciles de encontrar.

Un dominio está compuesto por el nombre de la organización y el tipo de organización, los más comunes son .com, .net y .org.

Dominio e internet

Gráfico Nº 15



Fuente: <http://web-gdl.com/>

Elaborado por: Web-Gdl

FUNDAMENTACIÓN SOCIAL

Según el artículo 14 de la sección segunda del buen vivir, La educación se centrará en el ser humano y garantizará su desarrollo holístico, en el marco del respeto a los derechos humanos, al medio ambiente sustentable y a la democracia; será participativa, obligatoria, intercultural, democrática, incluyente y diversa, de calidad y calidez; impulsará la equidad de género, la justicia, la solidaridad y la paz; estimulará el sentido crítico, el arte y la cultura física, la iniciativa individual y comunitaria, y el desarrollo de competencias y capacidades para crear y trabajar.

El presente proyecto tendrá gran impacto en la comunidad educativa, solventando los inconvenientes que actualmente presenta.

Se ha determinado que uno de los principales puntos a resolver es el tema de seguridad y al no funcionar correctamente el sistema de monitoreo que se tiene actualmente, se corre el riesgo de que existan eventualidades que pongan en riesgo el bienestar de los estudiantes, de las cuales no se tenga respaldo alguno, de tal manera que se ha presentado una solución viable y es la de readecuar con nuevos equipos de seguridad las instalaciones, permitiendo además tener un respaldo que pueda ser utilizado en cualquier momento.

En la educación actual el uso del internet es uno de los requisitos que toda institución educativa debe brindar a sus estudiantes mediante la enseñanza de su correcta utilización, pero desafortunadamente estamos en una era tecnológica en donde el estudiante fuera de la comunidad educativa tiene un libre acceso al internet y puede realizar cualquier tipo de actividad, en muchos casos esta no es productiva ya que se enfocan en el constante uso de redes sociales, juegos online, etc.

En la comunidad educativa ESNUALSA muchos de los estudiantes se dedican a utilizar el internet del laboratorio como si estuviesen en su casa, y hasta cierto punto es perjudicial ya que no están participando de la clase además de que puede darse el caso de que ingresen a páginas cuyo contenido atente contra la moral e integridad de las personas, producto de los enlaces publicitarios que aparecen en las mismas, lo que a su vez genera malestar al personal administrativo que si necesita darle un correcto uso.

Otra de las propuestas es implementar un servidor firewall que permita tener un mayor control de estas actividades que realizan los estudiantes, bloqueando las páginas que no son necesarias para el aprendizaje y permitiendo únicamente aquellas que el docente apruebe como idóneas para el estudiante, procurando brindar la excelencia académica que se destaca en esta comunidad educativa.

Para la comunidad educativa de ESNUALSA es importante adquirir un medio de información por internet, es por eso que se implementará un servidor donde se alojará el sitio web cuyo contenido será informativo y además se implementará un correo institucional de tal manera que se deje de utilizar las cuentas de correo gratuitas

FUNDAMENTACIÓN LEGAL
CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR
CAPÍTULO SEGUNDO - SECCIÓN TERCERA
Comunicación e información

Art. 16.- Todas las personas, en forma individual o colectiva tienen derecho a:

2. El acceso universal a las tecnologías de información y comunicación.

RÉGIMEN DEL BUEN VIVIR
CAPÍTULO PRIMERO - SECCIÓN PRIMERA
Educación

Art. 347.- Será responsabilidad del Estado:

8. Incorporar las tecnologías de la información y comunicación en el proceso educativo y propiciar el enlace de la enseñanza con las actividades productivas o sociales.

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y
MENSAJES DE DATOS
DE LOS MENSAJES DE DATOS
CAPÍTULO I – PRINCIPIOS GENERALES

Art.10.- Procedencia e identidad de un mensaje de datos.- Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido del mismo, cuando

de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguientes casos:

- a) Si se hubiere dado aviso que el mensaje de datos no proviene de quien consta como emisor; en este caso, el aviso se lo hará antes de que la persona que lo recibe actúe conforme a dicho mensaje. En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y,
- b) Si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o hizo caso omiso de su resultado.

HIPOTESIS

La seguridad en la comunidad educativa ESNUALSA durante los últimos años se ha visto afectada al no contar con un sistema de CCTV actualizado y en funcionamiento, lo que implica el no poder llevar un control total de las posibles eventualidades que se den dentro de las instalaciones y que a su vez representa una dificultad para hacer los respectivos seguimientos del suceso al no contar con una evidencia física.

El envío/recepción de documentación o información perteneciente a las actividades de la comunidad educativa (ya sea este entre docentes y personal administrativo o institución educativa y padres de familia) se ha visto afectada debido a que no se cuenta con medios tecnológicos de información propios como lo son:

- Un sitio web donde pueden hacer públicos los comunicados y que estarán al alcance de los padres de familia. Dejando atrás esas publicaciones en carteleras dentro de la institución, ya que muchos de los estudiantes son retirados por expresos escolares y no por sus representantes legales.
- Un correo institucional que permita identificar de forma rápida quien es la persona que envía información y con quien se está compartiendo la misma, para evitar un mal manejo de esta.

El no contar con un servidor proxy y dar libre acceso a internet a los estudiantes de la comunidad educativa ha provocado que las actividades que realiza el personal administrativo se vea entorpecido, ya que muchas de estas tareas necesitan del uso del internet y al ingresar los estudiantes a ciertas páginas

indebidas acaparan la mayor parte del ancho de banda, lo que genera una lenta navegación en la web y a su vez representa un bajo rendimiento específicamente en la materia de computación ya que el estudiantado muestra poco o nulo interés en las clases y se entretienen visitando sitios web no recomendables y muchos de ellos con contenido que va en contra de la moral e integridad de las personas, productos de la publicidad o enlaces publicitarios.

VARIABLES

Variables
Cuadro Nº 3

| TIPO DE VARIABLE | VARIABLE | INDICADOR |
|------------------|---|---|
| INDEPENDIENTE | Actualización del sistema de CCTV | Instalación de equipos de seguridad y configuraciones necesarias. |
| | Creación de servidores WEB, CORREO y FIREWALL- PROXY | Implementación de equipo (servidor físico) Virtualización de servidores: web, correo y firewall - proxy |
| DEPENDIENTE | Mejora de la seguridad dentro de las instalaciones | Análisis y valoración de un mejor nivel de seguridad. |
| | Mejora de la comunicación entre personal administrativo, docentes y padres de familia | Publicación mediante sitio web oficial. Creación de cuentas y envío/recepción utilizando el correo institucional |
| | Uso correcto del internet y ancho de banda | Diagnóstico del acceso restringido a internet desde el laboratorio. Análisis y valoración de mejor velocidad al navegar por internet en oficina. |

Fuente: Datos de la Investigación

Elaboración: Andrés Del Pozo Espín – Johanna Hernández Páramo

DEFINICIONES CONCEPTUALES

CCTV: Es el sistema de seguridad que se va a implementar en el cual constan los dispositivos de transmisión y recepción, el medio de conexión, y la forma de visualización.

DVR: Es el equipo en el que se conectarán las cámaras y se encarga de almacenar todos los videos que sean captados por las mismas.

BALUN: Son los transformadores que se ubican en los extremos del cable y van para conectar las cámaras con el DVR.

UTP: Es el tipo de cable que se utilizará para conectar las cámaras.

CÁMARAS: Son los dispositivos que capturan las imágenes y van a ser almacenadas en el DVR para su posterior visualización.

SERVIDOR: Es el equipo físico robusto en el cual se ubicarán las máquinas virtuales, que aprovecharán todos sus recursos en hardware.

MÁQUINA VIRTUAL: Es una máquina con un sistema operativo que prestará un servicio al que se le asignará una determinada función y simulará ser un equipo físico.

CENTOS 7: Es el sistema operativo que se instalará en las máquinas virtuales.

FIREWALL: Es una máquina virtual encargada de filtrar todo tráfico que se genera, para proteger a la red LAN de posibles ataques informáticos.

PROXY: Es un paquete que se instala en el firewall, el cual se encargará de restringir ciertas conexiones a internet no deseadas.

FILTRADO: Término utilizado para separar unas conexiones de otras.

TRAFICO: Son los datos que circulan por el ancho de banda.

ANCHO DE BANDA: es el canal por donde se transfieren todos los datos de forma simétrica.

SEGMENTAR: Dividir el ancho de banda en varios canales para asignarlos a una determinada función.

SITIO WEB: Son las páginas web informativas que se publicarán a través de internet.

DOMINIO: Es el nombre que se utilizará para que puedan acceder al sitio web.

CORREO INSTITUCIONAL: Se refiere al servidor de correo que se está implementando.

ZIMBRA: Es un paquete que se instalará en una máquina virtual, el cual permitirá acceder al correo institucional mediante una aplicación.

IP PÚBLICA: Es una dirección IP que asigna el proveedor de internet para poder ubicar el dominio.

INTERNET CORPORATIVO: Es un servicio de internet que se ofrece para empresas, el cual goza de mayores beneficios que un internet residencial.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

DISEÑO DE LA INVESTIGACIÓN

Modalidad de la investigación

En el presente tema de tesis “IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD CCTV Y VIRTUALIZACIÓN DE SERVIDORES FIREWALL-PROXY, CORREO Y WEB PARA LA UNIDAD EDUCATIVA ESNUALSA” se ha planteado una solución que ayudará a satisfacer las necesidades que se han explicado anteriormente

Está enmarcado como un Proyecto Factible, debido a que esta propuesta se basa en una solución tecnológica informática, ajustándose a las necesidades de la comunidad educativa ESNUALSA.

Tipo de investigación

El tipo de investigación de campo se basa específicamente en la observación directa del lugar donde se están dando los diferentes sucesos que dan origen al problema.

Otros autores manifiestan que:

La investigación de campo es aquella que consiste en la recolección de datos directamente de los sujetos investigados o de la realidad donde ocurren los hechos (datos primarios) sin manipular o controlar variable alguna, es decir, el investigador obtiene la información pero no altera las condiciones existentes.

De allí su carácter de investigación no experimental.

(Arias, 2012, p31)

Este tipo de investigación para obtener los datos, se ayuda de técnicas como la encuesta, la entrevista, observaciones entre otras. Puede describirse como el tipo de investigación más completa en lo que respecta a la recolección y organización de información documentada e inclusive basta con la información recabada por estos diferentes procedimientos, para darle validez a la investigación que se está realizando.

El presente proyecto se basa en esta clase de investigación, ya que se acude al lugar donde se origina la problemática y en el cuál se realizó un levantamiento de información, estableciendo un análisis de causa-efecto de la misma y aplicando encuestas al personal que labora en ambas instituciones como técnica de recolección de datos.

Culminado el proceso de obtención de datos y análisis de factibilidad, se puede proceder a la elaboración de una propuesta que mejore o dé solución a la problemática identificada.

Población y muestra

Una vez realizado el planteamiento del problema, establecidos los objetivos y delimitación del mismo, se procede a realizar un análisis para identificar cuáles son los elementos y/o individuos que se encuentran involucrados dentro del proyecto y que a su vez formarán parte de la investigación.

Lo que conduce a la definición de la población para el presente proyecto y de la cual se escogerá la muestra en caso de requerirse.

Algunos autores manifiestan que:

Una población está determinada por sus características definitorias. Por lo tanto, el conjunto de elementos que posea esta característica se denomina población o universo. Población es la totalidad del fenómeno a estudiar, donde las unidades de población poseen una característica común, la que se estudia y da origen a los datos de la investigación.

(Tesis de Investigación, 2011, párr.3)

Población

Como lo menciona Suárez (2011) la población es un “**conjunto de individuos al que se refiere nuestra pregunta de estudio o respecto al cual se pretende concluir algo**” (párr.1)

En el presente proyecto se ha determinado como población al personal docente y administrativo, quienes serán los beneficiados directamente con la realización del mismo.

Población
Cuadro N° 4

| POBLACION | CANTIDAD |
|-------------------------|----------|
| Personal administrativo | 9 |
| Personal docente | 31 |
| TOTAL | 40 |

Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández
Páramo

Muestra

Debido a que la población es pequeña en el presente proyecto, no se aplica muestreo para la recolección de datos, se utiliza a la población en su totalidad.

Instrumentos de recolección de datos

Técnica de investigación

La técnica de recolección de datos que se utilizará para el desarrollo del presente proyecto será la encuesta.

Encuesta

Es un conjunto de mecanismos y medios, comúnmente utilizada en la investigación de campo, se la puede considerar como un proceso interrogativo que se emplea para obtener datos sobre un determinado tema. Este procedimiento se lleva a cabo a través de la aplicación de un cuestionario a las

personas que se encuentran relacionadas directamente con la indagación que se está realizando.

Dicho cuestionario debe estar previamente elaborado con preguntas estratégicas que ayuden a recabar la información específica que se requiere conocer.

Esta técnica sirve para conocer las opiniones de los involucrados en una situación o problema.

Instrumento de investigación

El instrumento de investigación que se utilizará para la recolección de datos será el cuestionario.

El cuestionario es un conjunto de indicaciones y preguntas elaboradas para obtener los datos necesarios por parte de los encuestados, los cuales permiten cumplir con los objetivos planteados al inicio de una investigación y para la comprobación de hipótesis.

El cuestionario permite el análisis y tabulación de los resultados obtenidos en un tiempo relativamente corto.

Recolección de la información

La recolección de datos se realizó mediante la aplicación de encuestas físicas, efectuadas el 10 de agosto del presente año a las 12:30pm dentro de las instalaciones de la comunidad educativa, dirigidas al personal docente y administrativo de ambas instituciones.

Para recabar la información necesitada, la encuesta fue realizada a 40 personas (9 - personal administrativo, 31- personal docente) que comprenden el total de la población para el presente proyecto.

Procesamiento y análisis

Una vez realizada las encuestas a la población, se efectuó su respectivo procesamiento y análisis de resultados obteniendo lo siguiente:

1.- ¿Considera Ud. que la institución debe contar con un Sistema de Vigilancia y Monitoreo?

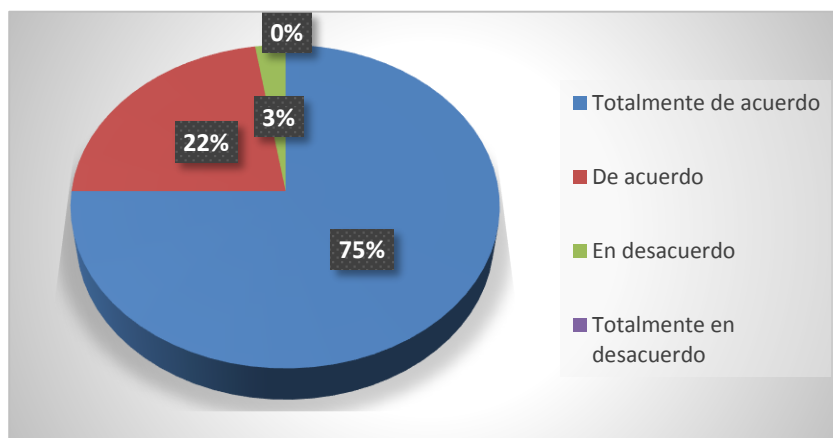
Frecuencia de pregunta Nº 1
Cuadro Nº 5

| DETALLE | FRECUENCIA | PORCENTAJE |
|--------------------------|------------|-------------|
| Totalmente de acuerdo | 30 | 75% |
| De acuerdo | 9 | 22% |
| En desacuerdo | 1 | 3% |
| Totalmente en desacuerdo | 0 | 0% |
| TOTAL | 40 | 100% |

Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández Páramo

Pregunta Nº 1
Gráfico Nº 16



Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández Páramo

Análisis: En el Gráfico se puede apreciar que el 75% de personas encuestadas consideran que las Instituciones deben contar con un Sistema de Vigilancia y Monitoreo.

2.- ¿Piensa que con la implementación de un Sistema de Vigilancia y Monitoreo, se está violando su privacidad?

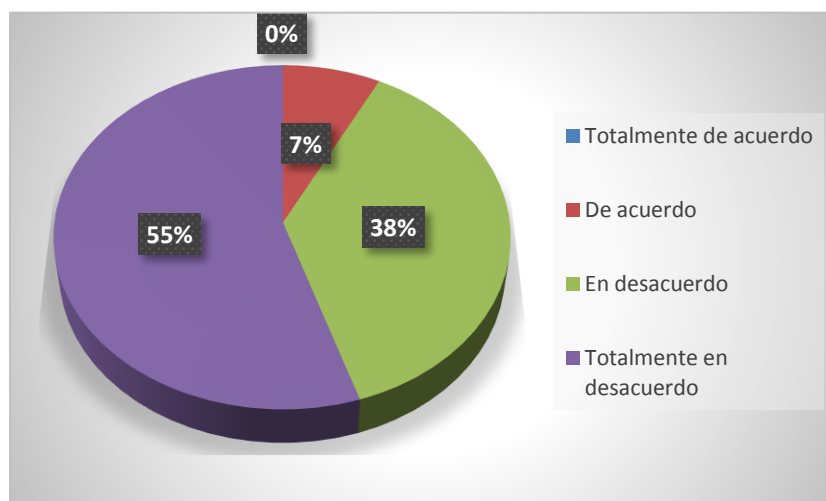
Frecuencia de pregunta Nº 2
Cuadro Nº 6

| DETALLE | FRECUENCIA | PORCENTAJE |
|--------------------------|------------|-------------|
| Totalmente de acuerdo | 0 | 0% |
| De acuerdo | 3 | 7% |
| En desacuerdo | 15 | 38% |
| Totalmente en desacuerdo | 22 | 55% |
| TOTAL | 40 | 100% |

Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández Páramo

Pregunta Nº 2
Gráfico Nº 17



Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández Páramo

Análisis: En el Gráfico se puede apreciar que el 55% de personas encuestadas consideran que al implementar un sistema de vigilancia y monitoreo, no se está violando el derecho a la privacidad.

3.- Con la existencia de un Sistema de Vigilancia y Monitoreo ¿se sentirá Ud. más seguro(a) en su ambiente de trabajo?

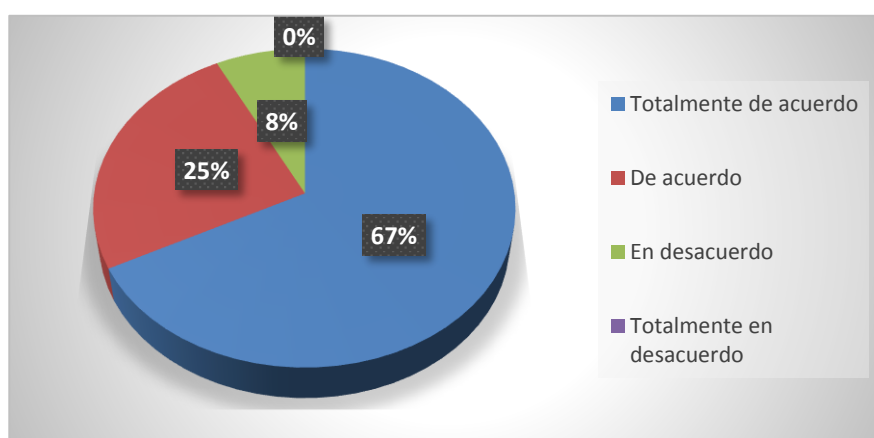
**Frecuencia de pregunta Nº 3
Cuadro Nº 7**

| DETALLE | FRECUENCIA | PORCENTAJE |
|---------------------------------|-------------------|-------------------|
| <i>Totalmente de acuerdo</i> | 27 | 67% |
| <i>De acuerdo</i> | 10 | 25% |
| <i>En desacuerdo</i> | 3 | 8% |
| <i>Totalmente en desacuerdo</i> | 0 | 0% |
| TOTAL | 40 | 100% |

Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández Páramo

**Pregunta Nº 3
Gráfico Nº 18**



Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández Páramo

Análisis: En el Gráfico se puede apreciar que el 67% de personas encuestadas consideran que en las instalaciones, al contar con un Sistema de Vigilancia y Monitoreo, se transmite un ambiente un poco más seguro.

4.- ¿Considera que es de gran utilidad para una institución educativa, el contar con un Sitio Web oficial para la emisión de comunicados?

Frecuencia de pregunta N° 4

Cuadro N° 8

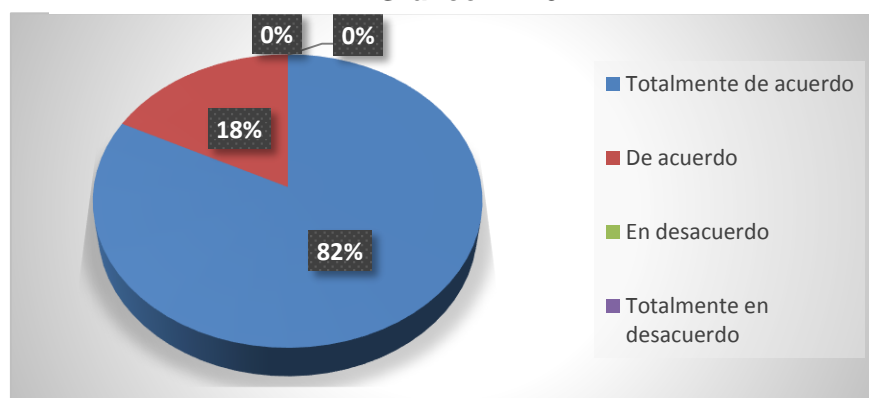
| DETALLE | FRECUENCIA | PORCENTAJE |
|---------------------------------|-------------------|-------------------|
| <i>Totalmente de acuerdo</i> | 33 | 82% |
| <i>De acuerdo</i> | 7 | 18% |
| <i>En desacuerdo</i> | 0 | 0% |
| <i>Totalmente en desacuerdo</i> | 0 | 0% |
| TOTAL | 40 | 100% |

Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández Páramo

Pregunta N° 4

Gráfico N° 19



Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández Páramo

Análisis: En el Gráfico se puede apreciar que el 82% de personas encuestadas consideran que se sería de gran utilidad para una institución educativa, el contar con un Sitio Web oficial para realizar la emisión de comunicados importantes para el conocimiento de los padres de familia.

5.- ¿Piensa que es inadecuado el uso de cuentas de correo personales con nombre de usuarios impropios para el envío de información institucional?

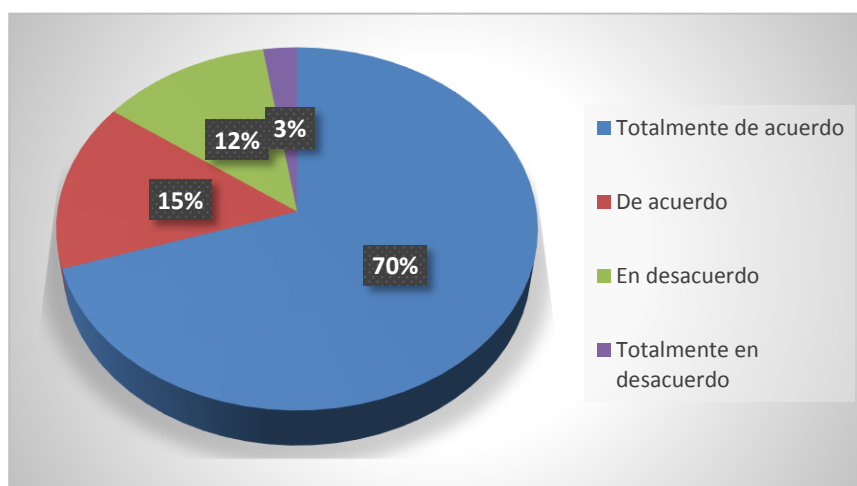
Frecuencia de pregunta N° 5
Cuadro N° 9

| DETALLE | FRECUENCIA | PORCENTAJE |
|--------------------------|------------|-------------|
| Totalmente de acuerdo | 28 | 70% |
| De acuerdo | 6 | 15% |
| En desacuerdo | 5 | 12% |
| Totalmente en desacuerdo | 1 | 3% |
| TOTAL | 40 | 100% |

Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández Páramo

Pregunta N° 5
Gráfico N° 20



Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández Páramo

Análisis: En el Gráfico se puede apreciar que el 70% de personas encuestadas consideran que es inadecuado el uso de cuentas de correo personales cuyos nombres de usuarios son inapropiados para el envío de información institucional.

6.- ¿Cree Ud. que el envío/recepción de información institucional del personal administrativo y/o docente debería realizarse a través de un correo oficial?

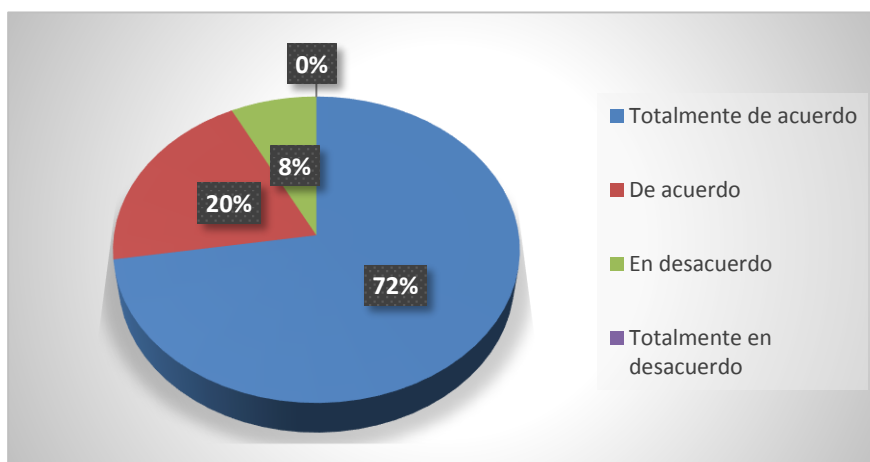
Frecuencia de pregunta Nº 6
Cuadro Nº 10

| DETALLE | FRECUENCIA | PORCENTAJE |
|--------------------------|------------|-------------|
| Totalmente de acuerdo | 29 | 72% |
| De acuerdo | 8 | 20% |
| En desacuerdo | 3 | 8% |
| Totalmente en desacuerdo | 0 | 0% |
| TOTAL | 40 | 100% |

Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández Páramo

Pregunta Nº 6
Gráfico Nº 21



Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández Páramo

Análisis: En el Gráfico se puede apreciar que el 72% de personas encuestadas consideran que sería mejor que en una institución el envío/recepción de información laboral entre el personal administrativo y/o docente debería realizarse a través de un correo oficial.

7.- ¿Considera que el acceso libre a internet que tienen los estudiantes en horas de clase (computación) representa un aspecto negativo para el aprendizaje?

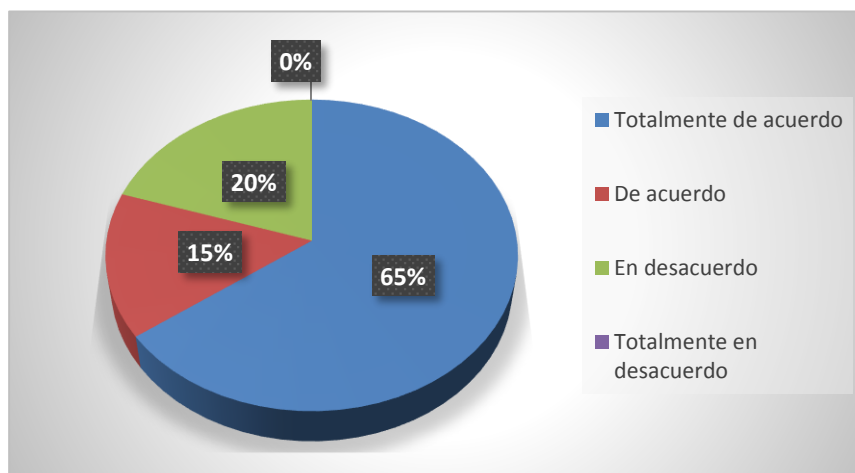
Frecuencia de pregunta N° 7
Cuadro N° 11

| DETALLE | FRECUENCIA | PORCENTAJE |
|--------------------------|------------|-------------|
| Totalmente de acuerdo | 26 | 65% |
| De acuerdo | 6 | 15% |
| En desacuerdo | 8 | 20% |
| Totalmente en desacuerdo | 0 | 0% |
| TOTAL | 40 | 100% |

Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández Páramo

Pregunta N° 7
Gráfico N° 22



Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández Páramo

Análisis: En el Gráfico se puede apreciar que el 65% de personas encuestadas consideran que el acceso libre que tienen los estudiantes al internet, durante las horas de clase de computación, representa un aspecto negativo para el aprendizaje en esas horas de clase.

8.- ¿Cree Ud. que al limitar el acceso a internet, los estudiantes tendrán menos distracciones en horas de computación y prestarán mayor atención a la clase?

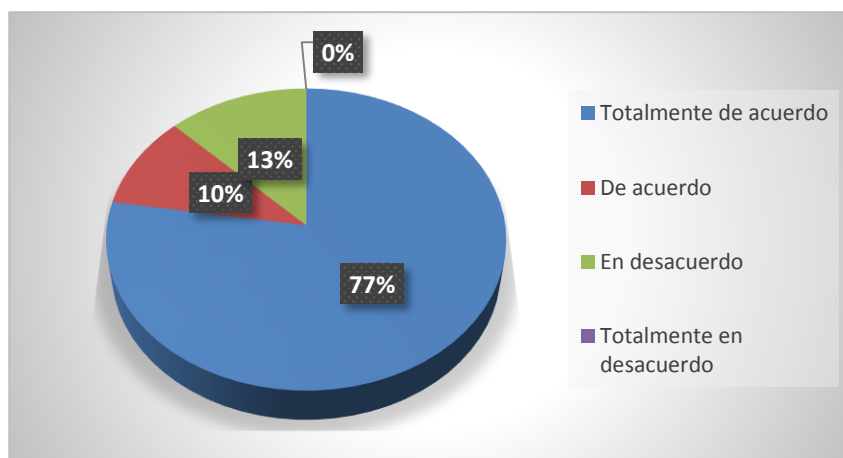
Frecuencia de pregunta Nº 8
Cuadro Nº 12

| DETALLE | FRECUENCIA | PORCENTAJE |
|--------------------------|------------|-------------|
| Totalmente de acuerdo | 31 | 77% |
| De acuerdo | 4 | 10% |
| En desacuerdo | 5 | 13% |
| Totalmente en desacuerdo | 0 | 0% |
| TOTAL | 40 | 100% |

Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández Páramo

Pregunta Nº 8
Gráfico Nº 23



Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández Páramo

Análisis: En el Gráfico se puede apreciar que el 77% de personas encuestadas consideran que al limitarles el acceso a las diferentes páginas web (internet) a los estudiantes en la hora de computación, tendrán menos distracciones y podrán prestar más atención a la clase.

9.- ¿Está de acuerdo que con la implementación de lo anteriormente mencionado, representará a futuro algún beneficio para la comunidad educativa?

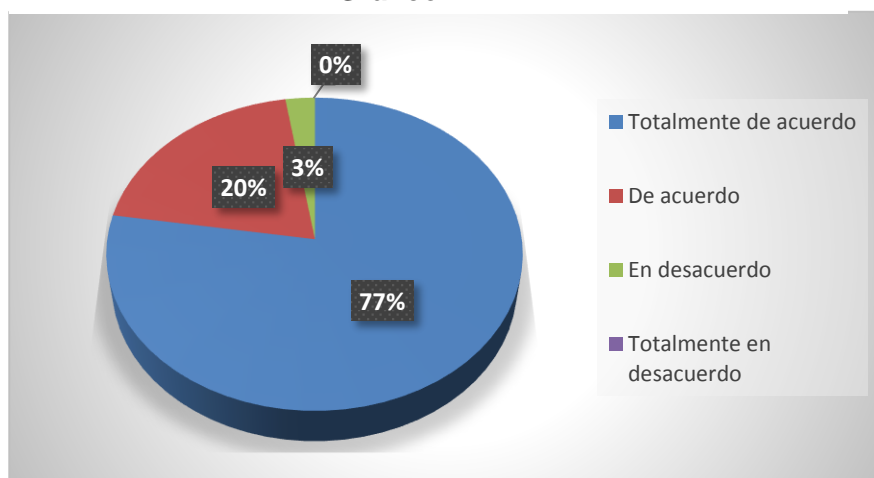
Frecuencia de pregunta Nº 9
Cuadro Nº 13

| DETALLE | FRECUENCIA | PORCENTAJE |
|--------------------------|------------|-------------|
| Totalmente de acuerdo | 31 | 77% |
| De acuerdo | 8 | 20% |
| En desacuerdo | 1 | 3% |
| Totalmente en desacuerdo | 0 | 0% |
| TOTAL | 40 | 100% |

Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández Páramo

Pregunta Nº 9
Gráfico Nº 24



Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín - Johanna Hernández Páramo

Análisis: En el Gráfico se puede apreciar que el 77% de personas encuestadas considera que al realizar todos los cambios mencionados en las preguntas anteriores, a futuro representará un beneficio significativo para las instituciones.

Validación de la hipótesis

Según la tabulación de los resultados obtenidos en la encuesta, se evidencia que más del 70% de la población concuerda en que la comunidad educativa transmite un ambiente de poca seguridad y no se puede realizar un seguimiento adecuado ante un evento suscitado con los estudiantes por motivo de que el sistema de seguridad CCTV es obsoleto y por ende no se encuentra en funcionamiento, que la utilización de correos personales para el manejo de la información estrictamente laboral es poco apropiado, la falta de un sitio web oficial dificulta la emisión de información para los padres de familia y que la falta de control sobre el uso del internet representa un aspecto negativo para los estudiantes y a su vez interrumpen las actividades del personal administrativo.

CAPÍTULO IV

PROPUESTA TECNOLÓGICA

La propuesta tecnológica que se va a implementar consta de 2 partes que son:

- Sistema CCTV.
- Servidores virtualizados.

Es necesario recalcar esto ya que son dos cosas totalmente distintas, que no se deben englobar en una sola idea.

Se llegó a estas propuestas como las más óptimas después de un amplio análisis considerando los recursos con los que se cuentan.

Sistema CCTV

- Se procedió a reemplazar por completo todo el cableado existente, mismo que poseía diversos inconvenientes y según fuentes tenía más de 10 años de uso en la institución por lo que no era viable su reutilización.
- Se reemplazó los equipos utilizados para monitoreo que constaban de 2 televisores y 2 switch de video (mismos que no tenían un respaldo de videos solo permitían visualizar) por un DVR de 16 canales y un monitor.

Cableado Estructurado

Previo a la instalación y configuración de los servidores, se tuvo la necesidad de hacer una reorganización en cuanto al cableado y los equipos de telecomunicaciones, debido a que las conexiones no eran las más óptimas para la implementación de este proyecto.

La ubicación de los equipos de telecomunicaciones no era la adecuada, por lo que se procedió a lo siguiente:

- Instalación de un soporte de pared que incluye, una bandeja, organizador horizontal y regleta de 8 tomacorrientes.

- Instalación de un switch rackeable de 24 puertos, reemplazando a los equipos que existentes.
- Instalación de un nuevo punto de red hacia el laboratorio de computación.
- Reubicación de los cables de red hacia el soporte de pared.

Servidores Virtualizados

- Ensamblaje del equipo físico.
- Instalación del software para virtualizar.
- Instalación y configuración de las máquinas virtuales.

Análisis de factibilidad

En base a las conclusiones y los resultados obtenidos, se puede afirmar que el presente proyecto es factible ya que será ejecutado por estudiantes de la Carrera de Ingeniería en Networking con sólidos conocimientos y además contando con el presupuesto necesario, además no presenta ningún tipo de restricción para su implementación.

También es considerada una obra sin fines de lucro y orientada a apoyar con el desarrollo de la comunidad educativa.

Se determinó que la propuesta es viable tomando en cuenta que el sector en el que se desenvuelve esta institución es el educativo, mismo que está inmerso a diversos cambios tecnológicos con el paso de los años, siendo este proyecto un paso importante para la constante innovación que tendrá esta Comunidad Educativa

Factibilidad Operacional

Mediante un estudio de carácter administrativo se determinó cual era la estructura organizacional de esta institución, con la finalidad de conocer quiénes y cómo van a utilizar este proyecto tecnológico.

Existe un apoyo total por parte de quienes conforman la comunidad educativa ESNUALSA S.A. para llevar a cabo el desarrollo de este proyecto, al ser algo llamativo e innovador en esta institución.

Factibilidad Técnica

Al ser un proyecto tecnológico de implementación es de fundamental importancia analizar que se requiere para el desarrollo del mismo, para lo cual se debe considerar los siguientes parámetros:

- a) Propuesta tecnológica y solución
- b) Tecnología disponible
- c) Conocimientos técnicos

a) Propuesta tecnológica y solución

Propuesta: Para la implementación del sistema CCTV se requiere de un equipo que sea capaz de albergar las 12 cámaras que existen actualmente y 3 cámaras nuevas adicionales, además este equipo debe almacenar por largos periodos de tiempo lo que receptan las cámaras, permitiendo realizar búsquedas de respaldos en caso de surgir una eventualidad.

La visualización y monitoreo también debe poder realizarse desde cualquier computadora que esté conectada a la red interna.

Solución: En base a este análisis se llegó a la conclusión de que se necesita adquirir un DVR de 16 canales con al menos 1TB de almacenamiento.

Propuesta: En cuanto a la otra parte del proyecto, se deben adquirir 3 servidores para que cumplan las siguientes funciones:

- 1 servidor de Firewall – proxy
- 1 servidor de correo
- 1 servidor Web

Además se deberá adquirir un dominio para poder ingresar a través de internet al sitio web y al correo institucional que se implementará.

Solución: Debido a que es demasiado costoso adquirir 3 equipos servidores y ante la carencia de espacio físico para poder ubicarlos, se llegó a la conclusión de que la virtualización es la mejor opción para cubrir estas necesidades, pero para esto se necesitaría ensamblar un equipo robusto.

b) Tecnología disponible

En base al análisis del punto anterior se indagó en el mercado y se determinó que para este proyecto se utilizará lo siguiente:

Hardware – CCTV

Para la implementación del nuevo sistema CCTV en la Comunidad Educativa ESNUALSA, se requerirá en primer lugar desmontar el sistema anterior el cual era obsoleto y se encontraba con falencias de tal manera que no se lo estaba usando, y será reemplazado por lo siguiente:

Hardware CCTV
Cuadro N° 14

| Cant. | Dispositivo | Marca/Modelo | Características |
|--------------|--------------------|------------------------------------|--|
| 1 | DVR | Samsung SDR-C5300 | 16 canales SD – HD 2TB HDD SO: Linux |
| 11 | Cámaras interior | Digital Color Bullet Camera | Tipo tubo Instaladas actualmente |
| 1 | Cámara interior | Digital Dome Camera | Tipo Domo Instalada actualmente |
| 2 | Cámara exterior | Hikvision IR Color camera | Tipo Tubo |
| 1 | Cámara interior | Hikvision IR vandal Dome camera | Tipo Domo |
| 1 | Monitor | Samsung Flatron L1753T | LCD 17” Resolución: 1280x1024 |

Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín-Johanna Hernández Páramo

Esta parte de la implementación no requirió de un software adicional, ya que el DVR contiene uno propio, para la visualización desde un equipo dentro de la red sólo es necesario conectarse vía browser (Internet Explorer) a la IP asignada al DVR y loguearse.

Hardware – Servidor

Como ya se explicó anteriormente al utilizar máquinas virtuales como servidores, estas requieren de un equipo físico robusto para un funcionamiento sin mayores inconvenientes, y es por eso que se decidió que se ensamblará un equipo con las siguientes características:

Hardware de Servidor
Cuadro N° 15

| Cant. | Dispositivo | Marca/Modelo | Características |
|--------------|--------------------|--------------------------|--|
| 1 | Gabinete - Case | Dipromacom | Con agarradera Negro |
| 1 | Fuente de poder | Real Agiler AGI-PS800 | 800W Ventilador 1x120mm Frecuencia 50-60Hz IN: 100 – 240 V OUT: +3.3V@24A, +5V@40A, +12V1@40A, +12V2@40A, -12V@0.5A, +5VSB@2.0A |
| 1 | Mainboard | Asus H87M-E | Puerto VGA Puerto DVI-D Puerto HDMI 4 puertos USB 3.0 2 Puertos USB 2.0 Puerto Ethernet Puertos Audio 3 Ranuras PCI Express 2.0 1 Ranura PCI Express 3.0 6 Puertos SATA 6gb/s 4 Slots DDR3 Socket Intel LGA 1150 Chipset Intel H87 |
| 1 | HDD | Seagate SN – 9QJ11CPS | 1TB 7200 RPM |
| 1 | HDD | Seagate SN – 29A25445 | 1TB 7200 RPM |
| 1 | HDD | Seagate SN- SQD21P1X | 750GB 7200 RPM |
| 2 | Memorias RAM | Kingston PC12800 | 8GB DDR3 1600 |
| 1 | Procesador | Intel Core | 4ta Generación |

| | | | |
|---|-----------------|----------------------------|---|
| | | I7-4790 | 4 núcleos Frecuencia básica 3.6 GHz Frecuencia máxima 4 GHz Velocidad del bus 5 GT/s Intel HD Graphics 4600 |
| 1 | Pendrive | Kingston | 8GB |
| 3 | Tarjetas de red | TP-Link TG-3468 | 10/100/1000 Mbps PCI Express Gigabit Compatibles con IEEE 802.3, IEEE 802.3u, IEEE 802.3ab |
| 2 | Cooler | LYF Sleeve | Dimensiones: 80mm x 80mm x 15mm |
| 1 | Switch | Trendnet – TE100-S24g/A | 24 Puertos 10/100Mbps Rackeable Tecnología GREENnet Conmutación 4.8 Gbps |

Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín – Johanna Hernández Páramo

Con todas estas piezas, se garantiza que el equipo tendrá una larga duración, y es suficiente como para soportar las máquinas virtuales que se van a configurar. Si la Comunidad Educativa requiere implementar un servidor extra a futuro lo puede hacer sin ningún problema, pero teniendo en cuenta la memoria RAM disponible, en caso de que no haya disponibilidad, se verán en la obligación de adquirir bajo su propia responsabilidad otras de similares características a las ya implementadas para mantener el estándar.

Cabe recalcar que el Switch no es parte/pieza del servidor pero si del proyecto, por lo que fue necesario detallar sus características.

Software – Servidor

Una vez detallado las características del equipo físico se procederá a detallar todo el software que se utilizará en la implementación de este proyecto.

Software Servidor
Cuadro N° 16

| Función | Software | Versión | Características |
|--------------------------|-----------------------|----------------|--------------------------------|
| Virtualizador | VMware vSphere ESxi | 6.0U2 | Tamaño: 357.95MB |
| Aplicación Virtualizador | VMware vSphere Client | 6.0U2 | Tamaño 349MB |
| SO Servidor Firewall | CentOS | 7 64 bits | ISO minimal Tamaño: 566MB |
| Proxy | squid | 3.3.8 | Paquete RPM Tamaño 8.54MB |
| Proxy Web | webmin | 1.8.10 | Paquete RPM Tamaño: 27.3MB |
| Firewall | iptables | 1.4.21 | Paquete RPM Tamaño 0.02 MB |
| SO Servidor Web | CentOS | 7 64 bits | ISO minimal Tamaño: 566MB |
| BD sitio web | MariaDB | 10.1.17 | Paquete TAR Tamaño: 433.6MB |
| webserver | httpd | 2.4.6 | Paquete RPM Tamaño: 7.5MB |
| CMS | Wordpress | 4.6 | Paquete TAR Tamaño: 8MB |
| SO Servidor Correo | CentOS | 7 64 bits | ISO minimal Tamaño: 566MB |
| Aplicación Correo | Zimbra | 8.7 | Paquete TGZ Tamaño: 290MB |
| DNS | Bind | 9.9.4 | Paquete TAR Tamaño: 8.9MB |

Fuente: Datos de la investigación

Elaborado por: Andrés Del Pozo Espín – Johanna Hernández Páramo

Cabe recalcar que todos estos softwares no representarán un costo adicional al proyecto ya que son gratuitos y de fácil acceso para ser descargados por internet.

c) Conocimientos técnicos

Todos los conocimientos que se aplicarán son los que se adquirieron durante los años de estudio en la Carrera de Ingeniería en Networking de la Universidad de Guayaquil, complementando con los obtenidos durante nuestras jornadas laborales.

Factibilidad Legal

En base a lo ya expuesto en el Capítulo II en la parte de Fundamentación Legal, se determinó que este proyecto de implementación no viola ni vulnera las leyes vigentes en la República del Ecuador ni tampoco en la reglamentación interna de la Comunidad Educativa ESNUALSA S.A., por lo que no se incurrirá en infracciones mismas que provoquen una imposibilidad para la ejecución o interrupción de los sistemas implementados.

Factibilidad Económica

Hay que mencionar que este proyecto será financiado por ambas partes, ESNUALSA S.A. financiará el sistema de CCTV, y los estudiantes cubrirán con los gastos de la implementación de los servidores.

Debido a que el equipo DVR se lo importará y al ser un gasto correspondiente a ESNUALSA no contarán con una factura que respalde ese gasto para sus declaraciones mensuales al SRI, motivo por el cual se llegará a un acuerdo el mismo que consiste en sumar algunos valores que les tocará cubrir a los estudiantes que participan en este proyecto para igualar el valor del DVR, de esta manera ESNUALSA S.A. podría tener un soporte para ese gasto.

La propuesta económicamente es factible ya que existe un ahorro considerable al utilizar máquinas virtuales y no adquirir servidores reales, también considerando el consumo de energía (en caso de tener servidores independientes) ya que estos

equipos deben obligatoriamente estar encendidos las 24 horas del día y solo apagarse en casos eventuales.

Etapas de la metodología del Proyecto

Como es de conocimiento general todo proyecto debe pasar por tres grandes etapas que son:

- Fase de Planificación
- Fase de ejecución
- Fase de entrega o puesta en marcha

Es recomendable añadir otras dos fases, ya que estas definen todo un conjunto de actividades que son básicas durante el desarrollo del proyecto, estas son:

- Fase de iniciación
- Fase de control

Fase de planificación

En una reunión previa con los directivos de ESNUALSA S.A., se comunicó en qué consistirá el proyecto, que requerimientos van a ser necesarios para la elaboración del mismo, costos aproximados (debido a la situación que enfrentó el país el 16 de Abril, los productos cambiaron su precio), una vez llegado al acuerdo se planificó:

- Los tiempos de inspección y levantamiento de información.
- Los tiempos de adquisición de materiales.
- Días y horas en que se laborarían para la implementación.

De esta manera se llevará un cronograma y debido a que en la institución se labora en dos jornadas, la mayor parte de la implementación se lo realizaría los fines de semana, de tal manera que se comprometieron a facilitarnos el acceso a las instalaciones durante esos días.

Fase de Iniciación

Se procederá a la búsqueda de los materiales, partes y piezas realizando cotizaciones en varios lugares para analizar la más conveniente y proceder a realizar la compra.

El orden en el que se realizará la implementación es el siguiente:

1. Sistema de CCTV
2. Servidores Virtuales

Fase de Ejecución

Una vez adquirido los materiales necesarios, se empezará con la implementación del sistema de CCTV para lo cual se debe regir al siguiente orden:

1. Remover el cableado antiguo y en mal estado.
2. Colocar la tubería por donde pasará el cableado
3. Realizar las mediciones para el nuevo cableado.
4. Cortar los distintos tramos de cable para las cámaras.
5. Unir los tramos de cables que vayan en la misma dirección para pasarlos por la tubería.
6. Ponchar los extremos de los cables con los conectores balun (video y poder).
7. Instalar el soporte de pared donde irán los equipos de telecomunicaciones y el DVR.
8. Instalar las cámaras en la nueva ubicación.
9. Conectar las cámaras al DVR.
10. Enfocar correctamente el lugar donde grabará cada cámara.

Previo a la implementación de los servidores virtuales, se realizó el ensamblaje del equipo físico, con todas las partes mencionadas al inicio de este capítulo.

Una vez de que se compruebe que el equipo encienda y en la BIOS consten las partes instaladas, se procederá a la instalación y configuración de las máquinas virtuales, se realizará en el siguiente orden:

1. Descargar el hypervisor VMware ESXi 6.0 de internet.
2. Realizar la instalación del hypervisor en el pendrive de 8GB, en esta se colocará el usuario y contraseña.
3. Configurar una tarjeta de red con una dirección IP de la LAN para conectarse con la aplicación cliente.
4. Instalar la aplicación cliente en la computadora del administrador.
5. Mediante la aplicación cliente ingresar al hypervisor usando las credenciales del paso 2.

6. Configurar los HDD y tarjetas de red para ser usados por las máquinas virtuales.
7. Descargar el ISO de CentOS 7 minimal de internet.
8. Crear un Data Store subiendo el ISO del CentOS 7 a uno de los HDD.
9. Crear la máquina virtual para el servidor firewall, asignándole recursos de hardware.
10. Instalar CentOS 7 en la máquina virtual creada en el paso anterior.
11. Instalar actualizaciones a la máquina virtual.
12. Instalar los paquetes necesarios para el firewall y proxy.
13. Crear los scripts necesarios para el proxy.
14. Crear el script para el firewall.
15. Crear el script para segmentar el ancho de banda.
16. Realizar pruebas con los equipos conectados a la red.
17. Crear la máquina virtual para el servidor de correo, asignándole recursos de hardware.
18. Instalar CentOS 7 en la máquina virtual del paso anterior.
19. Instalar las actualizaciones a la máquina virtual.
20. Descargar el paquete de Zimbra e instalarlo.
21. Instalar los paquetes necesarios para el DNS.
22. Configurar los archivos correspondientes al DNS.
23. Realizar pruebas de conexión a través de internet hacia el servidor de correo.
24. Crear cuentas de correo.
25. Realizar pruebas enviando y receptando correos, entre cuentas internas y externas.
26. Crear la máquina virtual para el servidor web, asignándole recursos de hardware.
27. Instalar CentOS 7 en la máquina virtual del paso anterior.
28. Instalar las actualizaciones a la máquina virtual.
29. Instalar los paquetes necesarios para el webserver.
30. Instalar y configurar la base de datos.
31. Descargar de internet e instalar Wordpress.
32. Verificar que se pueda acceder desde afuera al sitio web por medio del dominio contratado.

33. Diseñar el sitio web con información institucional.

Luego de realizar diversas pruebas con todos los servidores, se ubicará al equipo físico en su posición final, dentro de una estructura metálica diseñada a la medida, para evitar el manipuleo de terceras personas que tengan o no conocimiento sobre el mismo, además de que el equipo se encontrará empotrado en la pared a una altura considerable.

Fase de Entrega o puesta en marcha

Luego de determinar que el proyecto como tal ha superado con éxito las fases anteriores, se dará por concluido el mismo y será puesto en producción, para lo cual es necesario realizar las siguientes actividades:

- Crear políticas de almacenamiento de video en el DVR.
- Crear usuarios para visualización en el DVR.
- Habilitar la visualización en una computadora utilizando las credenciales de usuario creado en el paso anterior.
- Capacitación a la persona encargada del monitoreo de las cámaras.
- Capacitación al todo el personal que labora en la institución y que hará uso de las cuentas correo creadas.
- Capacitación al usuario administrador del servidor de correo.
- Capacitación al usuario administrador del sitio web.

Además en esta fase se determinará si se cumplieron con los tiempos establecidos en el cronograma que se elaboró inicialmente, de no ser así se deberán realizar las modificaciones pertinentes detallando el motivo por el que existió una demora.

Fase de Control

Durante las primeras semanas de implementación se realizarán constantes monitoreos para determinar falencias que hayan pasado por alto, se harán revisiones a nivel de hardware y software para determinar que el rendimiento sea el adecuado, además se coordinarán visitas técnicas a futuro para verificar el estado de los equipos y si es necesario realizar un mantenimiento se planificará una fecha adecuada en donde la intensidad de trabajo sea mínima en la institución, para que no se vean afectados mientras el equipo está fuera de línea.

Entregables del proyecto

Para este proyecto se entregarán 2 manuales, 1 de carácter técnico y 1 para usuario, los cuales contendrán lo siguiente:

Manual Técnico

- **Manual Técnico del sistema CCTV**

Se detallará cuales son y para qué sirven todas las partes del DVR, además se especificará el contenido del software, detalles técnicos de todas las cámaras instaladas.

- **Manual Técnico sobre:**

Hypervisor

En este manual se explicará la instalación y configuración del software tanto en la máquina servidor como en la máquina cliente, además se explicará sobre la creación de máquinas virtuales

Servidor Firewall - Proxy

Se detallará los pasos a seguir para instalar y configurar un servidor firewall y proxy, además la versión gráfica del proxy el webmin.

Servidor de Correo

Se detallará los pasos a seguir para instalar y configurar un servidor de correo utilizando Zimbra, además de la creación de las cuentas para los usuarios.

Servidor Web

Se detallará los pasos a seguir para instalar y configurar un servidor web.

Manual de Usuario

- **Manual de Usuario del sistema CCTV**

Se explicará cómo visualizar las diversas cámaras, revisar videos anteriores y descargar videos con una determinada duración.

- **Manual de Usuario sobre:**

Servidor de Correo

Se explicará las funciones de cada opción que hay en el entorno web de la aplicación Zimbra.

Sitio Web

Se explicará todas las funciones que existen en el entorno de administración del sitio web.

Webmin

Se enseñará el uso del proxy en un ambiente gráfico.

Criterios de validación de la propuesta

La propuesta tecnológica será validada mediante las pruebas que se realizarán en ambiente de producción, y también según los resultados de una encuesta de satisfacción que se colocará en el sitio web para que no solo el personal que labora en la institución lo pueda hacer, sino que también invitar a los padres de familia a que participen con su opinión respecto a la implementación que se llevará a cabo en la institución educativa donde se encuentran sus hijos.

Criterios de aceptación del Producto o Servicio

Con la implementación de esta propuesta, representantes de ESNUALSA S.A. aceptarán el proyecto cuando se cumpla con los siguientes requisitos:

- **Mejoras del sistema CCTV**

Podrán hacer uso de un renovado y mejorado sistema de monitoreo y seguridad CCTV, permitiendo a su vez interactuar con las diversas cámaras a la vez y además logar obtener un respaldo en caso de surgir una eventualidad.

- **Segmentación del Ancho de Banda**

El personal administrativo, podrá realizar sus actividades utilizando el internet con normalidad sin correr el riesgo de que este se vuelva lento producto de la conexión de muchas computadoras a la vez, pero se debe aclarar que contarán con lentitud en casos excepcionales cuando el proveedor de internet esté presentando fallas con el servicio, mismo que está fuera del alcance de este proyecto.

- **Restricción a Internet**

Los estudiantes, cuando utilicen las computadoras del laboratorio, sólo podrán acceder a ciertas páginas, en caso de no ser así inmediatamente

se mostrará el proxy en el navegador impidiendo al estudiante acceder a sitios bloqueados.

- **Acceso al sitio web**

Podrán hacer uso del sitio web como herramienta informativa para el público en general accediendo al siguiente dominio www.esnualsa.edu.ec

- **Correo institucional**

Harán uso de un correo institucional para el envío y recepción de información, dejando de lado las cuentas personales.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Una vez concluida la implementación del sistema de vigilancia y monitoreo, se brindará mayor seguridad para todos quienes forman parte de ESNUALSA, poniendo un fin a todos esos años en que ese sistema instalado no se lo utilizaba.
- Se mantiene una mejor organización para el cableado de red que se encontraba en oficina, identificando los puntos y que equipo está conectado al mismo.
- Existirá una mayor seguridad al emplear herramientas Open Source en la creación de los servidores virtuales, ya que estas se encuentra constantemente siendo revisadas por varias personas alrededor del mundo en busca de corregir errores o vulnerabilidades que afecten su correcto funcionamiento.
- El diseño del sitio web es sobrio buscando informar al público en general sobre cosas importantes de la institución.
- La ubicación final del equipo físico es la idónea ya que se buscó no entorpecer las actividades diarias del personal que labora ahí, debido al corto espacio físico con el que cuenta la oficina.

RECOMENDACIONES

- Para una mejor visualización de las cámaras se recomienda revisar las áreas donde se encuentran ubicadas las cámaras y realizar una limpieza para evitar que las telarañas tapen la visibilidad.
- No manipular si no se tiene conocimiento, los cables que se encuentran en el área destinada para los equipos de telecomunicaciones.
- La persona responsable de la administración de los servidores, deberá mantener un control estricto, cumpliendo con todas las políticas de seguridad implementadas, para de esta manera evitar vulnerabilidades que puedan ser detectadas por usuarios mal intencionados provocando daños severos.
- Mantener actualizado el sitio web para sacarle provecho.
- Evitar manipular el equipo servidor, en caso de existir alguna eventualidad, comunicar inmediatamente a la persona a cargo de la administración del mismo.

BIBLIOGRAFÍA

- **Arias, F.** (2012). El proyecto de Investigación Introducción a la metodología científica 6º ed.
- **Ayoví, J.** (2013). Virtualización de servidores para la nube de la Carrera de Ingeniería en Sistemas Computacionales
- **Esparza, J.** (2013a). Implementación de Firewall sobre plataforma Linux en la empresa de contabilidad Armas & Asociados
- **Esparza, J.** (2013b). Implementación de Firewall sobre plataforma Linux en la empresa de contabilidad Armas & Asociados
- **Esparza, J.** (2013c). Implementación de Firewall sobre plataforma Linux en la empresa de contabilidad Armas & Asociados
- **Esparza, J.** (2013d). Implementación de Firewall sobre plataforma Linux en la empresa de contabilidad Armas & Asociados
- **Guerrero, C.** (2011). Implementación de un ambiente de virtualización para el manejo de múltiples servidores VoIP sobre una plataforma común de hardware
- InformationWeek (s.f.) ¿Qué es la virtualización?
<http://www.vmware.com/latam/solutions/virtualization.html>
- **Padilla, H.** (2012). Análisis e implementación de un servidor de virtualización dedicado para integrar un servidor de correo zimbra virtualizado con un servidor multitarea zentyal físico como controlador de dominio, firewall y proxy utilizando herramientas como tecnologías de software libre.
- **Salvador, J.** (2014). ¿Para qué nos sirve un DVR?
<https://actelonline.wordpress.com/2014/07/31/que-es-un-dvr-y-para-que-nos-sirve/>
- **Siguencia, M.** (2012). Análisis, diseño e implementación del portal web del colegio Cesar Andrade y Cordero.
- **Suárez, P.** (2011). Población de estudio y muestra. Curso de la metodología de la investigación.
- **Tesis de Investigación** (2011). Población y muestra.
<http://tesisdeinvestig.blogspot.com/2011/06/poblacion-y-muestra-tamayo-y-tamayo.html>

- **VMware vSphere** (s.f.). VMware vSphere Ediciones de Enterprise y Enterprise Plus. <https://www.vmware.com/files/es/pdf/VMware-vSphere-Enterprise-Edition-Datasheet.pdf>
- **WordPress** (s.f.). <https://es.wordpress.org/>

ANEXOS

ENCUESTA APLICADA AL PERSONAL DOCENTE Y ADMINISTRATIVO DE LA COMUNIDAD EDUCATIVA ESNUALSA S.A.

Identificación de la Institución:

ESNUALSA S.A.

Objetivo de la encuesta:

- ✓ Conocer la opinión del personal docente y administrativo acerca de la seguridad dentro de las instalaciones de la comunidad educativa y la inclusión de tecnología para el desarrollo de sus actividades diarias.

Instrucciones para contestar:

- Lea detenidamente la pregunta y marque con una **X** una sola opción.

ITEM'S

1. ¿Considera Ud. que la institución debe contar con un Sistema de Vigilancia y Monitoreo?

- a) ☐ TOTALMENTE DE ACUERDO
- b) ☐ DE ACUERDO
- c) ☐ EN DESACUERDO
- d) ☐ TOTALMENTE EN DESACUERDO

2. ¿Piensa que con la implementación de un Sistema de Vigilancia y Monitoreo, se está violando su privacidad?

- a) ☐ TOTALMENTE DE ACUERDO
- b) ☐ DE ACUERDO
- c) ☐ EN DESACUERDO
- d) ☐ TOTALMENTE EN DESACUERDO

3. Con la existencia de un Sistema de Vigilancia y Monitoreo ¿se sentirá Ud. más seguro(a) en su ambiente de trabajo?

- a) ☐ TOTALMENTE DE ACUERDO
- b) ☐ DE ACUERDO
- c) ☐ EN DESACUERDO
- d) ☐ TOTALMENTE EN DESACUERDO

4. ¿Considera que es de gran utilidad para una institución educativa, el contar con un Sitio Web oficial para la emisión de comunicados?

- a) ☐ TOTALMENTE DE ACUERDO
- b) ☐ DE ACUERDO
- c) ☐ EN DESACUERDO
- d) ☐ TOTALMENTE EN DESACUERDO

5. ¿Piensa que es inadecuado el uso de cuentas de correo personales con nombre de usuarios improprios para el envío de información institucional?

- a) ____ TOTALMENTE DE ACUERDO
- b) ____ DE ACUERDO
- c) ____ EN DESACUERDO
- d) ____ TOTALMENTE EN DESACUERDO

6. ¿Cree Ud. que el envío/recepción de información institucional del personal administrativo y/o docente debería realizarse a través de un correo oficial?

- a) ____ TOTALMENTE DE ACUERDO
- b) ____ DE ACUERDO
- c) ____ EN DESACUERDO
- d) ____ TOTALMENTE EN DESACUERDO

7. ¿Considera que el acceso libre a internet que tienen los estudiantes en horas de clase (computación) representa un aspecto negativo para el aprendizaje?

- a) ____ TOTALMENTE DE ACUERDO
- b) ____ DE ACUERDO
- c) ____ EN DESACUERDO
- d) ____ TOTALMENTE EN DESACUERDO

8. ¿Cree Ud. que al limitar el acceso a internet, los estudiantes tendrán menos distracciones en horas de computación y prestarán mayor atención a la clase?

- a) ____ TOTALMENTE DE ACUERDO
- b) ____ DE ACUERDO
- c) ____ EN DESACUERDO
- d) ____ TOTALMENTE EN DESACUERDO

9. ¿Está de acuerdo que con la implementación de lo anteriormente mencionado, representará a futuro algún beneficio para la comunidad educativa?

- a) ____ TOTALMENTE DE ACUERDO
- b) ____ DE ACUERDO
- c) ____ EN DESACUERDO
- d) ____ TOTALMENTE EN DESACUERDO

CRONOGRAMA GENERAL DE TRABAJO

| ACTIVIDADES | RESPONSABLES | N° de Semana | | | | | | | | | |
|---|---|--------------|---|---|---|-------|---|---|---|--------|---|
| | | Junio | | | | Julio | | | | Agosto | |
| | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 |
| FASE DE PLANIFICACIÓN | | | | | | | | | | | |
| Reunión con autoridades | - Estudiantes - Representante Legal - Supervisora | X | | | | | | | | | |
| Levantamiento de información | - Estudiantes | X | | | | | | | | | |
| Diseño y propuesta del proyecto | - Estudiantes - Supervisora | X | | | | | | | | | |
| Reunión con el Tutor | - Estudiantes - Tutor | X | | | | | | | | | |
| Designación de Recursos para | - Estudiantes - Supervisora | X | | | | | | | | | |
| FASE DE EJECUCIÓN | | | | | | | | | | | |
| Cotización de materiales para CCTV | - Estudiantes | | X | X | | | | | | | |
| Cotización de materiales para Servidor | - Estudiantes | | | X | X | X | | | | | |
| Compra de materiales para CCTV | - Estudiantes - Supervisora | | | X | X | | | | | | |
| Compra de materiales para Servidor | - Estudiantes | | | | | X | X | X | | | |
| Compra de dominio por 5 años | - Estudiantes | | | | X | | | | | | |
| Instalación de cableado para CCTV | - Estudiantes | | | X | X | X | X | | | | |
| Instalación de estructura para equipos | - Estudiantes | | | | | | X | | | | |
| Instalación de cámaras | - Estudiantes | | | | X | X | X | | | | |
| Visita del Tutor | - Estudiantes - Tutor | | | | | | | | X | X | X |
| Ensamblaje y configuración de servidor | - Estudiantes | | | | | | | X | X | X | X |
| Instalación de Servidores Virtuales | - Estudiantes | | | | | | | X | X | X | X |
| Configuración de Servidores Virtuales | - Estudiantes | | | | | | | X | X | X | X |
| Instalación de Servidor | - Estudiantes | | | | | | | | | X | X |
| FASE DE EVALUACIÓN | | | | | | | | | | | |
| Elaboración y aplicación de encuesta a los beneficiarios directos de la comunidad | - Estudiantes | | | | | | | | | X | X |
| Capacitación a sobre las herramientas implementadas en el presente proyecto | - Estudiantes - Beneficiarios | | | | | | | | | X | X |
| Elaboración de informe final | - Estudiantes - Tutor | | | | | | | | | X | X |

Responsables:

Estudiantes: Andrés Del Pozo Espín y Johanna Hernández Páramo.

Tutor: Ing. Ángel Ochoa Flores.

Representante Legal: Ing. Pablo Baquerizo Vivar.

Supervisora designada por la institución: Dra. Consuelo Chafla Jarama.

Beneficiarios: Docentes y Personal Administrativo.

JORNADA DE TRABAJO Y TOTAL DE HORAS A LABORAR

| Nº | Responsable | Actividad | Lugar | Fecha (dd/mm/aa) | Horario | Nº Horas Trabajadas |
|----|---|---|----------|---------------------|---------------|------------------------|
| 1 | - Estudiantes - Representante legal - Supervisora | Reunión con autoridades y propuesta de proyecto comunitario en las instalaciones de la Comunidad Educativa. | ESNUALSA | 01/06/2016 | 15:00 – 16:00 | 1 |
| 2 | - Estudiantes | - Revisión de las condiciones del cableado actual del sistema CCTV. - Revisión del funcionamiento de las cámaras actuales. - Análisis de ubicación de 3 cámaras nuevas. | ESNUALSA | 04/06/2016 | 12:00 – 18:00 | 6 |
| 3 | - Estudiantes | - Revisión de las condiciones del cableado actual del sistema CCTV. - Revisión del funcionamiento de las cámaras actuales. | ESNUALSA | 05/06/2016 | 07:00 – 19:00 | 6 |
| 4 | - Estudiantes | - Creación de listado de materiales necesarios. | ESNUALSA | 06/06/2016 | 16:00 – 18:00 | 2 |
| 5 | - Estudiantes | - Análisis de ubicación de 3 cámaras nuevas. | ESNUALSA | 08/06/2016 | 16:00 – 20:00 | 4 |
| 6 | - Estudiantes | - Cotización y compra de materiales para cableado. | MARTEL | 09/06/2016 | 12:00 – 14:00 | 2 |
| 7 | - Estudiantes | - Medición, Corte y unión de cables para cámaras 1, 2, 3, 4, 5, 6 y 7. | ESNUALSA | 11/06/2016 | 12:00 – 18:00 | 6 |
| 8 | - Estudiantes | - Medición, Corte y unión de cables para cámaras 1, 2, 3, 4, 5, 6 y 7. | ESNUALSA | 12/06/2016 | 07:00 – 19:00 | 6 |
| 9 | - Estudiantes | - Medición, Corte y unión de cables para cámaras 1, 2, 3, 4, 5, 6 y 7. | ESNUALSA | 13/06/2016 | 16:00 – 18:00 | 2 |
| 10 | - Estudiantes | - Instalación de cableado de cámaras 4 y 5. | ESNUALSA | 15/06/2016 | 16:00 – 20:00 | 4 |
| 11 | - Estudiantes | - Instalación de cableado para cámaras 6 y 7. - Desconexión y retirada de antiguo cableado. | ESNUALSA | 18/06/2016 | 12:00 – 18:00 | 6 |
| 12 | - Estudiantes | - Instalación de cableado para cámaras 1, 2 y 3. - Desconexión y retirada de antiguo cableado. | ESNUALSA | 19/06/2016 | 07:00 – 19:00 | 6 |
| 13 | - Estudiantes | - Desconexión y retirada de antiguo cableado. | ESNUALSA | 20/06/2016 | 16:00 – 17:00 | 3 |

| | | | | | | |
|----|---------------|---|----------|------------|---------------|---|
| 14 | - Estudiantes | - Instalación de conectores en el nuevo cableado instalado. | ESNUALSA | 22/06/2016 | 16:00 – 20:00 | 4 |
| 15 | - Estudiantes | - Instalación de conectores en el nuevo cableado instalado. - Desmontaje de antiguo sistema de monitoreo de cámaras - Compra de materiales de ferretería faltantes. | ESNUALSA | 02/07/2016 | 12:00 – 18:00 | 6 |
| 16 | - Estudiantes | - Cotización y compra de materiales faltantes para el CCTV y servidor. | MARTEL | 12/07/2016 | 14:00 – 16:00 | 2 |
| 17 | - Estudiantes | - Instalación de soporte de pared 5ur. - Medición, Corte y unión de cables para cámaras 9, 10 y 11. | ESNUALSA | 16/07/2016 | 12:00 – 18:00 | 6 |
| 18 | - Estudiantes | - Instalación de cableado para cámaras 9, 10 y 11. - Instalación de DVR. | ESNUALSA | 17/07/2016 | 07:00 – 19:00 | 6 |
| 19 | - Estudiantes | - Conexión de cámara 11 con el nuevo cableado al DVR. | ESNUALSA | 18/07/2016 | 16:00 – 19:00 | 3 |
| 20 | - Estudiantes | - Instalación de Monitor debajo del soporte de pared. | ESNUALSA | 20/07/2016 | 16:00 – 20:00 | 4 |
| 21 | - Estudiantes | - Reubicación y conexión al DVR de cámaras 1, 2, 4 y 5 con el cableado nuevo. - Compra de 3 cámaras nuevas. | ESNUALSA | 23/07/2016 | 12:00 – 18:00 | 6 |
| 22 | - Estudiantes | - Instalación de conectores en cableado de cámaras 10 y 11. - Reubicación y conexión de cámaras 10 y 11 al DVR. - Instalación de cámara 6. - Medición, Corte y unión de cables para cámaras 12, 13, 14 y 15. | ESNUALSA | 24/07/2016 | 08:00 – 14:00 | 6 |
| 23 | - Estudiantes | - Instalación de cableado para cámaras 12, 13, 14 y 15. - Instalación de conectores para el cableado mencionado anteriormente. | ESNUALSA | 25/07/2016 | 08:00 – 14:00 | 6 |
| 24 | - Estudiantes | - Reubicación y conexión de cámaras 12, 13, 14 y 15 al DVR. | ESNUALSA | 27/07/2016 | 16:00 – 21:00 | 5 |

| | | | | | | |
|----|--------------------------|---|----------|------------|---------------|---|
| 25 | - Estudiantes | - Cotización y compra de Switch de 24 puertos rackeable. | SERIMTEC | 29/07/2016 | 10:00 – 14:00 | 4 |
| 26 | - Estudiantes - Tutor | - Compra de partes y piezas para servidor. - Reubicación y conexión al DVR de cámara 3 con el cableado nuevo. - Visita del Tutor. - Medición y Corte de cables para cámara 8 y puntos de datos D1 y D2 en laboratorio. - Ensamblaje de servidor | ESNUALSA | 30/07/2016 | 10:00 – 16:00 | 6 |
| 27 | - Estudiantes | - Instalación de cámara 8 y puntos de datos D1 y D2 en laboratorio. - Instalación de Switch de 24 puertos rackeable en el soporte de pared. - Identificación de cableado de red de oficina y reubicación al soporte de pared. - Conexión del cableado de oficina al switch nuevo de 24 | ESNUALSA | 31/07/2016 | 10:00 – 16:00 | 6 |
| 28 | - Estudiantes | - Creación de esxi 6.0 incluyendo los drivers para las tarjetas de red. - Instalación del hypervisor esxi 6.0 en el servidor. - Configuración de los HDD e interfaces de red. - Creación de una red LAN para pruebas | OFICINA | 01/08/2016 | 08:00 – 12:00 | 4 |
| 29 | - Estudiantes | - Creación del DataStore en el servidor, importación de iso de Centos 7. - Creación de máquina virtual para el servidor Firewall. - Instalación de máquina virtual FW con sistema operativo Centos 7 | OFICINA | 02/08/2016 | 08:00 – 12:00 | 4 |
| 30 | - Estudiantes | - Configuración de servidor FW, instalación de Squid. - Creación de iptables. - Creación de listas de acceso. - Creación de script para segmentar el ancho de banda. - Pruebas con el FW y el proxy | OFICINA | 03/08/2016 | 08:00 – 12:00 | 4 |

| | | | | | | |
|----|---|---|----------|------------|---------------|---|
| 31 | - Estudiantes | - Creación de máquina virtual para el servidor web. - Instalación de máquina virtual para servidor web con sistema operativo Centos 7 - Configuración de servidor web. - Instalación de wordpress. | OFICINA | 04/08/2016 | 08:00 – 12:00 | 4 |
| 32 | - Estudiantes - Beneficiarios - Supervisora | - Pruebas con el FW y Servidor Web. - Diseño de Sitio Web. - Encuestas | OFICINA | 05/08/2016 | 08:00 – 12:00 | 4 |
| 33 | - Estudiantes - Tutor | - Visita de Tutor - Diseño de Sitio Web. | OFICINA | 06/08/2016 | 12:00 – 17:00 | 5 |
| 34 | - Estudiantes | - Diseño de Sitio Web. - Creación de máquina virtual para el servidor de correo, asignando 2 HDD. | OFICINA | 07/08/2016 | 10:00 – 15:00 | 5 |
| 35 | - Estudiantes | - Instalación de máquina virtual para servidor mail con sistema operativo Centos 7 utilizando RAID 1. | OFICINA | 08/08/2016 | 08:00 – 11:00 | 3 |
| 36 | - Estudiantes | - Configuración de servidor mail. | OFICINA | 09/08/2016 | 08:00 – 10:00 | 2 |
| 37 | - Estudiantes | - Diseño de Sitio Web. | OFICINA | 11/08/2016 | 08:00 – 10:00 | 2 |
| 38 | - Estudiantes | - Instalación de Zimbra 8.7 en el servidor mail | OFICINA | 12/08/2016 | 08:00 – 11:00 | 3 |
| 39 | - Estudiantes | - Diseño de Sitio Web. | ESNUALSA | 13/08/2016 | 12:00 – 14:00 | 2 |
| 40 | - Estudiantes | - Instalación y configuración de DNS en el servidor de Correo | ESNUALSA | 14/08/2016 | 08:00 – 11:00 | 3 |
| 41 | - Estudiantes | - Diseño de Sitio Web. - Configuración de Zimbra. - Creación de cuentas de correo de prueba. | OFICINA | 15/08/2016 | 08:00 – 12:00 | 5 |
| 42 | - Estudiantes | - Diseño de Sitio Web. - Instalación y configuración de servidores con red de ESNUALSA. - Instalación y configuración de DNS en el servidor de Correo | ESNUALSA | 16/08/2016 | 12:00 – 18:00 | 6 |
| 43 | - Estudiantes - Beneficiarios - Supervisora | - Presentación de Sitio web y correo institucional. - Capacitación sobre uso de cuentas de correo institucional. - Creación de cuentas de correo para personal administrativo y docente. | ESNUALSA | 17/08/2016 | 10:00 – 14:00 | 6 |

| | | | | | | |
|-----------------------------|--------------------------|--|----------|------------|---------------|-----|
| 44 | - Estudiantes - Tutor | - Instalación de Servidor en estructura metálica - Visita de Tutor - Informe Final | ESNUALSA | 18/08/2016 | 08:00 – 16:00 | 6 |
| DURACION TOTAL DEL PROYECTO | | | | | | 192 |

Responsables:

Estudiantes: Andrés Del Pozo Espín y Johanna Hernández Páramo.

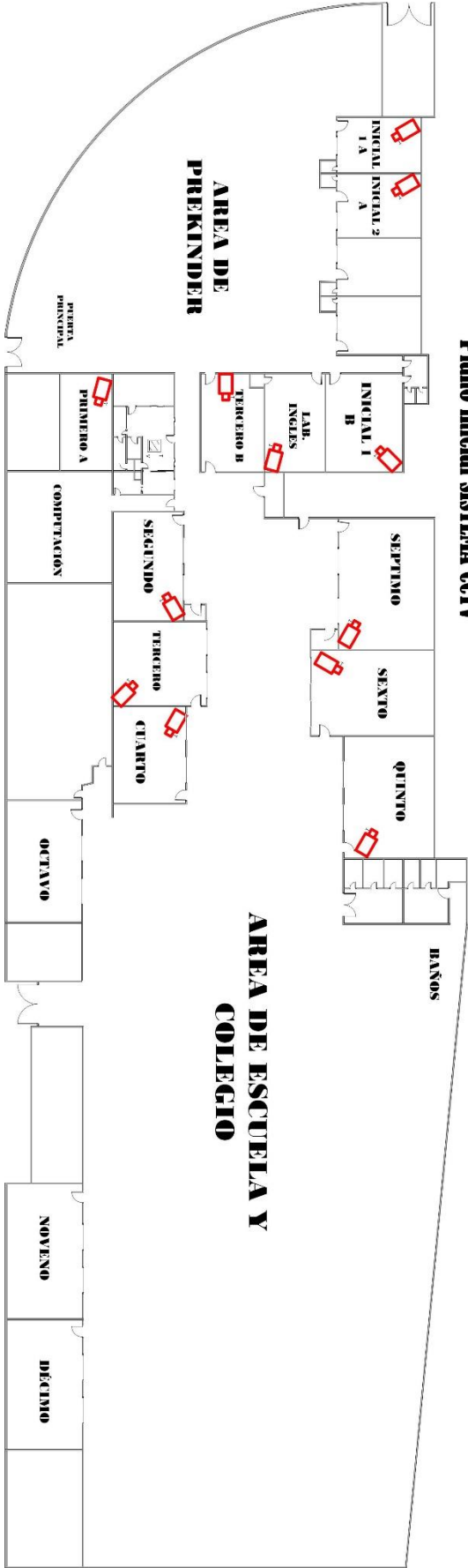
Tutor: Ing. Ángel Ochoa Flores.

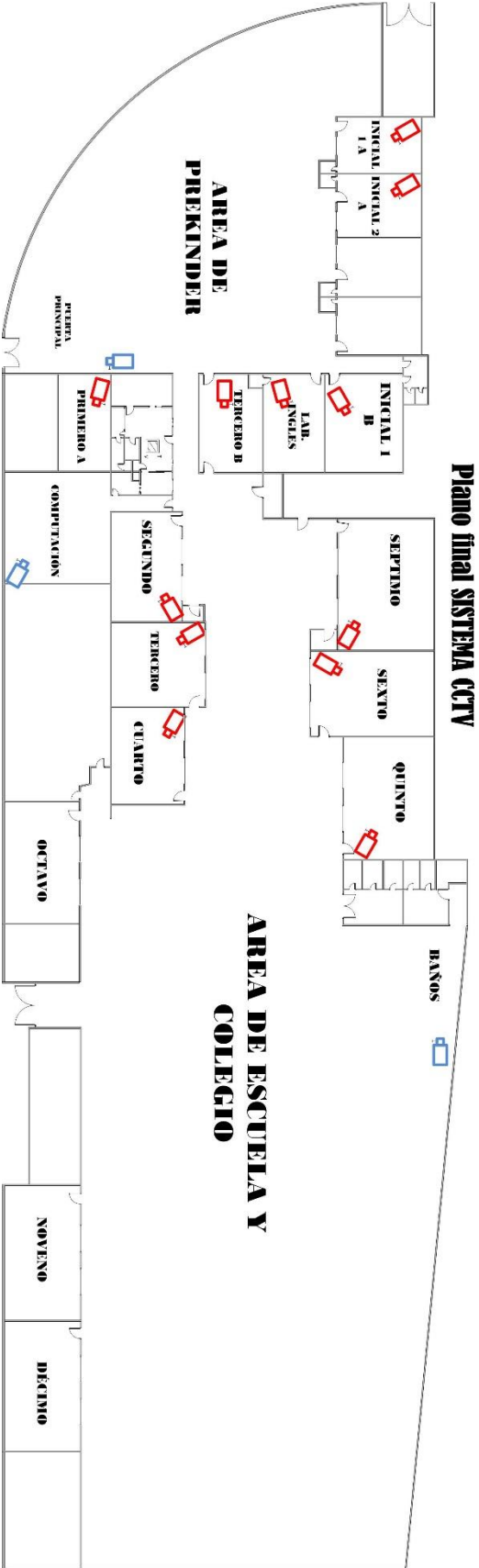
Representante Legal: Ing. Pablo Baquerizo Vivar.

Supervisora designada por la institución: Dra. Consuelo Chafía Jarama.

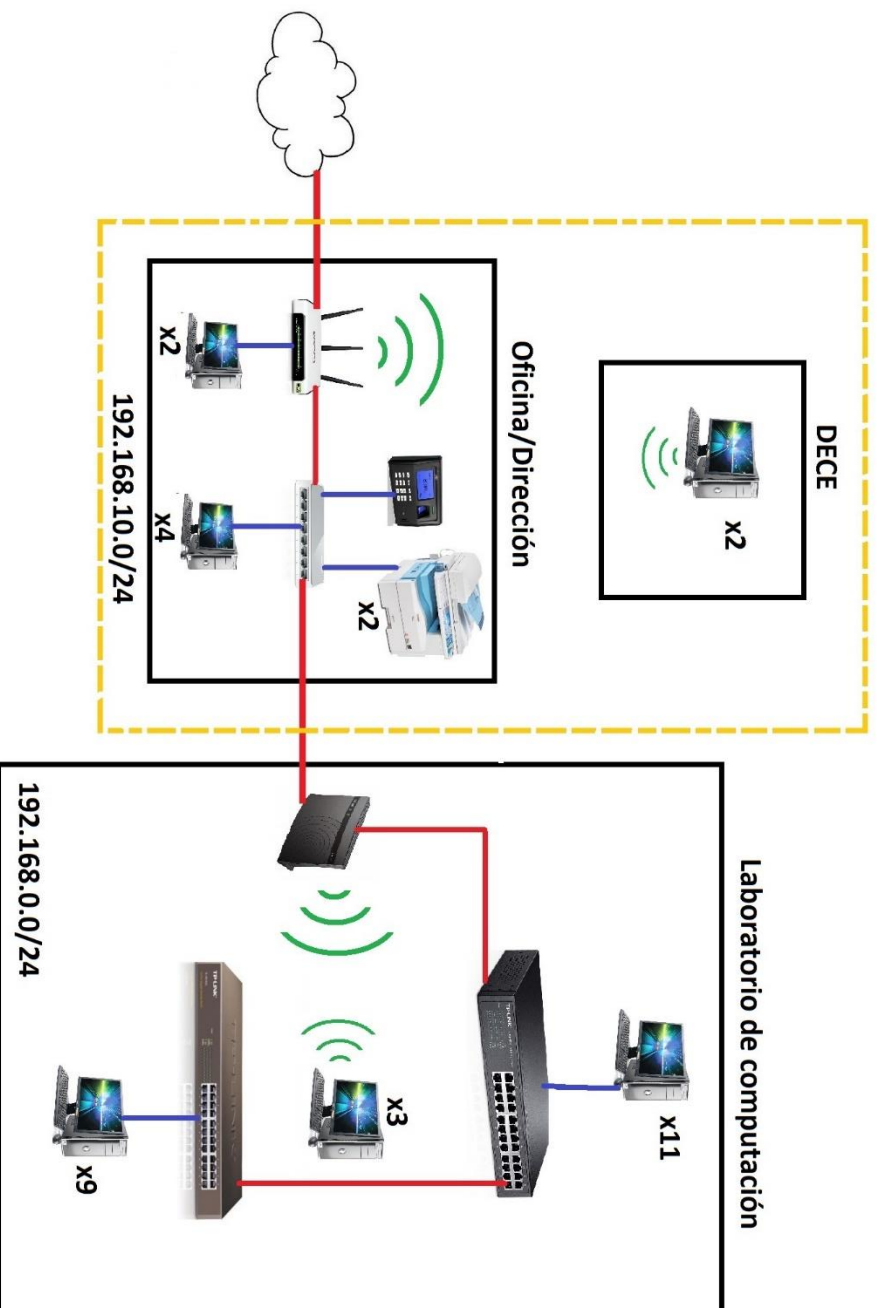
Beneficiarios: Docentes y Personal Administrativo.

Plano Inicial SISTEMA CCTV

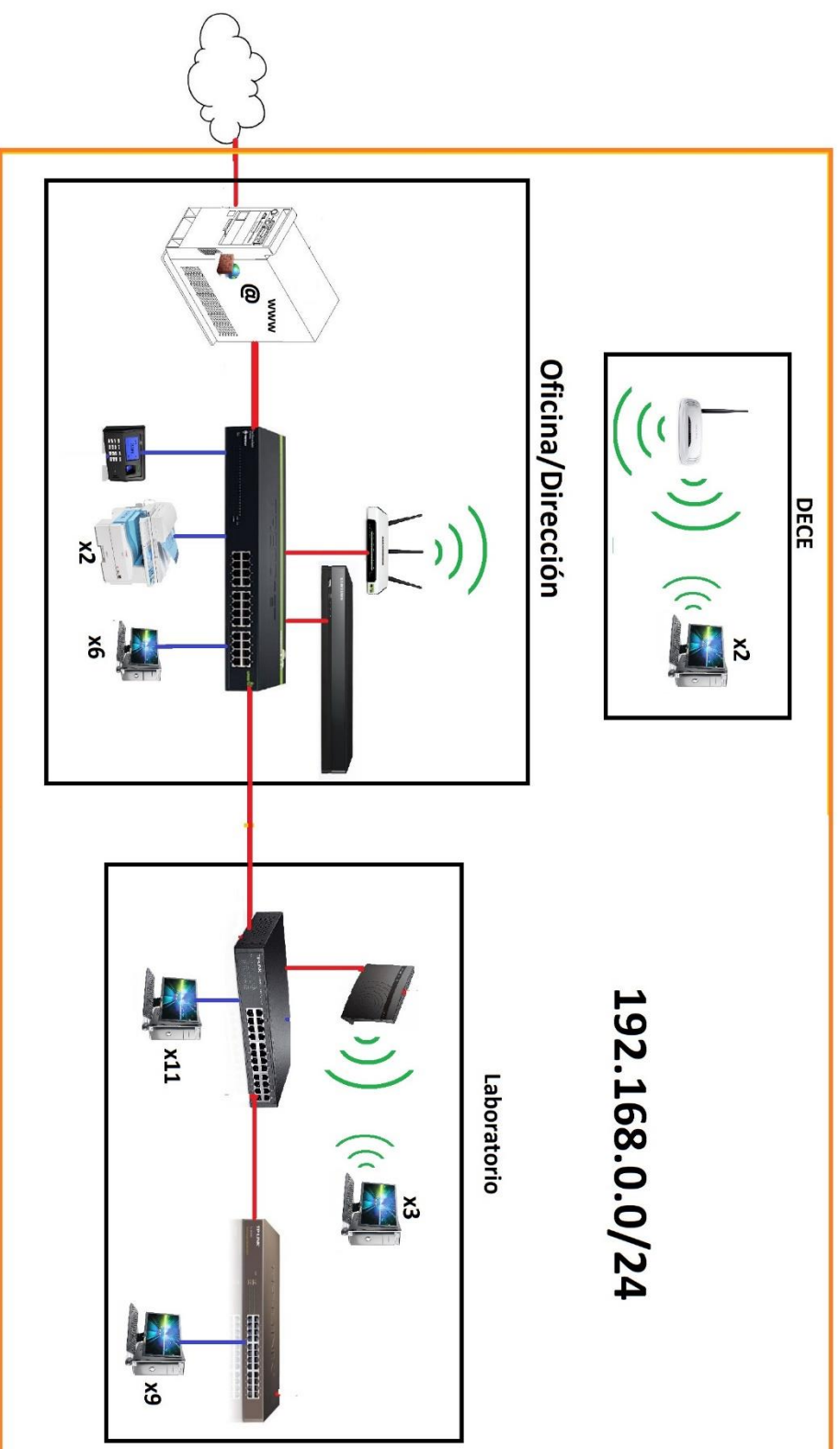




DISEÑO DE LA SITUACIÓN INICIAL DE LA RED

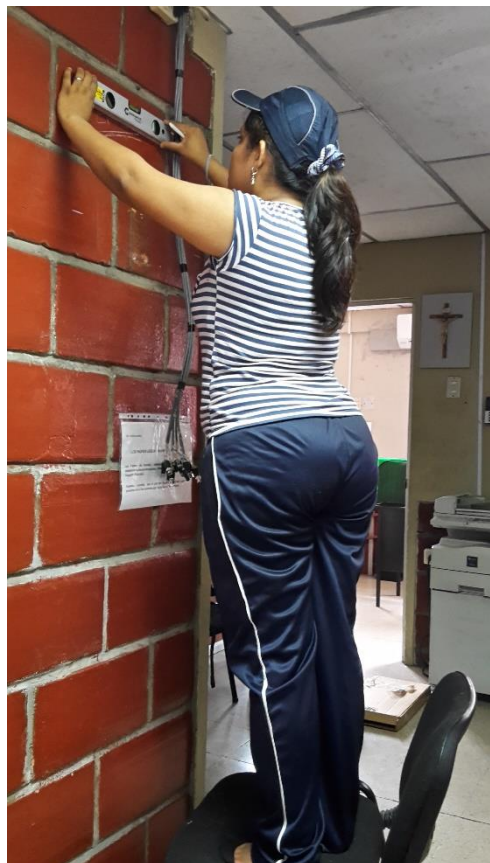


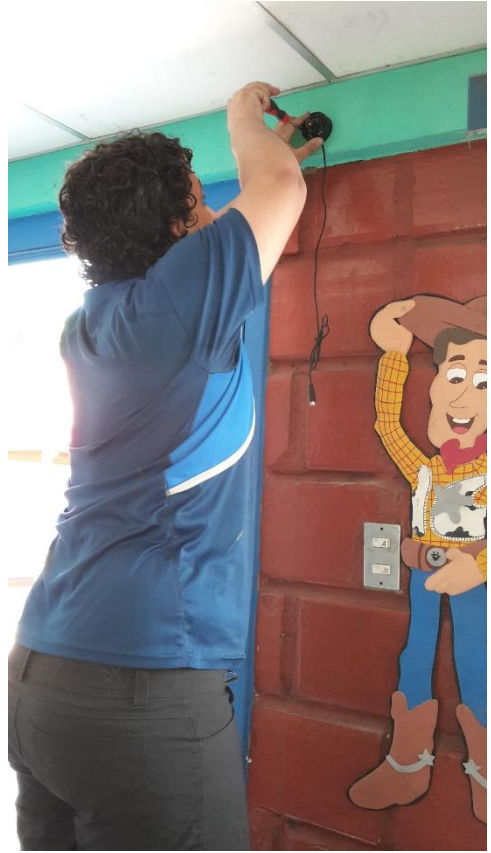
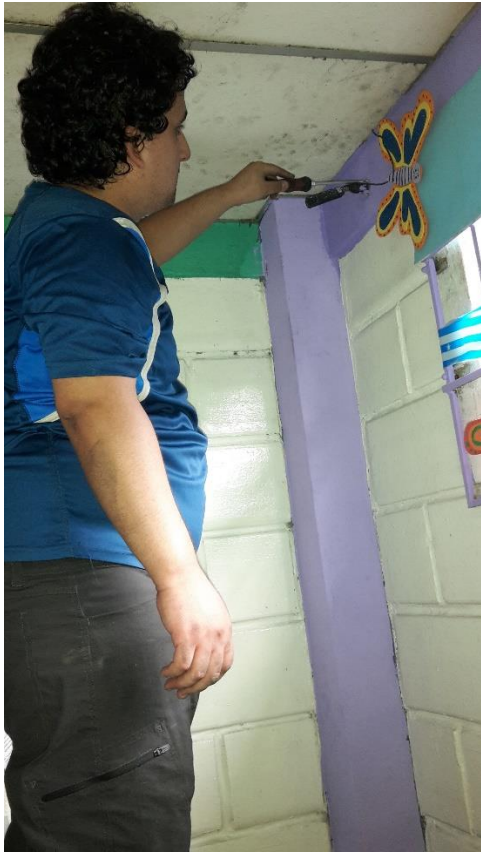
DISEÑO DE LA SITUACIÓN FINAL DE LA RED

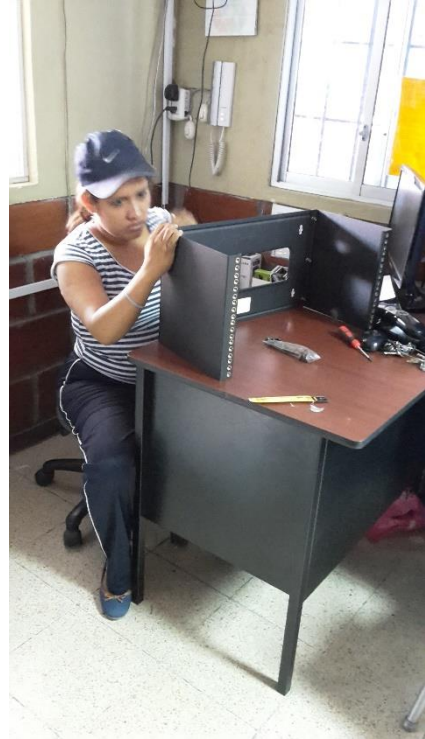
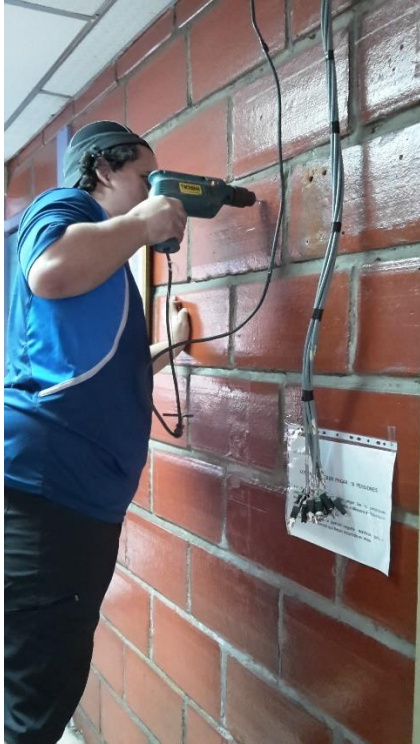


EVIDENCIAS



















UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD CCTV Y
VIRTUALIZACIÓN DE SERVIDORES FIREWALL – PROXY,
CORREO Y WEB PARA LA UNIDAD EDUCATIVA
ESNUALSA

MANUAL DE USUARIO
WORDPRESS
WEBMIN
ZIMBRA
SISTEMA CCTV

Previa a la obtención del Título de:

INGENIERO EN NETWORKING Y TELECOMUNICACIONES

AUTORES:

Wilson Andrés Del Pozo Espín

Johanna Alejandrina Hernández Páramo

GUAYAQUIL – ECUADOR
2016

ÍNDICE GENERAL

| | |
|---|-----------|
| INDICE GENERAL | II |
| MANUAL DE USUARIO WORDPRESS | 1 |
| WORDPRESS | 2 |
| • Acceder al sitio web | 2 |
| • Selección y activación del tema | 2 |
| • Personalización del tema | 4 |
| • Menú de configuración del tema | 5 |
| ○ Identidad del sitio | 5 |
| ○ Insertar una imagen en el tema | 6 |
| ○ Guardar cambios | 7 |
| • Layout | 8 |
| • Diseño | 8 |
| • Colores | 10 |
| • Tipografía | 10 |
| • Cabecera | 12 |
| • Escritorio del sitio web | 17 |
| • Entradas | 17 |
| • Páginas | 18 |
| • Medios | 18 |
| • Apariencia | 19 |
| • Plugins | 21 |
| • Usuario | 22 |
| • Herramienta | 23 |
| • Ajustes | 24 |
| MANUAL DE USUARIO WEBMIN | 25 |
| WEBMIN | 26 |
| • Acceder a WEBMIN | 26 |
| • Archivos de configuración | 28 |
| • Permitir el acceso a Internet | 29 |
| MANUAL DE USUARIO SERVIDOR DE CORREO | 30 |
| SERVIDOR DE CORREO | 31 |
| • Ingresar a Zimbra | 31 |

| | |
|--|----|
| • Enviar un nuevo mensaje | 31 |
| • Contactos | 33 |
| • Agenda | 34 |
| • Tareas | 34 |
| • Maletín | 34 |
| • Preferencias | 35 |
| MANUAL DE USUARIO SISTEMA CCTV | 37 |
| SISTEMA CCTV | 38 |
| • Ingresar al DVR por medio de Internet Explorer | 38 |
| • Búsqueda de Video | 38 |
| • Ingresar al DVR por medio de Smart Viewer | 40 |
| • Búsqueda de Video | 41 |
| • Realizar una copia de seguridad | 42 |

MANUAL DE USUARIO

WORDPRESS

WORDPRESS

Acceder al sitio web

1. Abrir una ventana del navegador y digitar la dirección de dominio de la página web, añadiendo al final /wp-admin para ingresar al entorno de configuración de la página.

Insertar nombre de usuario y contraseña.

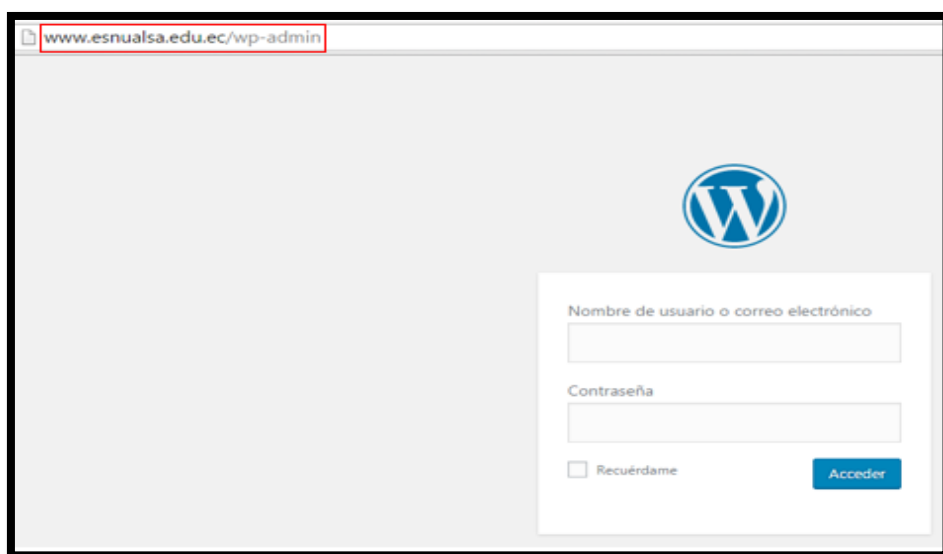


Imagen 01 – Acceso al sitio

Selección y activación del tema

2. Mostrará el escritorio de configuraciones de Wordpress, dar click en el botón Personalizar Sitio para ver las opciones de configuración.

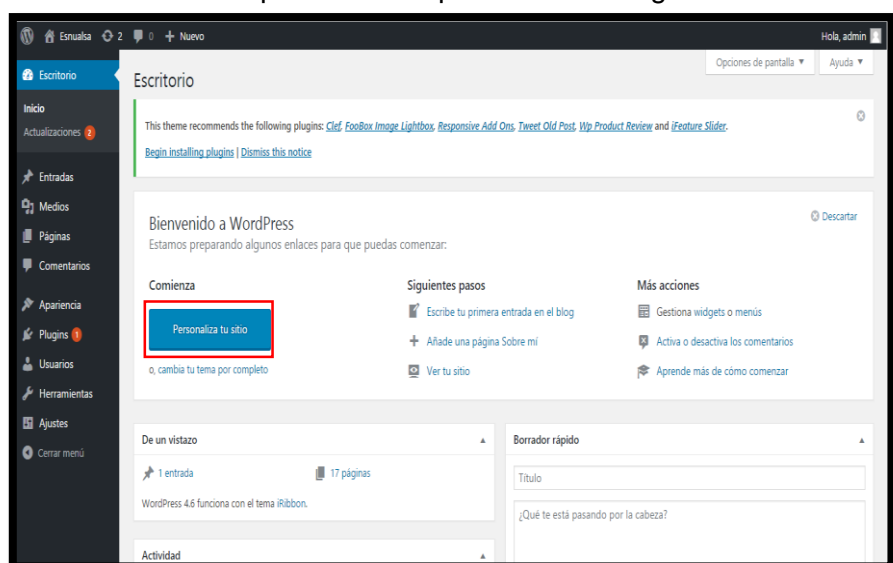


Imagen 02 – Personalizar sitio

3. Aparecerá la opción para escoger el tema para el sitio. Se puede escoger uno de los temas que ya vienen dentro del Wordpress, dando click en el botón activar y el tema se activa para el sitio web o se puede buscar el tema dando click en el botón añadir nuevo.

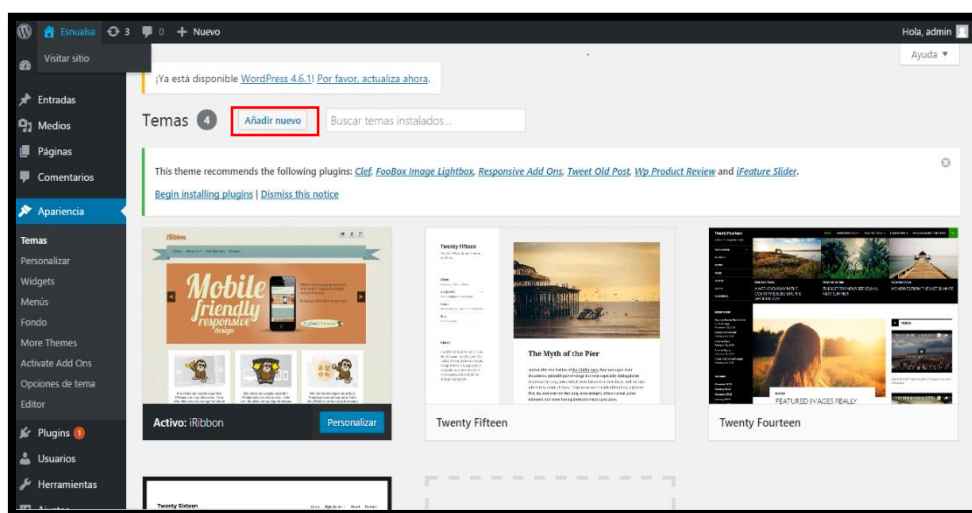


Imagen 03 – Añadir tema

4. Se mostrará en la ventana una serie de temas para instalar. Se puede escoger uno de esos pasando el mouse sobre el tema y dando click en el botón instalar tema.

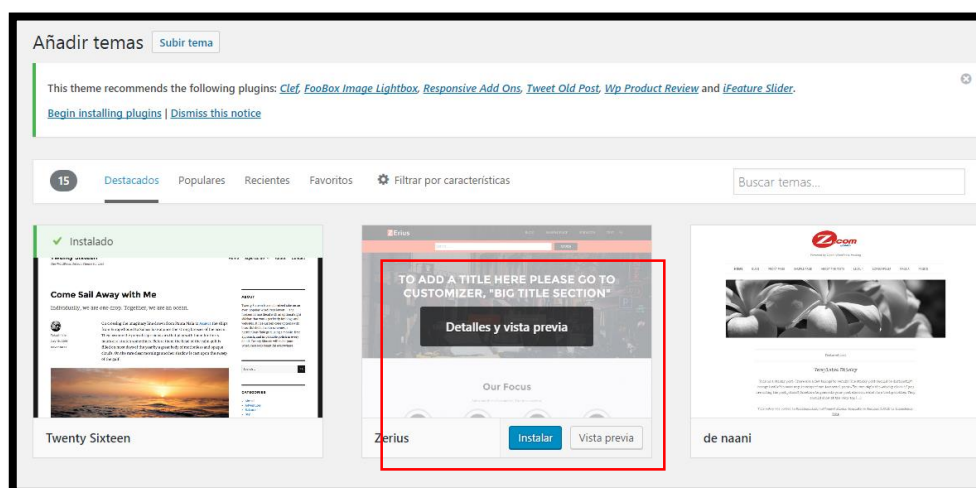


Imagen 04 – Instalación de tema

También puede buscar más temas dando click en una de las opciones del menú que se muestra en la parte superior o escribiendo el nombre en la sección de buscar tema.

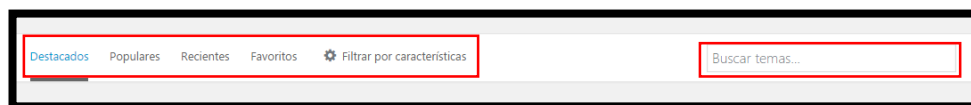


Imagen 05 – Búsqueda de temas

Otra forma de escoger el tema es subiendo uno que ya se tenga previamente descargado y almacenado en el equipo físico de donde se está trabajando el sitio web. Dar click en el botón subir tema que se encuentra en la parte superior y escoger el tema que se tiene previamente descargado. En este caso se instaló el tema iRibbon.



Imagen 06 – Subir temas desde el equipo

Personalización del tema

5. Ya activado el tema deseado, dar click en el botón personalizar para comenzar a caracterizar el sitio web.

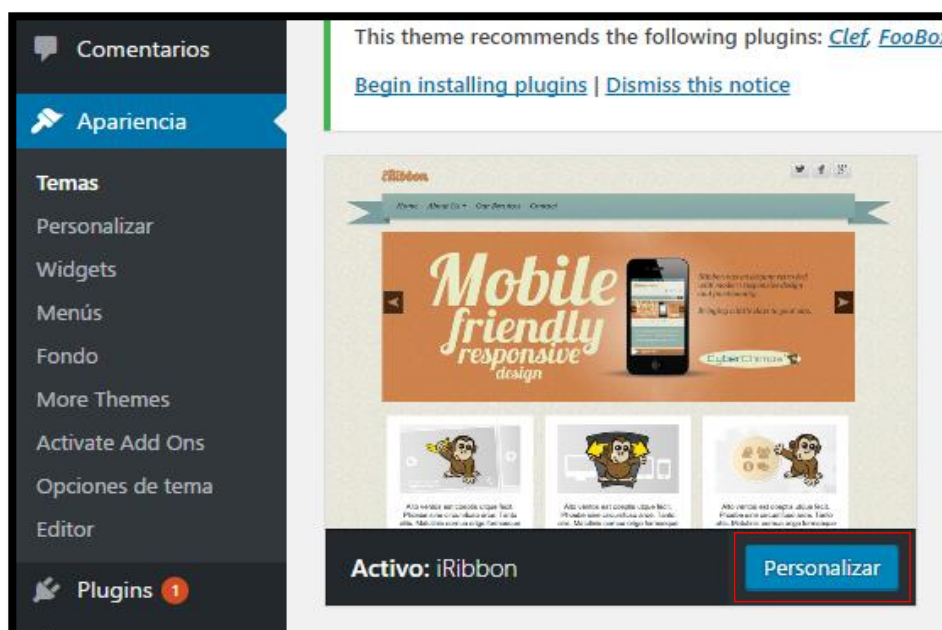


Imagen 07 – Personalización del tema

6. Se mostrará el menú principal de configuración del tema escogido en la parte lateral izquierda y una vista previa del sitio web.



Imagen 08 – Menú principal de configuración

Menú de configuración del tema

Identidad del sitio

7. En la opción identidad del sitio se debe especificar el nombre de la institución, se debe escribir una pequeña descripción de la misma y escoger un icono para el sitio.

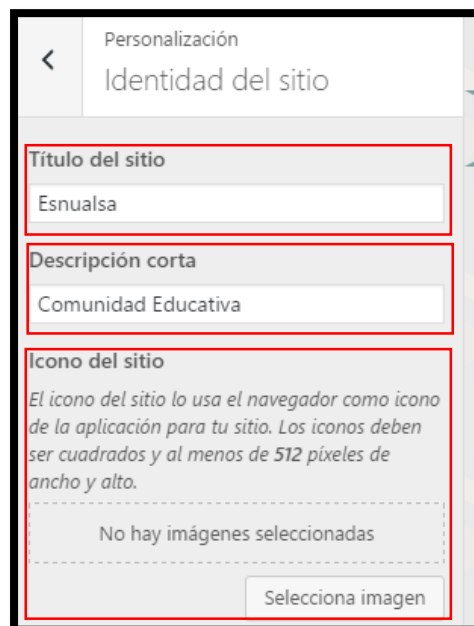


Imagen 09 – Identidad del sitio

Insertar una imagen en el tema

8. Dar click en el botón selecciona imagen.

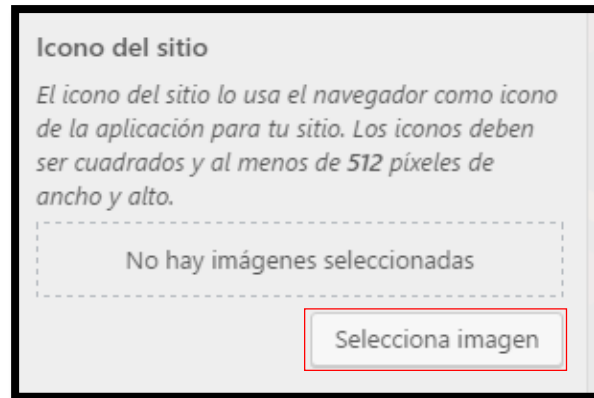


Imagen 10 – Configuración del icono del sitio

9. Se abrirá una ventana nueva, elegir la opción subir archivo y luego dar click en el botón selecciona archivos. En la parte inferior del botón hace referencia al tamaño que deben tener las imágenes a subir.



Imagen 11 – Subida de imagen al web

10. Se abrirá la ventana para buscar la imagen a subir, una vez seleccionada dar click en el botón abrir.

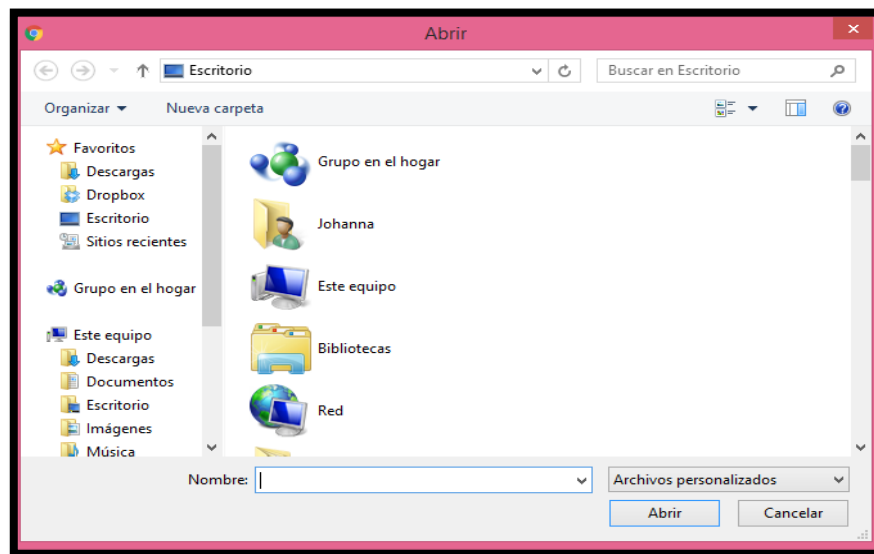


Imagen 12 – Buscando imagen para subir al sitio web

Si no excede del tamaño establecido, la imagen se agregará automáticamente a la biblioteca multimedia del tema, luego dar click en el botón elegir y esta se añadirá.

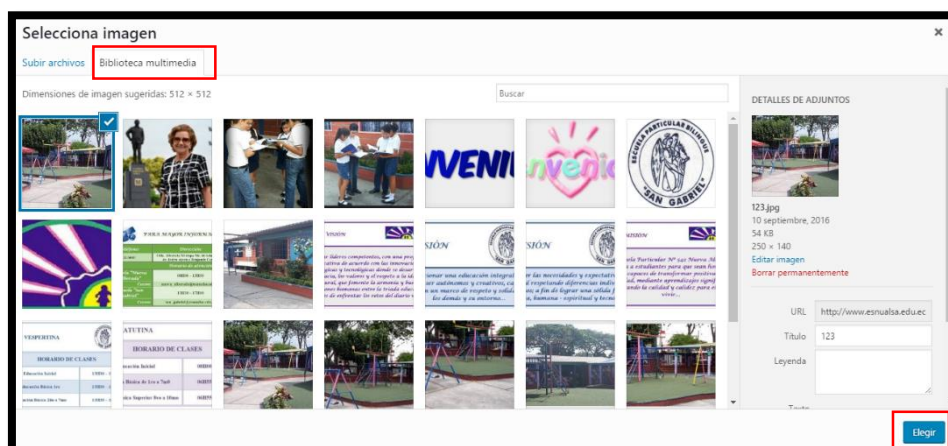


Imagen 13 – Biblioteca multimedia del sitio

Este proceso será el mismo para todas las opciones donde el tema permita colocar una imagen en su personalización.

Guardar cambios

11. Una vez hecho los cambios correspondientes, para guardarlos se debe dar click en el botón guardar y publicar, para guardar los cambios realizados y

actualizar el sitio web. Esto deberá repetirse cada vez que se realice un cambio.

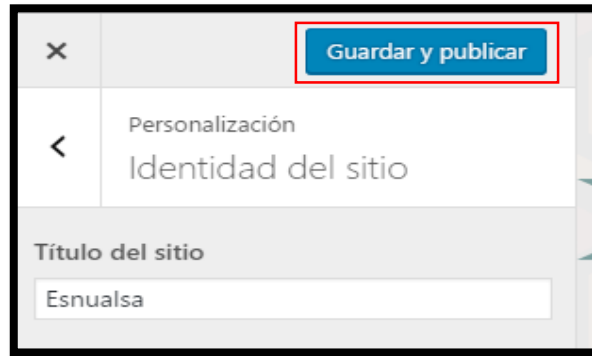


Imagen 14 – Guardar cambios

Layout

12. En la opción Layout (Diseño) escoger lo que podrá contener el sitio web. Marcar las opciones que se deseen. Definir también la anchura de la barra lateral.

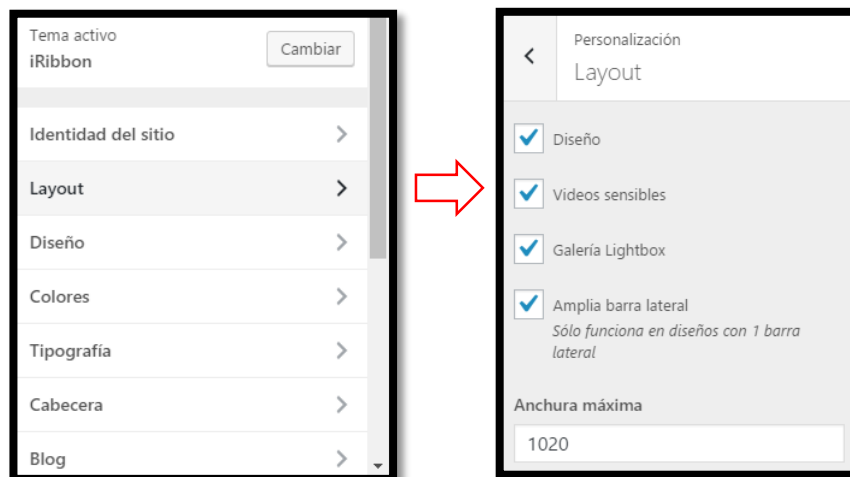


Imagen 15 – Opciones de diseño del sitio web

Diseño

13. En la opción diseño, dar click y se mostrara tres opciones para cambiar el color del texto, de los vínculos y los enlaces.

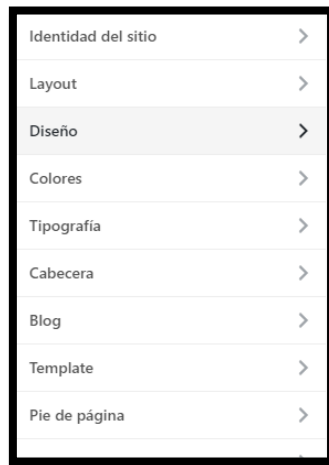


Imagen 16 – Opción de diseño

14. Dar click en la opción elegir color y se desplegará un recuadro con los diferentes colores que se puede escoger, seleccionar el color y guardar los cambios. Es el mismo proceso en las tres opciones.

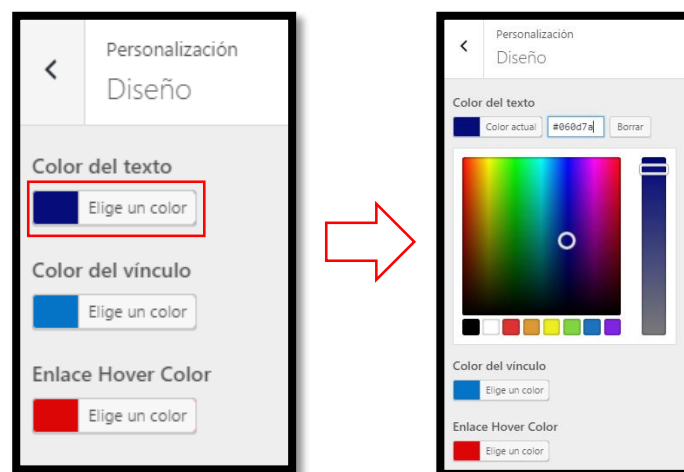


Imagen 17 – Paleta de colores

Colores

15. En la opción colores dar click para cambiar el color de fondo del tema, después dar click en el botón elegir un color y seleccionar el color al gusto.



Imagen 18 – Selección de colores del texto

Tipografía

16. En la opción tipografía dar click, se mostrarán diferentes opciones para cambiar el tipo de letra que se utilizará en el sitio.

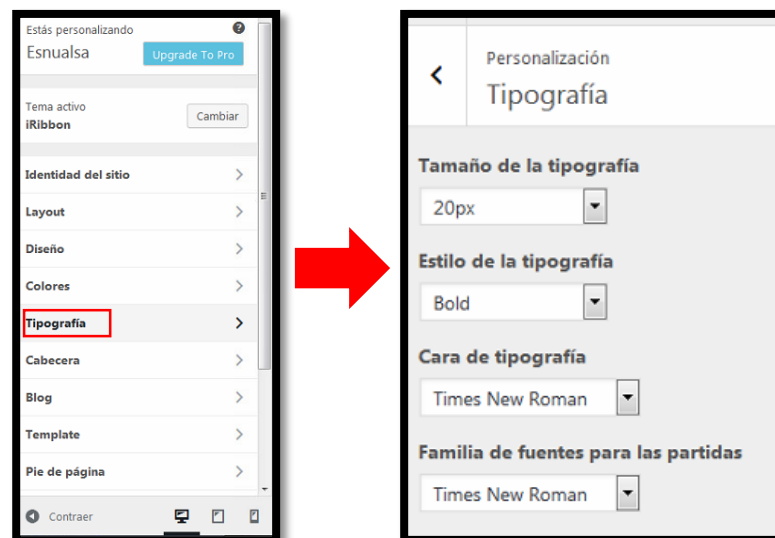


Imagen 19 – Selección del tipo de tipografía

Se mostrará opciones para cambiar el tamaño, el estilo de la tipografía de las diferentes secciones del sitio web, se da click en el botón que tiene una flecha apuntando hacia abajo y se desplegara las opciones para escoger.

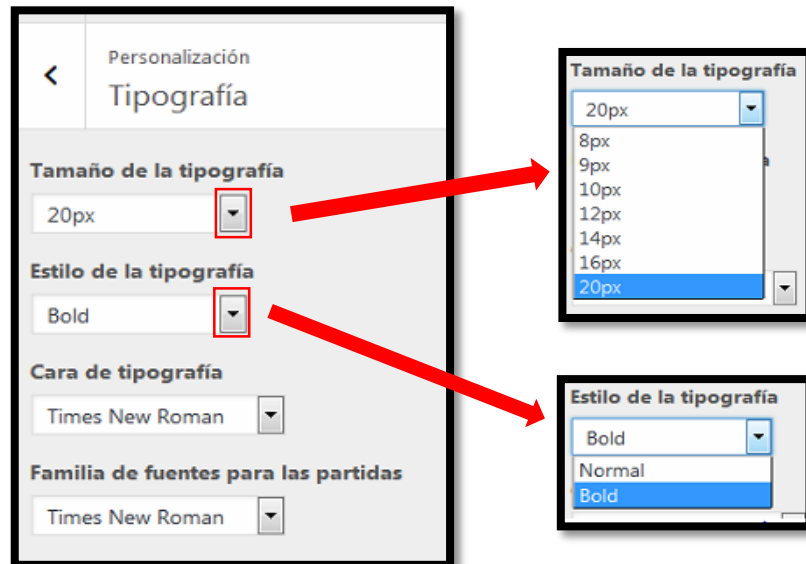


Imagen 20 – Modificación de la tipografía del sitio

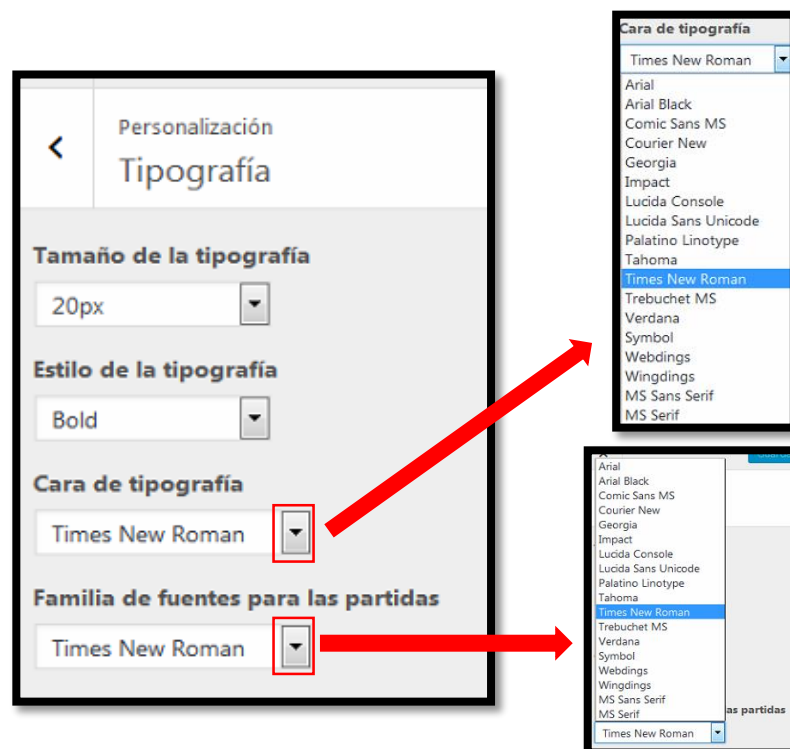


Imagen 21 – Tipos de letras

Cabecera

17. Dar click en la opción cabecera, se mostrarán dos opciones de configuración.

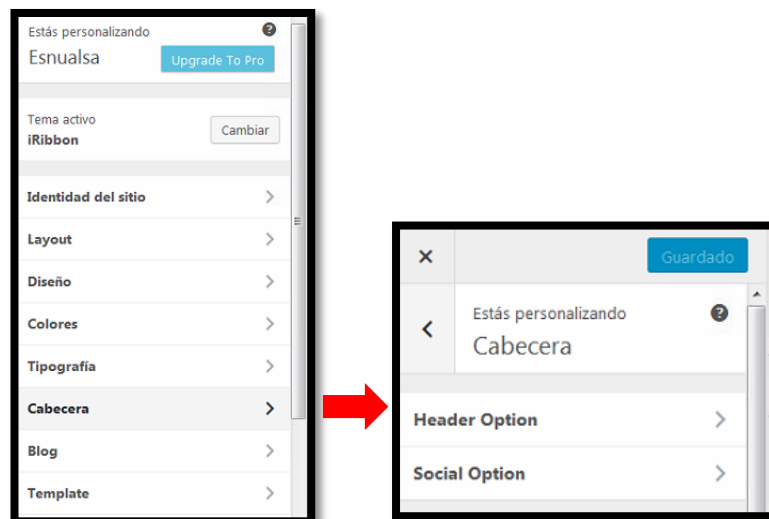


Imagen 22 – Configuración de la cabecera

18. En la opción Header Option se mostrará un menú de opciones para configurar en la cabecera del sitio web. La primera es la configuración del icono del sitio y la dirección enlazada al mismo. En este caso no se utilizó ningún icono para el sitio web. Pero en caso de requerirse marcar en Display logo, seleccionar la imagen y escribir la dirección de enlace en el Enter Custom Logo URL. Al dar click en el logo, se dirigirá a la dirección establecida.

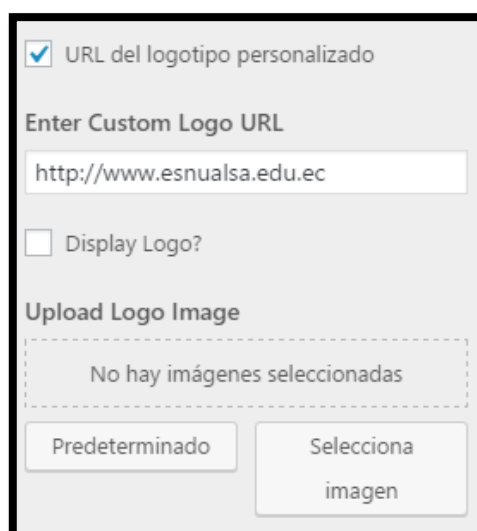


Imagen 23 – Configuración del loga de la cabecera

19. La segunda opción de configuración es el Favicon. En caso de utilizarse marcar la opción Display Favicon y elegir la imagen.

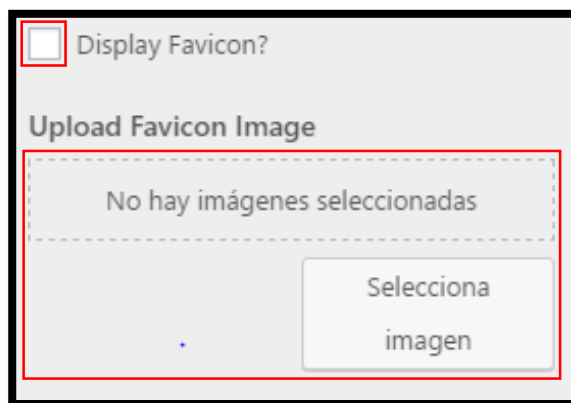


Imagen 24 – Configuración del Favicon

20. La segunda opción es el Custom Apple touch icon, en casa de requerirse marcar el Display Custom Apple touch ico y seleccionar la imagen.



Imagen 25 – Configuración del Custom Apple Touch

21. La tercera opción es la activación del buscador, marcar el Display Search.

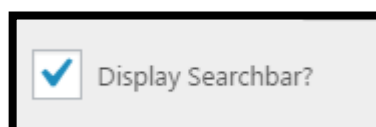


Imagen 26 – Configuración del buscador

22. En la opción Social Option, permite la activación de los iconos de los diferentes sitios sociales. Marcar el que se desee activar para el sitio.

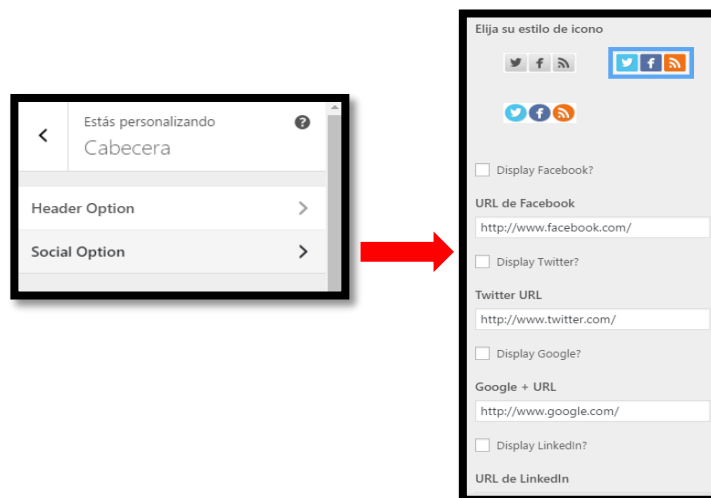


Imagen 27 – Configuración de redes sociales en el sitio web

23. En elección blog se encuentran todas las opciones para configurar las imágenes en la portada del sitio web.



Imagen 28 – Configuración blog

24. La opción Blog Slider Lite permite configurar las imágenes que van en slider de la portada del web site. Seleccionar las imágenes de la biblioteca.

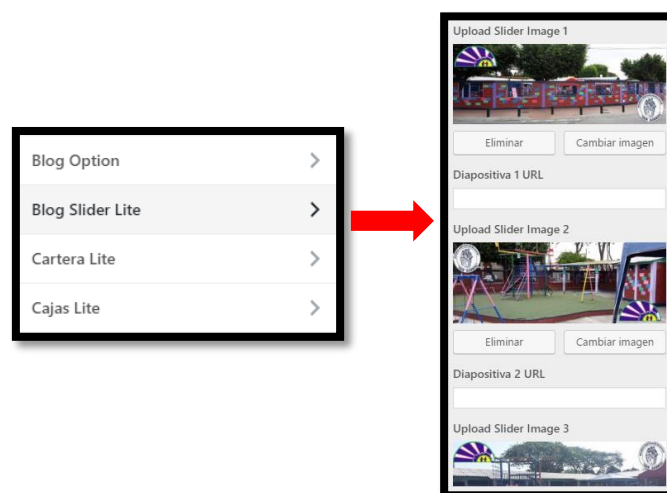


Imagen 29 – Configuración del slider

25. La opción Cajas Lite permite configurar los cuadros de imágenes de la portada del sitio web. Seleccionar las imágenes y hacer la descripción de cada una.

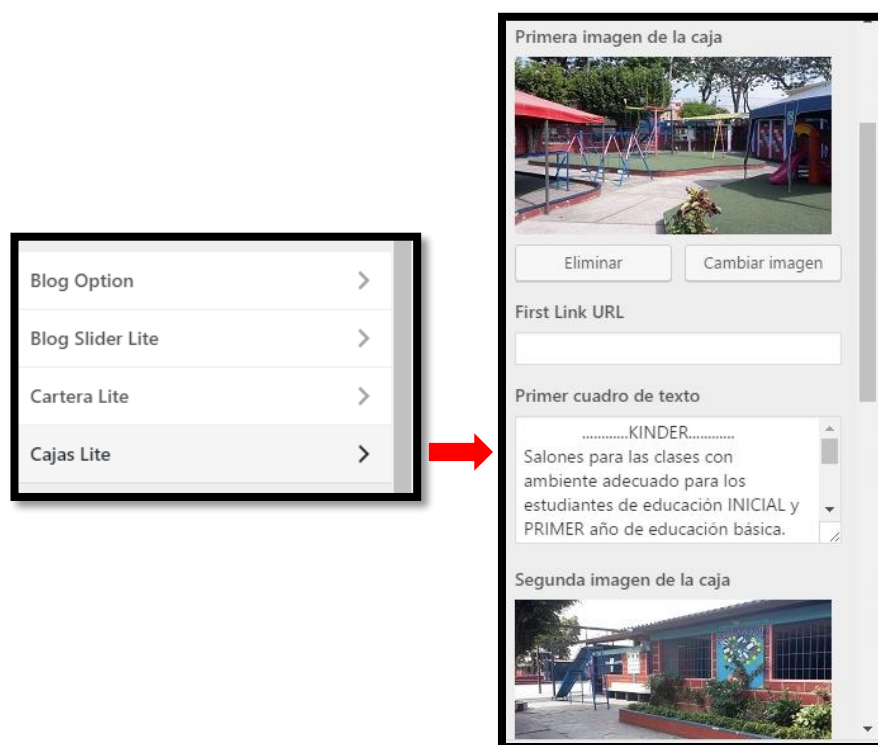


Imagen 30 – Configuración de Cajas Lite



Imagen 31 – Cajas Lite de la portada del sitio web

26. En la opción Pie de página configurar lo que se desea que se muestre al final de la página web. Escoger la opción de mostrar widgets o un texto

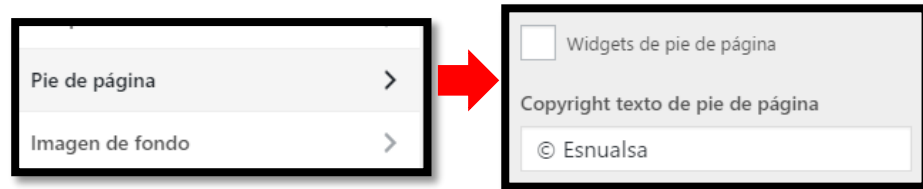


Imagen 32 – Configuración del pie de página

27. En la opción Imagen de fondo, seleccionar una imagen como fondo del sitio o escoger un fondo que viene por defecto en el tema del sitio.



Imagen 33 – Configuración del fondo

28. Opción de portada estática, permite establecer entradas o páginas para que siempre se mantengan en la portada del sitio.

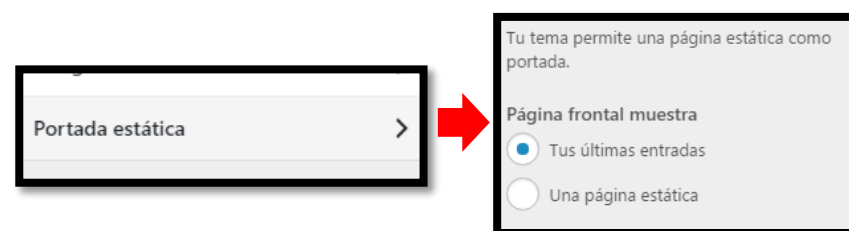


Imagen 34 – Configuración de la portada estática

Escritorio del sitio web

29. En el escritorio del sitio web se muestra un menú lateral con diferentes opciones.

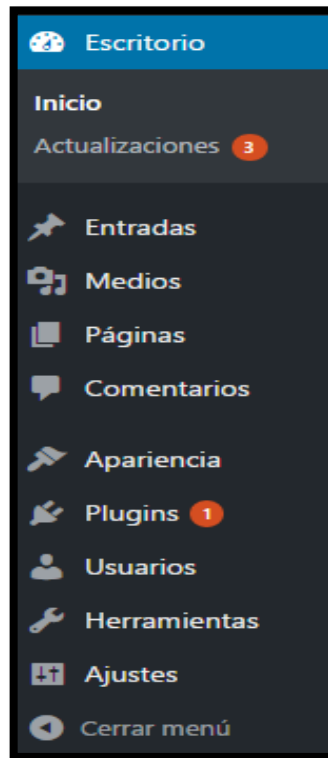


Imagen 35 – Menú de escritorio

Entradas

30. En el menú lateral tenemos las entradas. Para añadir una nueva, dar click en entradas después en añadir nueva. Al finalizar la edición presionar publicar y se crea la entrada.

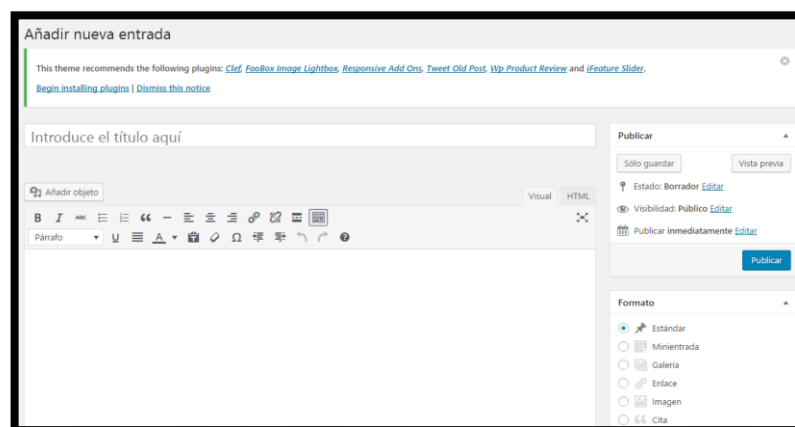


Imagen 36 – Creación de entradas

Páginas

31. Para crear una página seleccionar la opción páginas del menú del escritorio después en añadir nueva. Al finalizar la edición presionar el botón publicar.

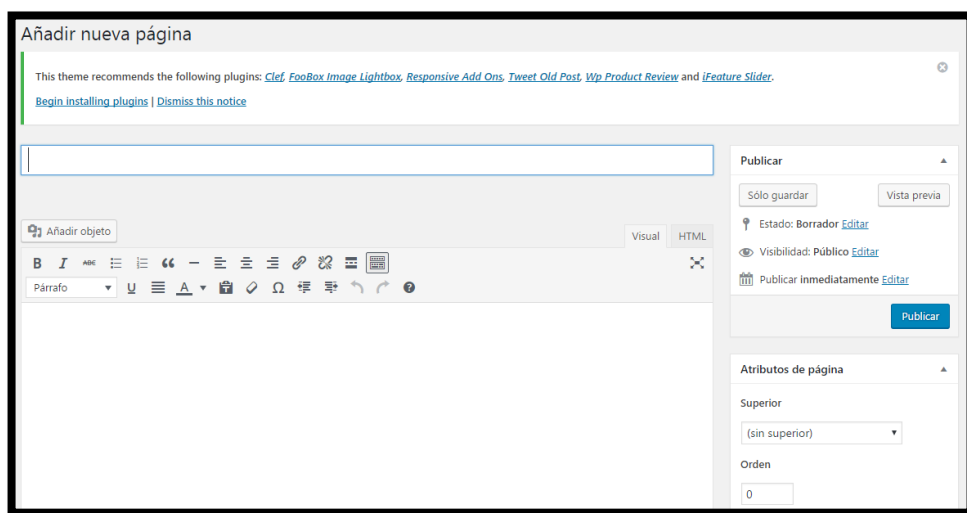


Imagen 37 – Creación de páginas

Medios

32. En la opción medios del menú lateral se almacenan todas las imágenes, videos, recursos multimedia que se utilicen en el sitio web y añadir nuevos.

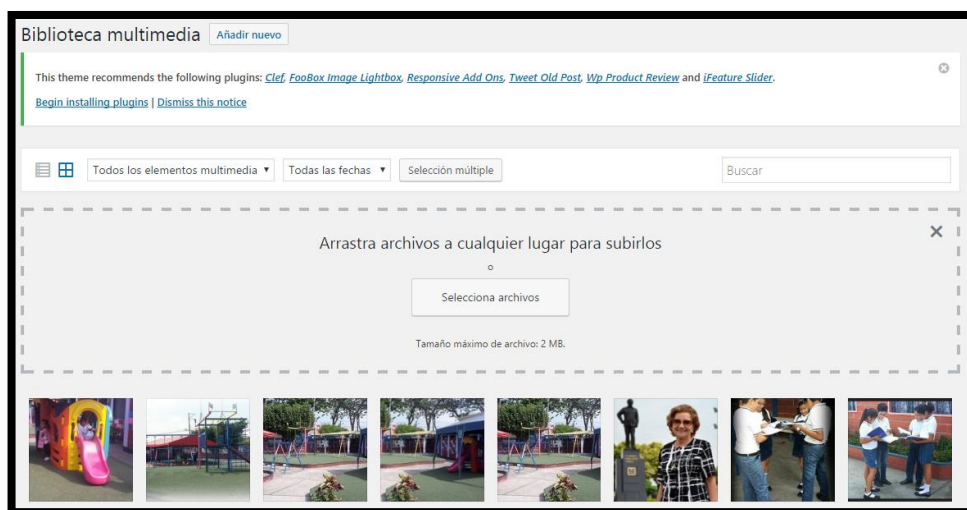


Imagen 38 – Recurso multimedia del sitio

Apariencia

33. En la opción apariencia encontramos una lista de opciones para configurar el tema del sitio web descritos anteriormente.

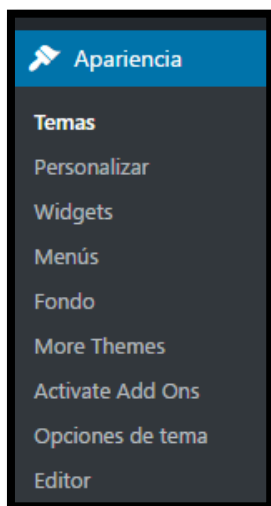


Imagen 39 – Menú apariencia

34. La opción Menús, permite crear menú principal y menú lateral. Seleccionar la opción crear menú, escribir el nombre del menú y dar click en el botón crear menú.

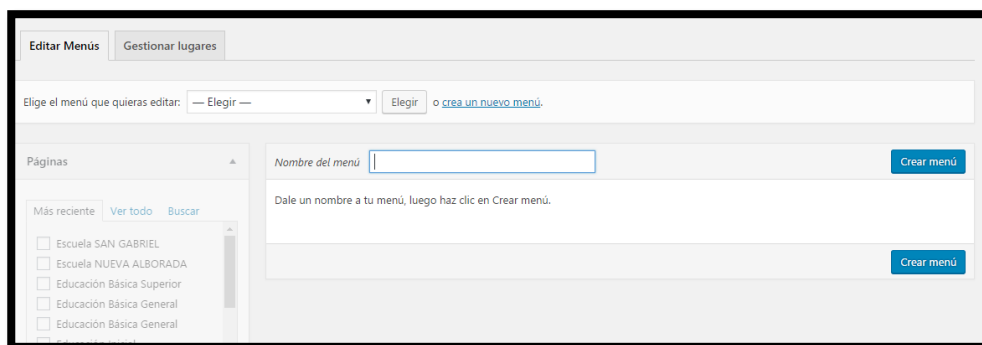


Imagen 40 – Creación de menú

35. Añadir las páginas que formaran parte del menú con respectivos niveles, en la parte lateral izquierda marcar la página que se desea añadir y dar click en el botón agregar al menú. Para guardar los cambios dar click en el botón guardar menú..

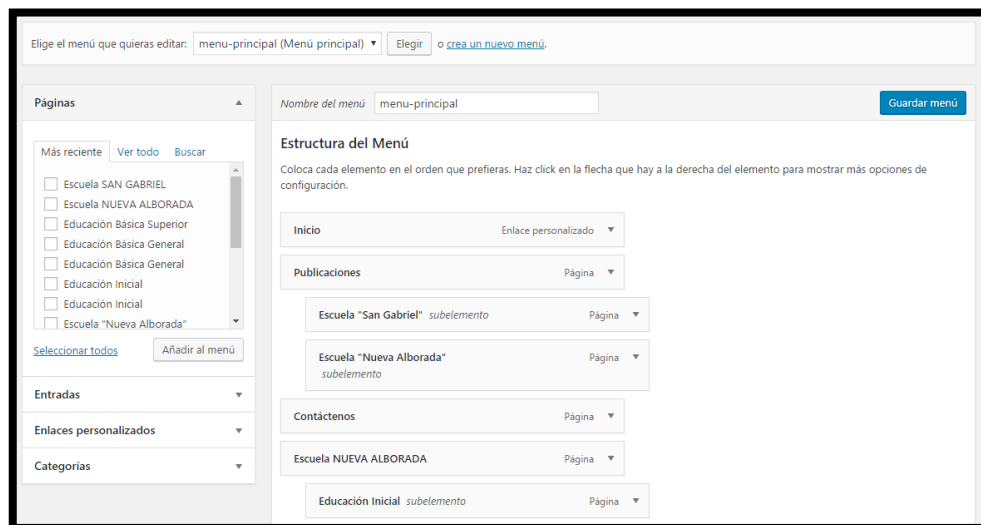


Imagen 41 – Configuración del menú

36. Para determinar la ubicación del menú, seleccionar la opción Gestionar lugares y seleccionar el menú que se desea que sea el principal. Presionar el botón guardar cambios para guardar los cambios.

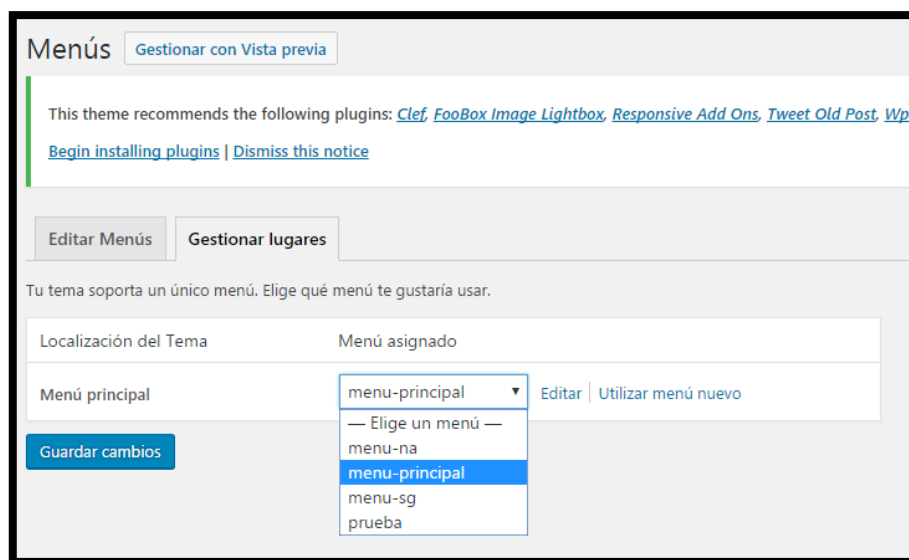


Imagen 42 – Selección del menú principal

37. La opción editor, muestra la ventana de configuración a base de código.



Imagen 43 – Ventana de codificación

Plugins

38. En la opción se muestran los diferentes plugins que pueden activarse para el sitio web. Marca el plugins a utilizar y dar el click en aplicar.

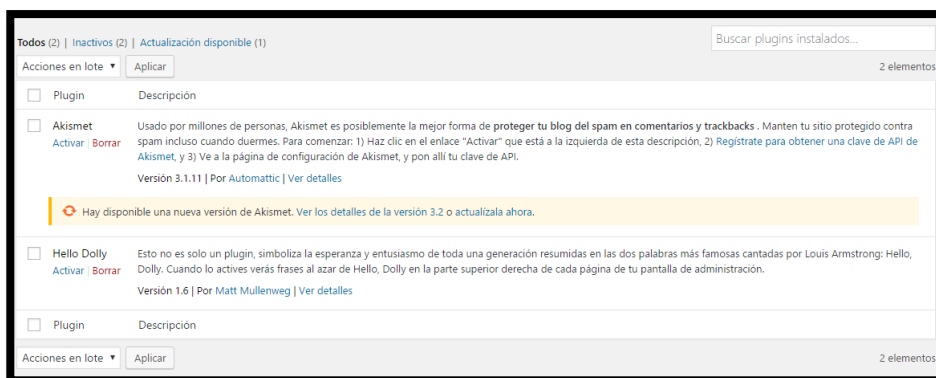


Imagen 44 – Activación de plugins

39. Para añadir un plugins, seleccionar la opción añadir nuevo y dar click en instalar en cualquiera de los plugins que se muestran, si se desea buscar seleccionar una de las opciones del menú de la parte superior y si se desea subir un plugins previamente descargado en el equipo seleccionar el botón subir plugins.

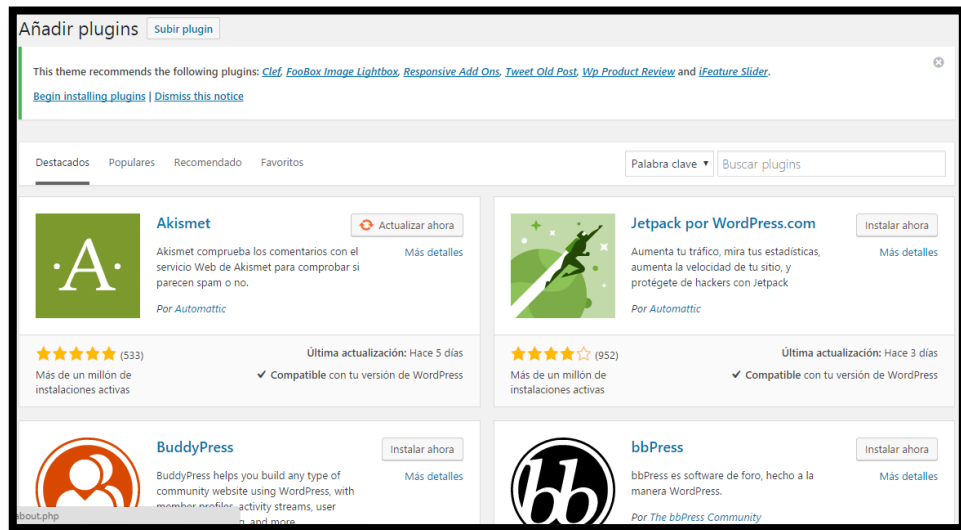


Imagen 45 – Selección de plugins en el sitio web

Usuario

40. En la opción usuario, se puede configurar los diversos usuarios que manejarán la página. El usuario que viene por defecto es admin.

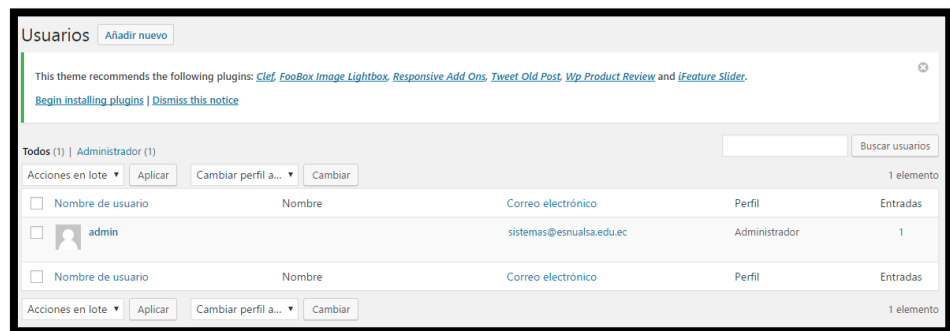


Imagen 46 – Configuración de usuarios

41. Para crear un nuevo usuario dar click en añadir nuevo y llenar los campos que se solicitan en el sitio web como nombre de usuario, contraseña, correo electrónico, escoger los privilegios a dar al usuario y presionar el botón añadir nuevo usuario ubicado en la parte inferior.

Crea un nuevo usuario y añádelo a este sitio.

Nombre de usuario *(obligatorio)*

Correo electrónico *(obligatorio)*

Nombre

Apellidos

Web

Contraseña [Mostrar contraseña](#)

Enviar aviso al usuario ☒ Envía al usuario nuevo un correo electrónico con información sobre su cuenta.

Perfil Suscriptor ▼

[Añadir nuevo usuario](#)

Imagen 47 – Creación de un nuevo usuario

Herramientas

42. En la opción herramientas se mostrarán las herramientas que se pueden activar en la página web.

Escritorio

Entradas

Medios

Páginas

Comentarios

Apariencia

Plugins 1

Usuarios

Herramientas

Herramientas disponibles

Importar

Exportar

Ajustes

Cerrar menú

Publicar esto

"Publica esto" es una herramienta que te permite capturar trozos de la web y crear nuevas entradas con facilidad.

Utiliza Publicar esto para copiar texto, imágenes y vídeos de cualquier página Web. Después corrige y añade más directamente desde Publicar esto antes de guardarlo o publicarlo en una entrada del sitio.

Instala Publicar esto

Marcador

Arrastra el marcador inferior a tu barra de marcadores. Entonces, cuando te encuentres en una página que quieras compartir, simplemente púlsalo.

Publicar esto

Enlace directo (mejor para móviles)

Haz clic en el enlace para abrir "Publicar esto". Una vez hecho, añádelo a los marcadores de tu dispositivo o pantalla de inicio.

Abrir "Publicar esto"

Imagen 48 – Ventana de herramientas

43. En la opción importar, muestra una lista de herramientas que se pueden importar para activar en el sitio web. Dar click en instalar ahora.



Imagen 49 – Importación de herramientas

Ajustes

44. En ajustes, mostrará una serie de opciones de configuraciones generales del sitio web.



Imagen 50 – Configuraciones generales

MANUAL DE USUARIO

WEBMIN

WEBMIN

Esta herramienta le permitirá a las docentes que imparten la asignatura de computación en la Comunidad Educativa ESNUALSA, tener un control sobre el uso del internet por parte de los estudiantes.

Para cada jornada existirá un usuario distinto con permisos de uso para su respectiva franja horaria laboral, además por cuestiones de seguridad únicamente se tendrá acceso a esta herramienta desde la computadora asignada a la docente de computación y se cerrará sesión después de 15 minutos de inactividad.

Previo a su uso, se debe tener conocimiento sobre los archivos creados y el contenido del mismo.

Existe una carpeta llamada **reglas** que se encuentra en la ruta /etc/squid, y contiene varios archivos, pero para este manual se hará hincapié en estos:

- **ip_navegacion:** Direcciones IP con permisos para navegar con ciertas restricciones
- **ip_estudiantes:** Direcciones IP con restricciones de navegación.

Además dentro de **reglas** existe una carpeta llamada **listas** que contiene los siguientes archivos:

- **palabras-prohibidas:** Archivo con lista de palabras que al ponerlas en el navegador saltará el proxy.
- **redes-sociales:** Archivo con direcciones web de redes sociales que están bloqueadas.
- **restringidas:** Archivo con sitios web a los cuales que no se tendrá acceso.
- **sitios-inocentes:** Archivo con sitios web que no se requiere sean bloqueados por el servidor.
- **updates:** Archivo con sitios web que usan las computadoras para descargar actualizaciones.
- **videos:** Archivo que contiene sitios bloqueados de servidores de video.

45. Acceder a WEBMIN

Abrir una ventana del navegador y digitar lo siguiente:

<https://srvfw.esnualsa.edu.ec:10000/>

Insertar nombre de usuario y contraseña asignados.

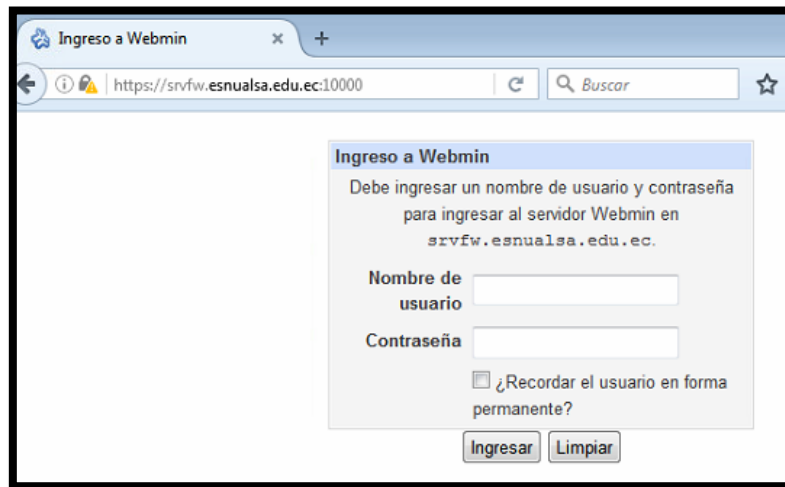


Imagen 51 – Login de Webmin

46. Aparecerá la ventana principal de WEBMIN con la información del servidor.

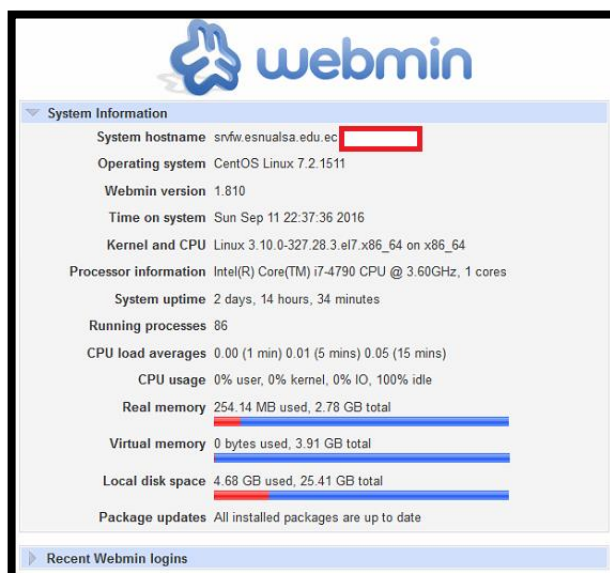


Imagen 52 – Información de Webmin

47. En la parte izquierda hay una opción llamada **Servidores** al presionarla se debe elegir **Squid-Servidor Proxy** y aparecerá un ícono para editar los archivos de configuración.

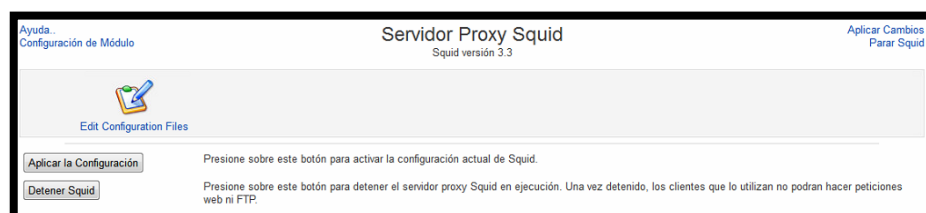


Imagen 53 – Servidor Proxy Squid

48. Archivos de configuración

Seleccionar el ícono **Edit Configuration Files** y a continuación se mostrarán todos los archivos mencionados al principio de este manual

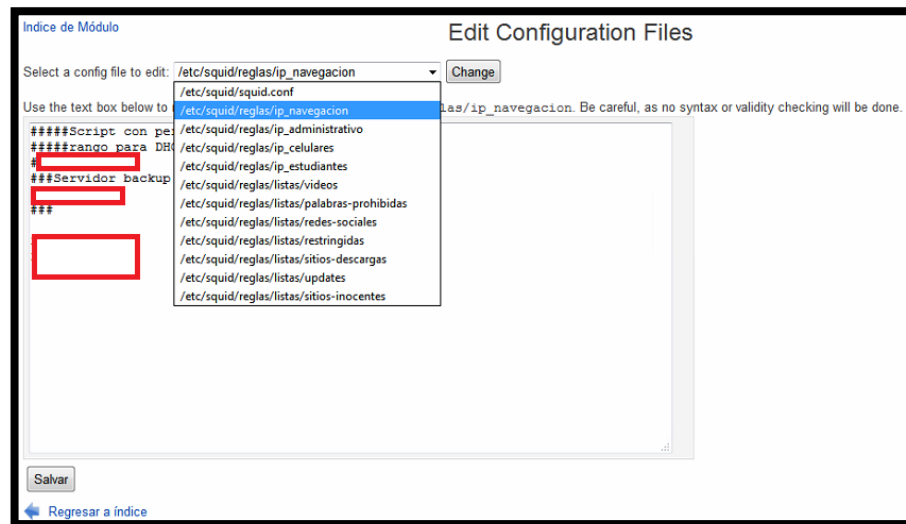


Imagen 54 – ip_navegacion

49. Seleccionar el archivo **ip_estudiantes** y presionar el botón **Change** para editar.

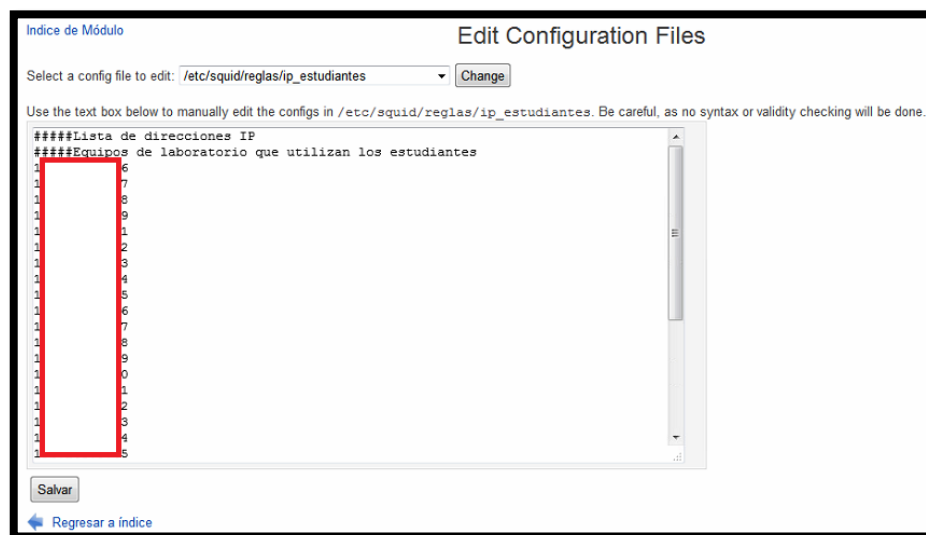


Imagen 55 – ip_estudiantes

En este archivo se alojan todas las direcciones IP de las computadoras que se encuentran en el laboratorio de computación y son utilizadas por los estudiantes.

Las docentes tendrán un listado con las direcciones IP para que puedan identificar a que computadora corresponde cada una.

50. Permitir el acceso a Internet

Si se requiere dar acceso a un estudiante o a un determinado grupo de estudiantes acceso a internet, en el archivo **ip_estudiantes** se debe **comentar** con un # al inicio de las IP deseadas y luego presionar el botón **Salvar** para guardar los cambios.

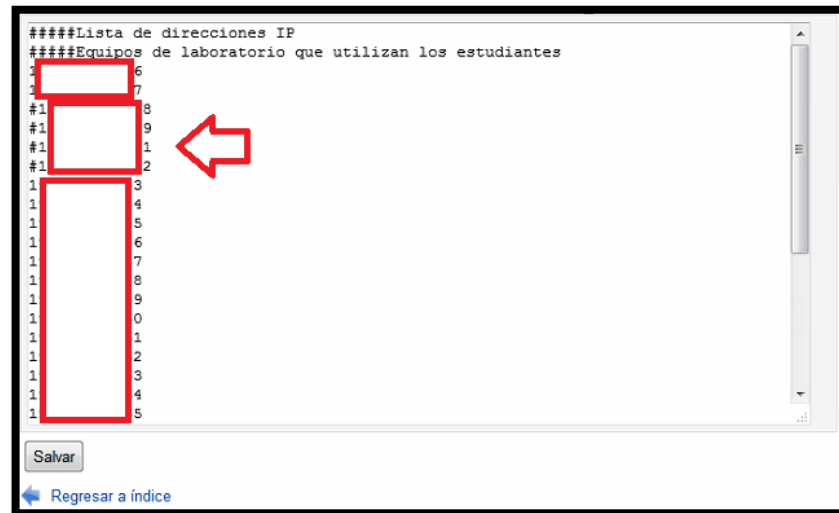


Imagen 56 – ip_estudiantes IPs comentadas

51. Dirigirse al archivo **ip_navegacion** y escribir las direcciones que se comentaron anteriormente, presionar el botón **Salvar** y luego presionar el botón **Aplicar la Configuración**.

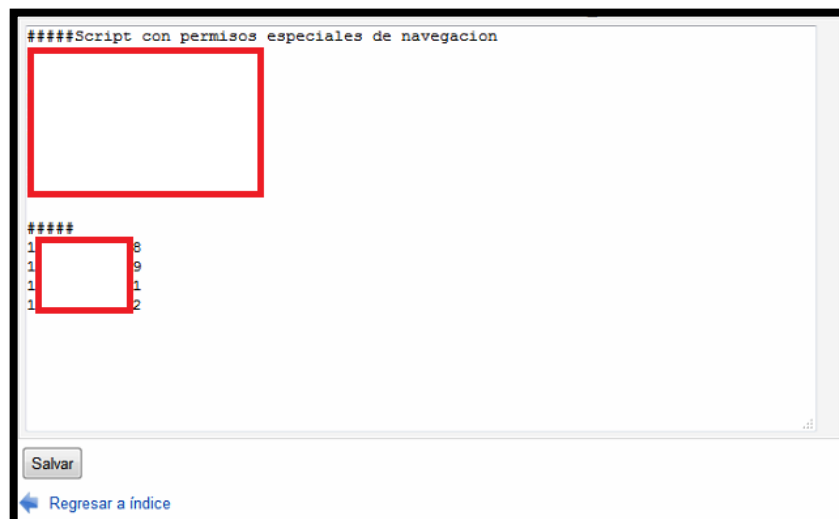


Imagen 57 – ip_estudiantes IPs comentadas

52. Solicitar a los estudiantes que realicen pruebas de navegación, estas serán exitosas sin duda.

MANUAL DE USUARIO

SERVIDOR DE CORREO

SERVIDOR DE CORREO

1. Ingresar a Zimbra

Abrir una ventana del navegador y digitar lo siguiente:

<https://mail.esnualsa.edu.ec:8443/>

Insertar la cuenta y contraseña asignadas.



Imagen 58 – Ventana de Login de Zimbra

2. Se abrirá la ventana principal con la bandeja de entrada.

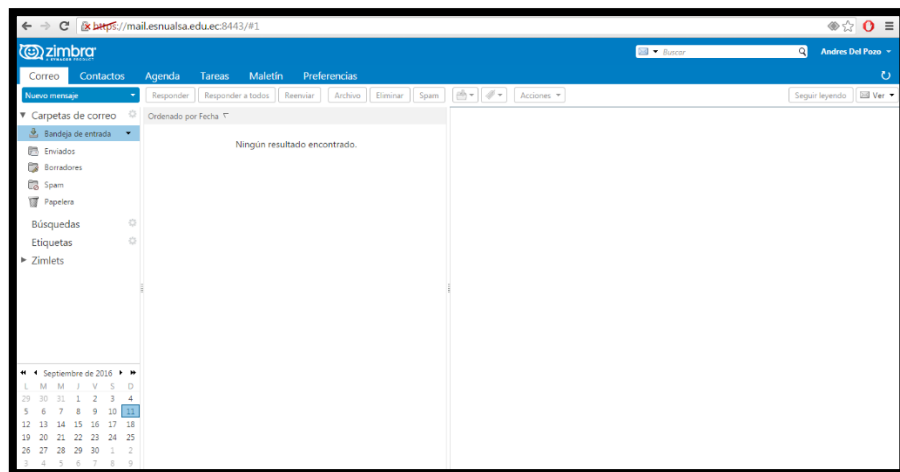


Imagen 59 – Ventana principal de Zimbra

3. Enviar un nuevo mensaje

En la parte superior derecha se encuentra la opción **Nuevo mensaje** y presionarla, automáticamente dentro del zimbra se abrirá una nueva pestaña para redactar el nuevo correo.

Es similar a cualquier servidor de correo gratuito (Hotmail, gmail, yahoo) se colocará la dirección de correo a la cual se enviará el mensaje, el asunto, un adjunto en caso de ser necesario y el cuerpo con el texto que necesite ser revisado por el receptor.



Imagen 60 – Redactando un correo

A continuación presionar el botón enviar y aparecerá un cartel amarillo con la leyenda **Mensaje Enviado**.

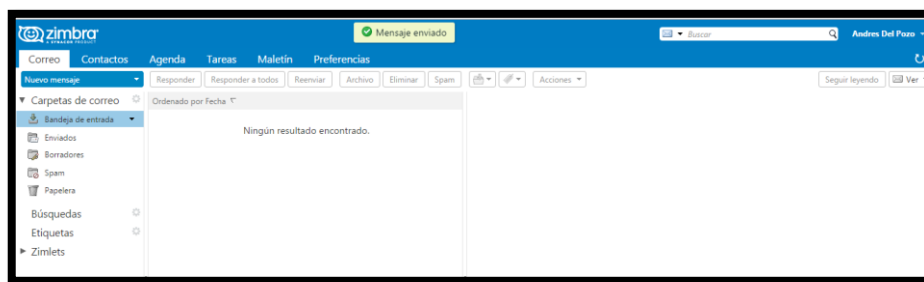


Imagen 61 – Mensaje enviado

4. Al ser esta una prueba, se confirmará que se recibió el correo y se lo responderá

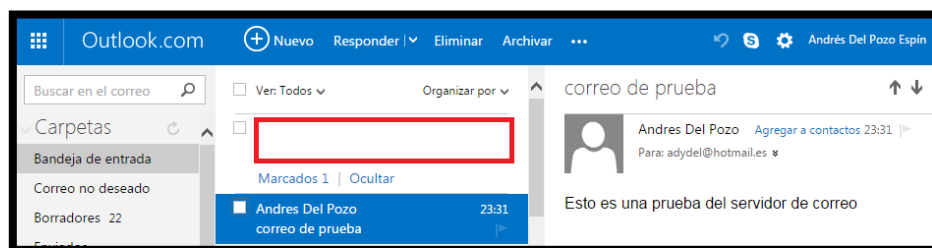


Imagen 62 – Mensaje visto desde el receptor

Se procedió a responder el correo, para ser visto desde la bandeja de entrada del Zimbra.

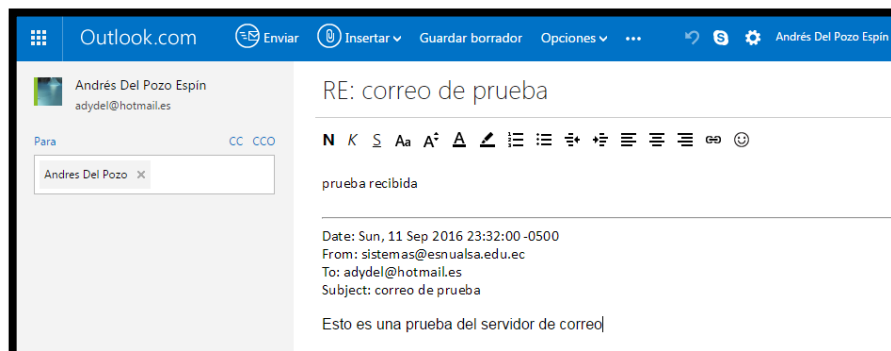


Imagen 63 – Respondiendo el correo

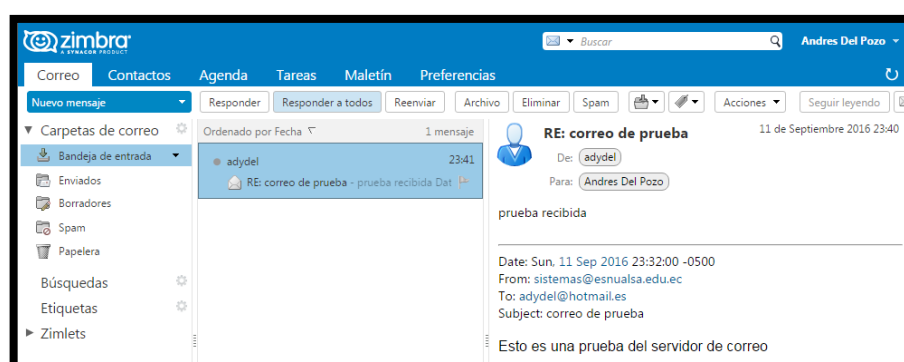


Imagen 64 – Correo recibido

5. Contactos

En esta pestaña se puede añadir contactos con un nombre determinado para que se pueda identificar rápidamente a una persona cuando se envíe o reciba un correo.

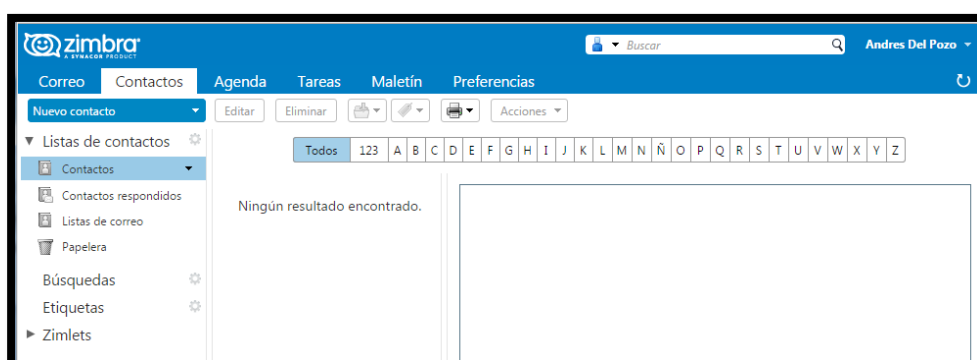


Imagen 65 – Contactos

6. Agenda

En esta pestaña se puede realizar lo mismo que en cualquier otro servidor de correo gratuito, colocar recordatorios de fechas importantes que el usuario necesite recordar a futuro.

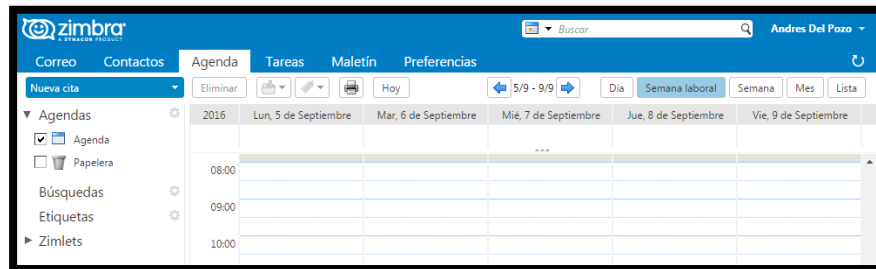


Imagen 66 – Agenda

7. Tareas

En esta pestaña se puede incluir notas o textos que se requieran encontrar más rápido que enviarse un correo y luego buscarlo en la bandeja de entrada.

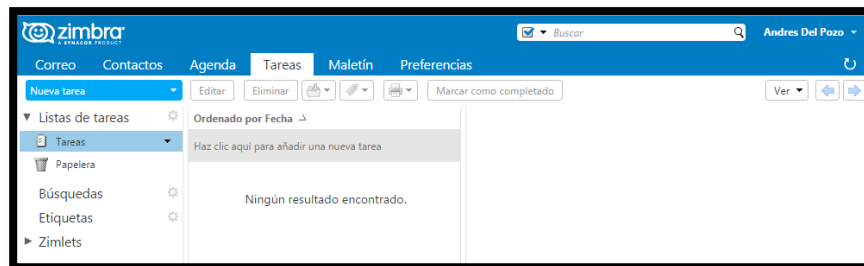


Imagen 67 – Tareas

8. Maletín

En esta pestaña se puede almacenar archivos de cualquier tipo que no sobrepasen del límite permitido, los mismos que se pueden descargar desde cualquier lugar ya que se almacenan en el servidor.

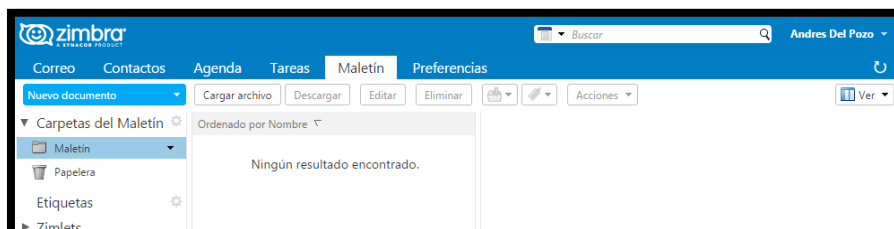


Imagen 68 – Maletín

9. Preferencias

Esta pestaña contiene varias opciones para ser configuradas al gusto del usuario, estas son:

- **General:** Contiene opciones de la apariencia, zona horaria, idioma y formas de búsqueda.
- **Cuentas:** En caso de poseer dos cuentas esta opción sirve para añadir la segunda cuenta y permitir enviar correos desde ambas cuentas sin necesidad de tener dos sesiones abiertas.
- **Correo:** Tiene las opciones de cómo se desea visualizar los correos en las bandejas, colores, tipos de letra, tamaño, etc.
- **Filtros:** Permite crear filtros para determinados correos y tener las bandejas mejor ordenadas.
- **Firmas:** Permite diseñar una firma que se colocará automáticamente cuando se envíe un correo.
- **Fuera de la oficina:** Esta opción permite enviar una respuesta automática en caso de recibir un correo en un determinado horario cuando el usuario no esté revisando su cuenta.
- **Direcciones fiables:** Con esta opción se podrá añadir direcciones de correo de las cuales se reciban archivos adjuntos que no se puedan visualizar y requieran una aprobación.
- **Contactos:** Permite realizar configuraciones sobre los contactos.
- **Agenda:** Permite realizar configuraciones sobre la agenda.
- **Compartir:** Esta opción sirve para administrar todas las carpetas que el usuario haya compartido, o carpetas que compartieron otros usuarios con el dueño de esta cuenta.
- **Notificaciones:** Permite enviar una notificación a otro correo.
- **Importar/Exportar:** Esta opción permite importar o exporta un determinado archivo, correo, contacto, etc.
- **Accesos directos:** Son combinaciones de teclas para que el usuario pueda acceder más rápido a un determinado lugar dentro del zimbra.
- **Zimlets:** Son complementos de aplicaciones que mejoran la funcionalidad de la aplicación.

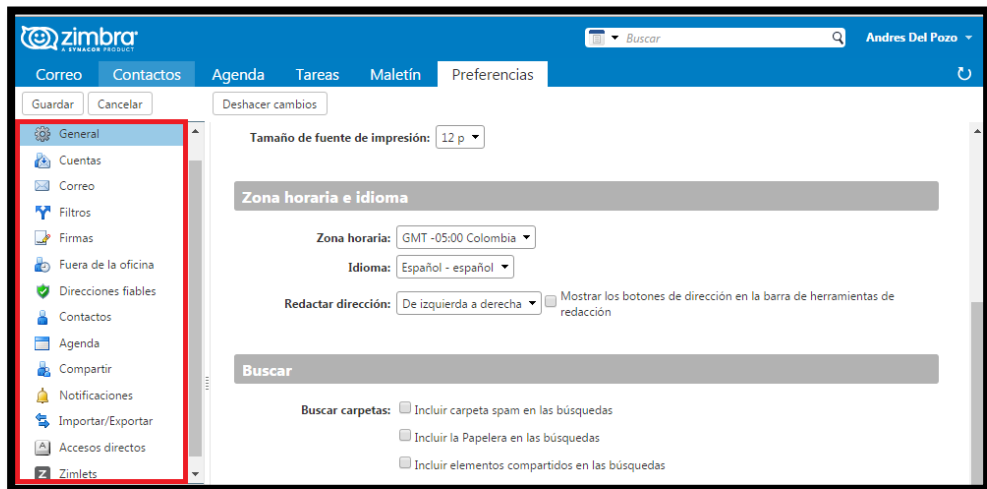


Imagen 69 – Maletín

Sea cual sea la opción que se haya modificado en esta pestaña, no olvidar presionar el botón Guardar que se encuentra en la parte superior izquierda, para conservar los cambios.

MANUAL DE USUARIO

SISTEMA CCTV

SISTEMA CCTV

1. Ingresar al DVR por medio de Internet Explorer

Abrir una el navegador Internet Explorer y digitar la dirección IP del DVR:
Insertar la cuenta y contraseña asignadas.

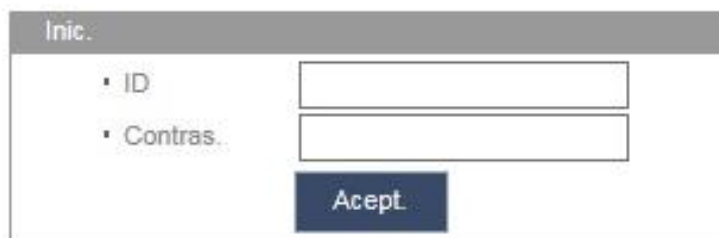
A screenshot of the DVR login window. It has a title bar with 'Inic.'. Below it, there are two input fields: the first is labeled 'ID' and the second is labeled 'Contras.'. Below these fields is a blue button labeled 'Acept.'. The window has a simple, functional design with a light gray background.

Imagen 70 – Ventana de Login del DVR

2. Una vez dentro aparecerán todas las cámaras para visualizar en vivo.

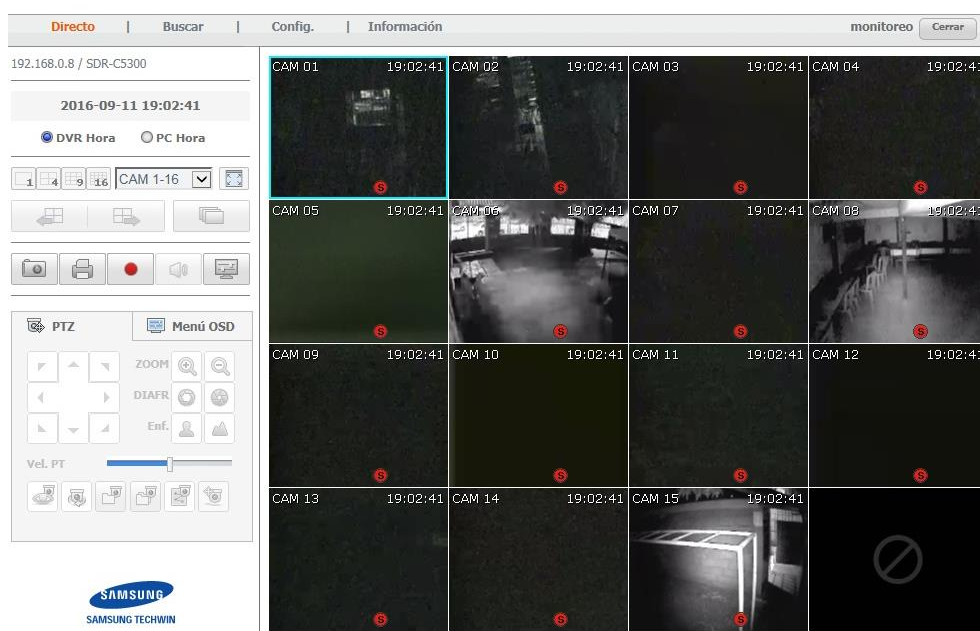


Imagen 71 – Ventana de monitoreo

3. Búsqueda de Video

En ocasiones existirá la necesidad de revisar un acontecimiento en una determinada fecha, para lo cual dentro de esta ventana se deberá seleccionar la opción Buscar, por defecto aparecerán las primeras imágenes del día en que se realiza la búsqueda.

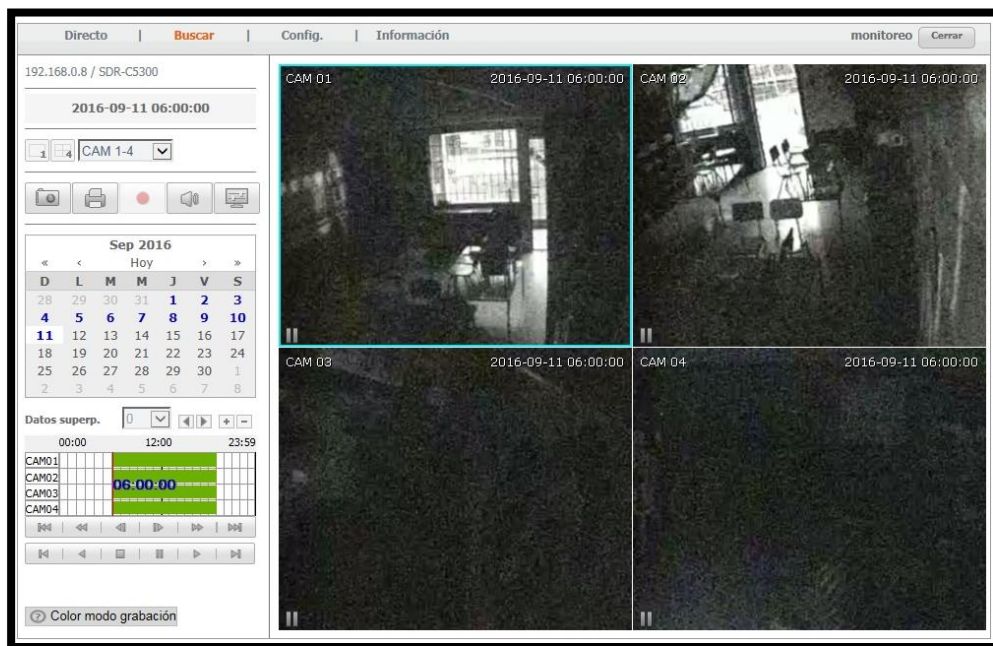


Imagen 72 – Ventana de búsqueda

4. A continuación se debe seleccionar la fecha, la hora y la cámara donde se suscitó el evento que se requiera revisar, presionar el botón **Reproducir** para visualizar.

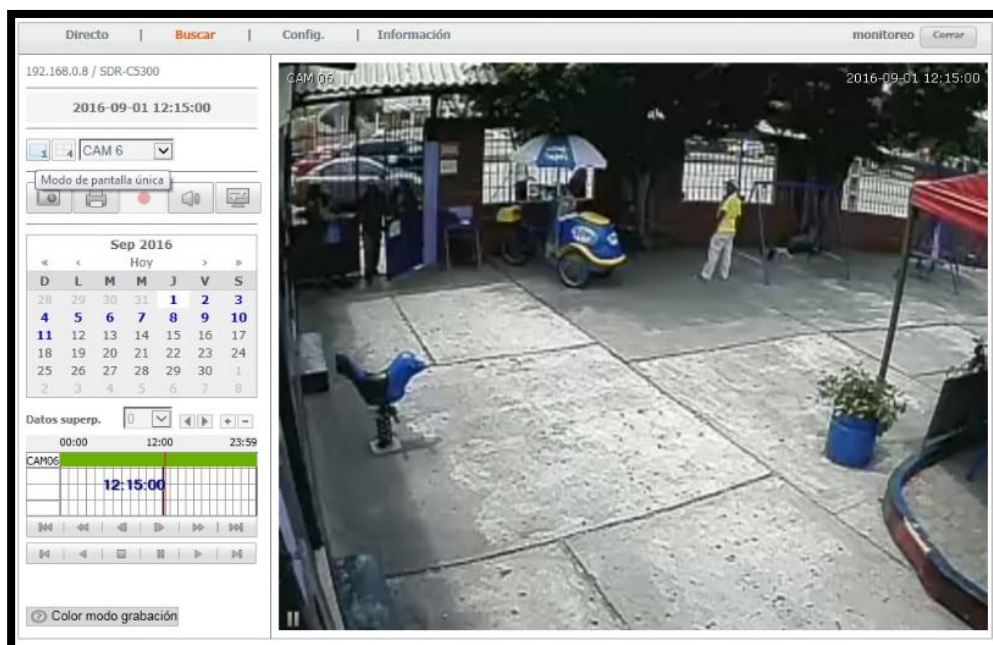


Imagen 73 – Búsqueda de un video

5. Ingresar al DVR por medio de Smart Viewer

Ejecutar el ícono de Smart Viewer y luego ingresar las credenciales asignadas para este programa.



Imagen 74 – Ícono de Smart Viewer



Imagen 75 – Login de Smart Viewer

6. Una vez dentro aparecerá el programa con todos los canales pero sin poder visualizarlos.

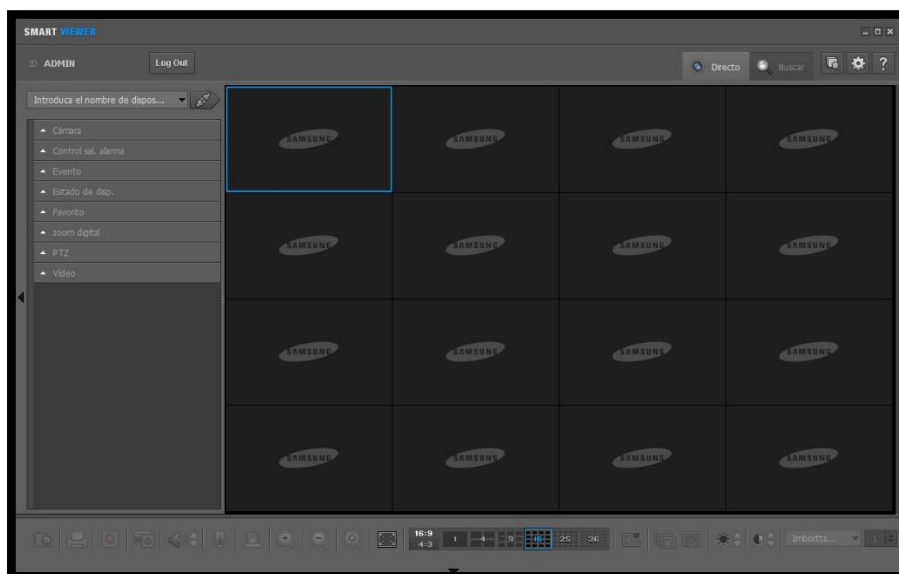


Imagen 76 –Smart Viewer

7. Para poder visualizar las cámaras se deberá presionar el botón **Conectar**.

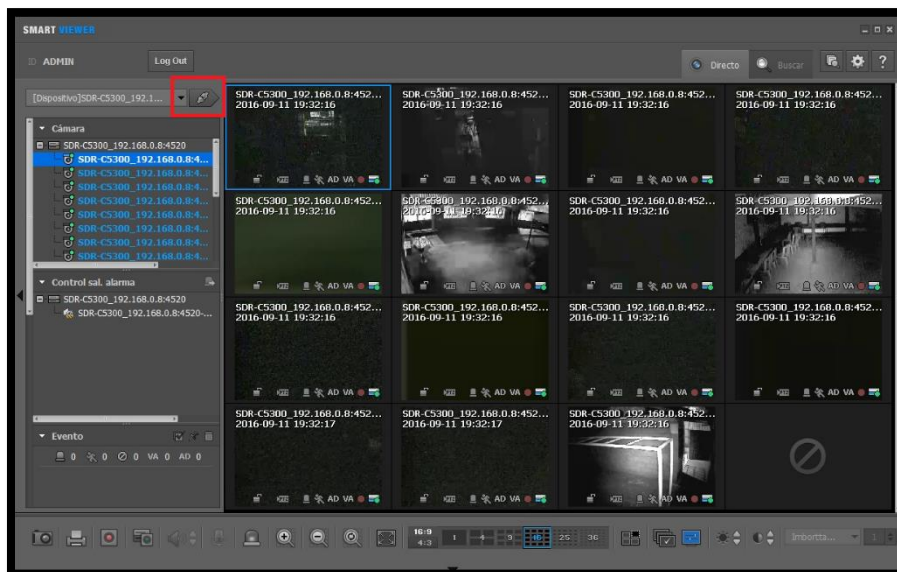


Imagen 77 –Smart Viewer visualización de cámaras

8. Búsqueda de Video

En este software para buscar un video, se debe seleccionar la opción **Buscar** que se encuentra en la parte superior derecha, una vez seleccionada se deberá elegir la fecha, hora y cámara para visualizar el evento. En caso de necesitar una copia de algún evento suscitado presionar el botón **Co Seg** que se encuentra en la parte inferior izquierda.

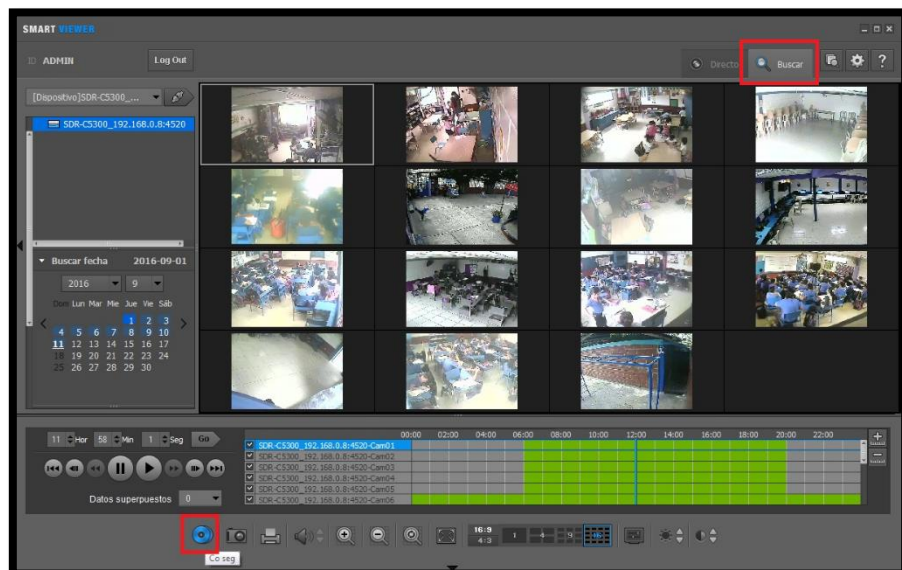


Imagen 78 –Smart Viewer búsqueda de video

9. Realizar una copia de seguridad

Una vez seleccionada la opción anterior se abrirá una ventana, en donde se deberá elegir la cámara, la hora exacta en que se suscitó el evento y la hora de finalización, por lo general suelen ser minutos de grabación los que se requieren, para esto se debe elegir la ruta donde se descargará el video y seleccionar el formato de archivo AVI, para que se pueda reproducir en cualquier equipo, una vez listo todo seleccionar el botón **Iniciar**.

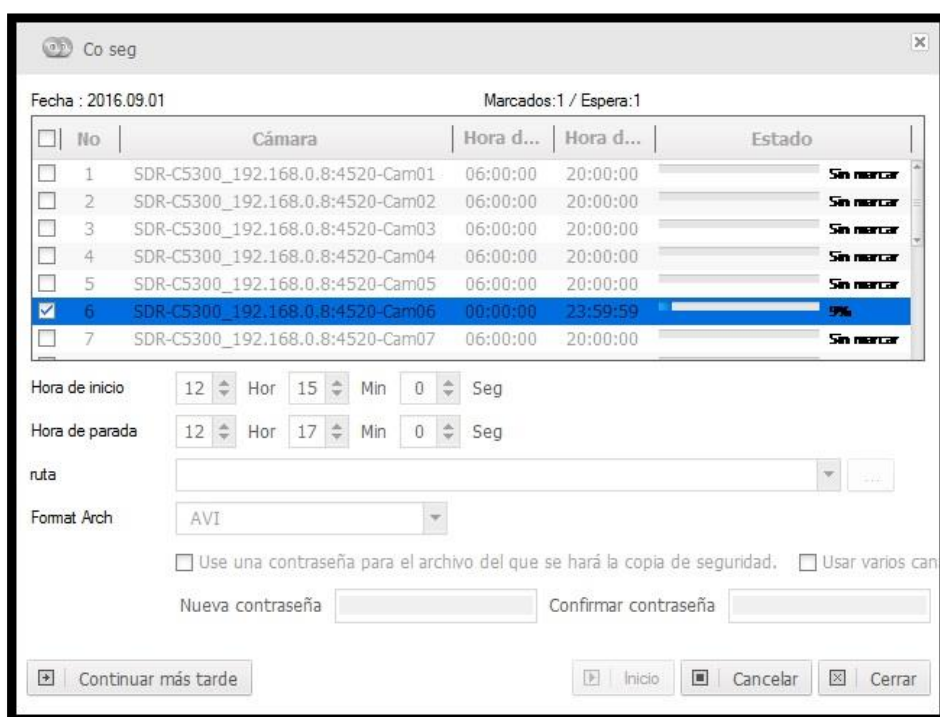


Imagen 79 – Copia de Seguridad

10. Una vez finalizado aparecerá un mensaje indicando que se terminó de realizar la copia y tendrá dos botones, uno para ir a la carpeta en donde se descargó y el otro para cerrar. Presionar el primer botón y reproducir el video.



Imagen 80 – Ícono del video descargado



Imagen 81 – Reproducción del video

Una vez obtenido el video ya es responsabilidad del usuario encargado el destino final del video.



UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD CCTV Y
VIRTUALIZACIÓN DE SERVIDORES FIREWALL – PROXY,
CORREO Y WEB PARA LA UNIDAD EDUCATIVA
ESNUALSA

MANUAL TÉCNICO
VIRTUALIZACIÓN DE SERVIDORES
SISTEMA DE CCTV

Previa a la obtención del Título de:

INGENIERO EN NETWORKING Y TELECOMUNICACIONES

AUTORES:

Wilson Andrés Del Pozo Espín

Johanna Alejandrina Hernández Páramo

GUAYAQUIL – ECUADOR
2016

ÍNDICE GENERAL

| | |
|--|-----------|
| INDICE GENERAL | II |
| MANUAL TÉCNICO VIRTUALIZACIÓN DE SERVIDORES | 1 |
| ESPECIFICACIONES TÉCNICAS | 2 |
| • Mainboard - Asus H87M-E | 2 |
| • Procesador – Intel Core I7 4790 | 2 |
| • Fuente de poder – Agiler AGI-PS800 | 3 |
| • HDD – Seagate | 3 |
| • Memoria – RAM 8GB | 4 |
| • Tarjetas de red – TP-Link TG-3468 | 4 |
| • Cooler – LYF Sleeve | 4 |
| • Pendrive – Kingston 8GB | 5 |
| • Case – Dipromacom | 5 |
| INSTALACIÓN DE LAS HERRAMIENTAS DE VIRTUALIZACIÓN | 6 |
| • Descarga del hypervisor | 6 |
| • Instalación del ESXi | 8 |
| INSTALACIÓN DE VMWARE VSPHERE CLIENT | 15 |
| • Configuración del vSphere Client | 19 |
| • Creación del Data Store | 28 |
| INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES | 30 |
| • Creación del Servidor Firewall | 30 |
| • Instalación y configuración del proxy. | 53 |
| • Opción maximum_object_size | 53 |
| • Opciones cache_swap_low y cache_swap_high | 53 |
| • Opción cache_mem | 53 |
| • Instalación y configuración de iptables | 54 |
| • Segmentación del ancho de banda | 61 |
| • Instalación de Webmin | 64 |
| CREACIÓN DEL SERVIDOR DE CORREO | 65 |
| • Instalación del sistema operativo | 71 |
| • Configuración del DNS | 77 |
| • Instalación de Zimbra | 81 |

| | |
|---|-----|
| • Creación de Cuentas | 85 |
| • Creación del Servidor Web | 87 |
| • Instalación de la máquina virtual | 87 |
| • Instalación del paquete para el servidor web. | 90 |
| • Instalación de la Base de Datos | 91 |
| • Instalación de phpmyadmin | 92 |
| • Instalación de WordPress | 93 |
| MANUAL TÉCNICO SISTEMACCTV | 98 |
| ESPECIFICACIONES TÉCNICAS | 99 |
| • DVR Samsung SDR-C5300 | 99 |
| • Control Remoto | 99 |
| • Cámaras Color Bullet | 99 |
| • Cámara tipo domo | 99 |
| • Cámaras Hikvision tipo tubo para exteriores | 100 |
| • Cámara Hikvision tipo domo para interior | 100 |
| • Conectores balun | 100 |
| • Cable UTP categoría 6 NEXXT | 101 |
| INSTALACIÓN Y CONFIGURACIÓN DEL DVR | 102 |
| • Instalación de cámaras al DVR | 102 |
| • Configuración del DVR | 104 |

MANUAL TÉCNICO

VIRTUALIZACIÓN DE SERVIDORES

ESPECIFICACIONES TÉCNICAS

El equipo físico que alojará las máquinas virtuales al no ser de naturaleza “Servidor”, debe ser lo más robusto posible para evitar percances a futuro. Por este motivo se decidió ensamblar una máquina con las siguientes características:

- **Mainboard - Asus H87M-E**

Fuera de lo tradicional en todas las placas madre podemos destacar lo siguiente de esta:

- ✓ Posee un socket LGA1150 que es compatible con procesadores de 4ta generación.
- ✓ Tiene 4 ranuras para memoria RAM DDR3 en 1600/1333/1066 MHz, soporta hasta 32GB.
- ✓ Posee un procesador gráfico integrado además de que tiene puertos HDMI/DVI-D/RGB.
- ✓ Tiene 4 slots de expansión, 1 PCI Express 3.0 y 3 PCI Express 2.0
- ✓ El chipset de esta placa soporta RAID 0, 1, 5, 10 y viene con 6 puertos SATA 6.0 Gb/s de color amarillo.
- ✓ El puerto Ethernet es realtek 8111G Gigabit.
- ✓ En cuanto a los puertos USB viene con 2 puertos 2.0, 4 puertos 3.0 y permite conectar hasta 4 puertos 2.0 en la parte frontal

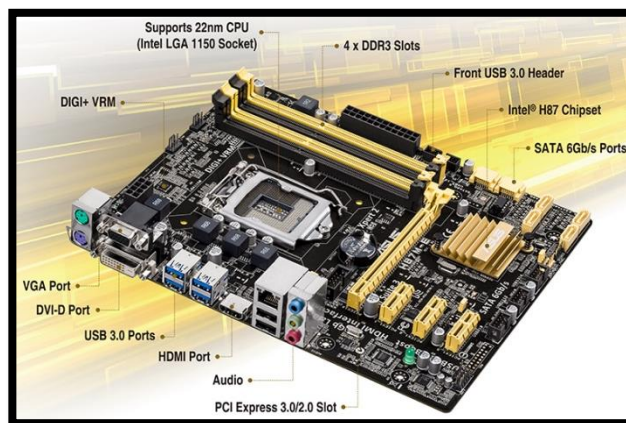


Imagen 01 - Mainboard

- **Procesador – Intel Core I7 4790**

- ✓ Es un procesador de 4ta generación.
- ✓ Posee 4 núcleos y la cantidad de subprocesos es 8.

- ✓ Trabaja en una frecuencia básica de 3.6MHz. y una frecuencia turbo máxima de 4 MHz.
- ✓ Permite un máximo de 32GB de memoria.
- ✓ La gráfica que tiene es Intel® HD Graphics 4600.
- ✓ Su zócalo es FCLGA1150 compatible con la mainboard detallada anteriormente.



Imagen 02 – Procesador

- **Fuente de poder – Agiler AGI-PS800**

- ✓ Esta fuente es de 800w y es ideal para computadoras GAMER.
- ✓ Viene con un conector de 8 pines para la mainboard.
- ✓ Es del tipo ATX de 12V.
- ✓ Posee protección de sobre voltaje y sobrecarga.



Imagen 03 – Fuente de Poder

- **HDD – Seagate**

- ✓ Se adquirió 3 discos duros de 7200RPM 2 de 1TB y el otro de 750 GB.



Imagen 04 – Disco Duro

- **Memoria – RAM 8GB**

- ✓ Se adquirió 2 memorias.
- ✓ Son DDR3 PC3-12800 y trabajan a 1600MHz.



Imagen 05 – Memoria RAM

- **Tarjetas de red – TP-Link TG-3468**

- ✓ Se adquirió 3 de estas tarjetas.
- ✓ Son PCI Express compatibles con las ranuras de la mainboard.
- ✓ Trabajan a 10/100/1000 Mbps.



Imagen 06 – Tarjeta de Red

- **Cooler – LYF Sleeve**

- ✓ Para mantener una temperatura óptima del equipo se adquirió 2 cooler.



Imagen 07 – Cooler

- **Pendrive – Kingston 8GB**

- ✓ El pendrive es del modelo DTSE9
- ✓ Trabaja en USB 2.0



Imagen 08 – Pendrive

- **Case – Dipromacom**

- ✓ Dimensiones 185x420x440mm.
- ✓ Tapa lateral transparente.
- ✓ Agarradera.



Imagen 09 – Case/Gabinete

INSTALACIÓN DE LAS HERRAMIENTAS DE VIRTUALIZACIÓN

Antes de proceder con los pasos de instalación, cabe mencionar que se deberá tener una cuenta en la página de VMware, caso contrario se deberá registrar para continuar.

Descarga del hypervisor

1. Ingresar desde su navegador preferido a <https://myvmware.com/> y loguearse

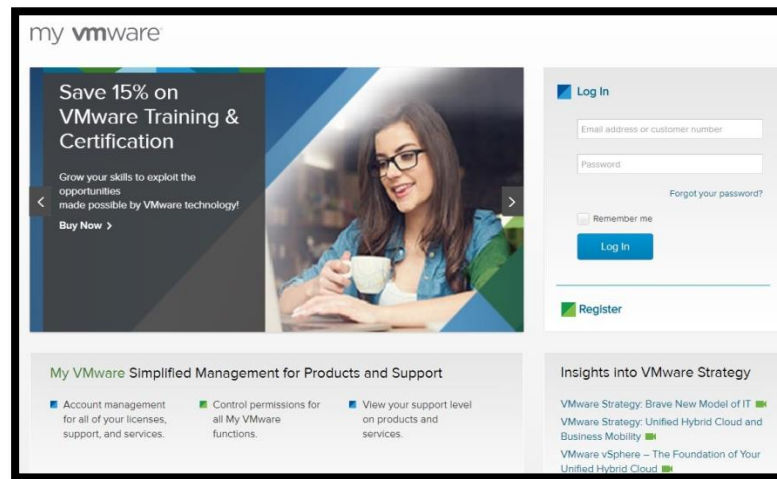


Imagen 10 – My VMware

2. Una vez dentro, dar click en **All Downloads**, lo que conducirá a otra página para seleccionar la pestaña **All Products**, ahí se deberá escoger la opción de **VMware vSphere**.

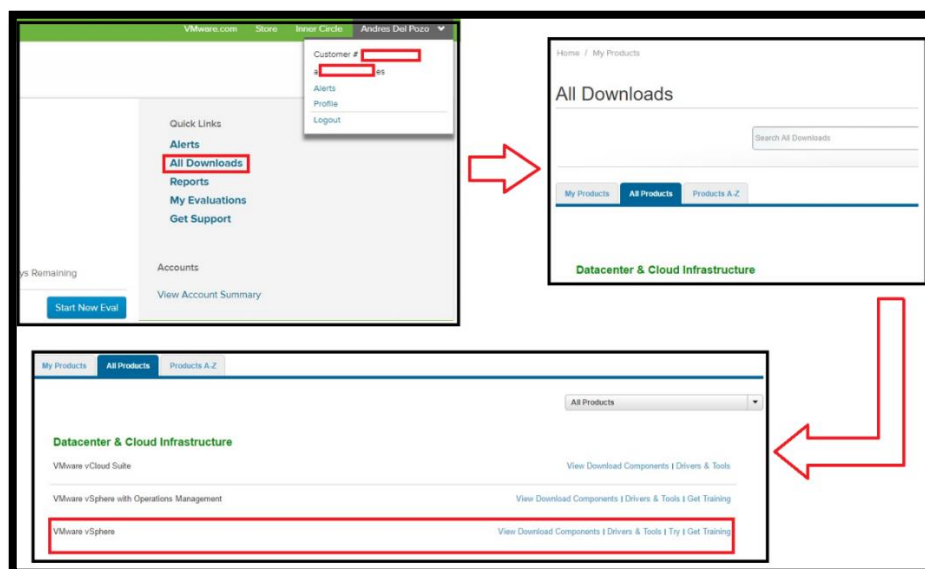


Imagen 11 – Búsqueda de paquetes

3. Ya en la ventana del vSphere presionar el botón **Download Now**, para que aparezca la opción **Download Trial** la cual hay seleccionar para que finalmente despliegue los paquetes del hypervisor.

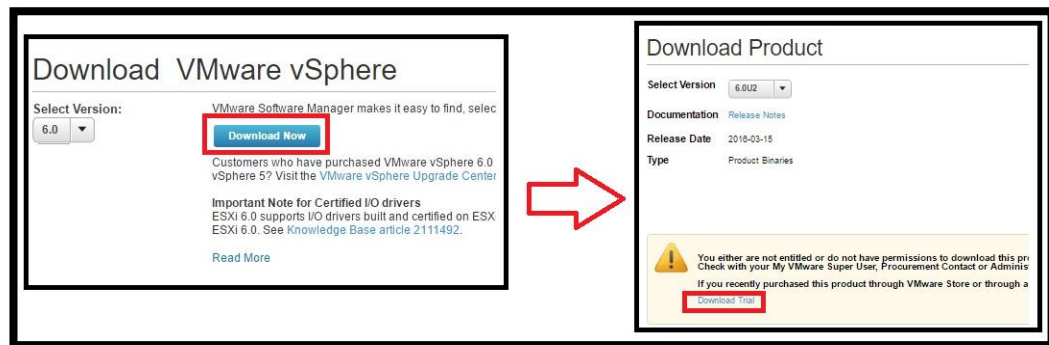


Imagen 12 – Botones de descarga

4. Presionar en los botones **Manually Download** para descargar ESXi y el VMware vSphere Client

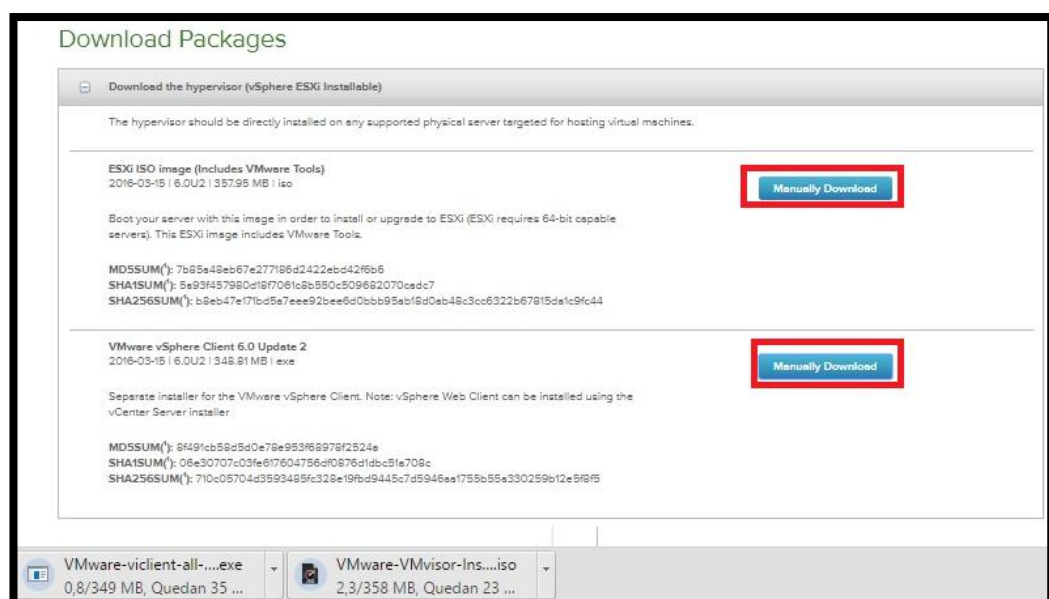


Imagen 13 – Descarga de paquetes

Dependiendo de la conexión a internet que se tenga tardará aproximadamente uno 30 minutos en descargarse los dos archivos.

Una vez que se hayan descargado los archivos se deberá quemar el ISO en un CD para proceder con la instalación en el servidor.

Instalación del ESXi

El equipo físico deberá estar listo no olvidar conectar el teclado y mouse, el lugar donde se alojará este software será en el pendrive de 8GB debido a que no pesa mucho.

1. Ingresar a la BIOS para seleccionar que la opción de booteo sea desde la unidad de CD/DVD.

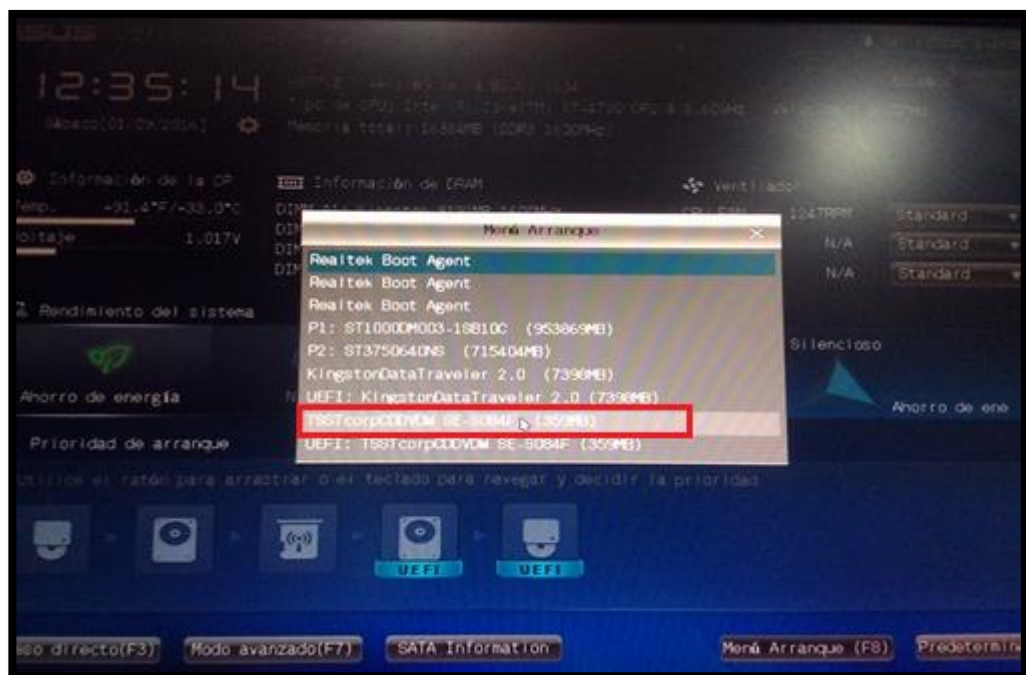


Imagen 14 – Menú arranque de la BIOS

2. Una vez que empiece a bootear, seleccionar la primera opción.

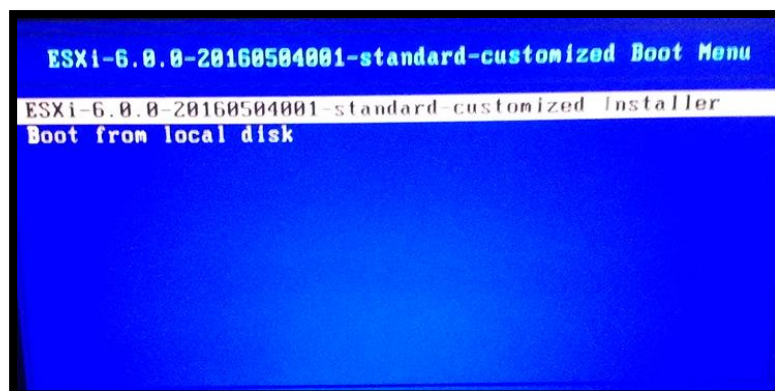


Imagen 15 – Selección del instalador

3. Esperar unos minutos a que empiece a cargar todos los componentes del ISO y a detectar todos los elementos del equipo físico.

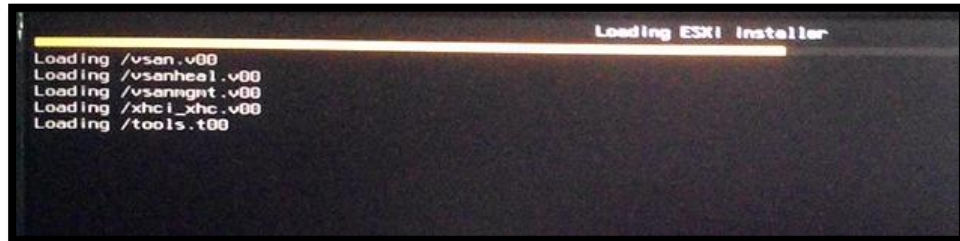


Imagen 16 – Cargando instalador

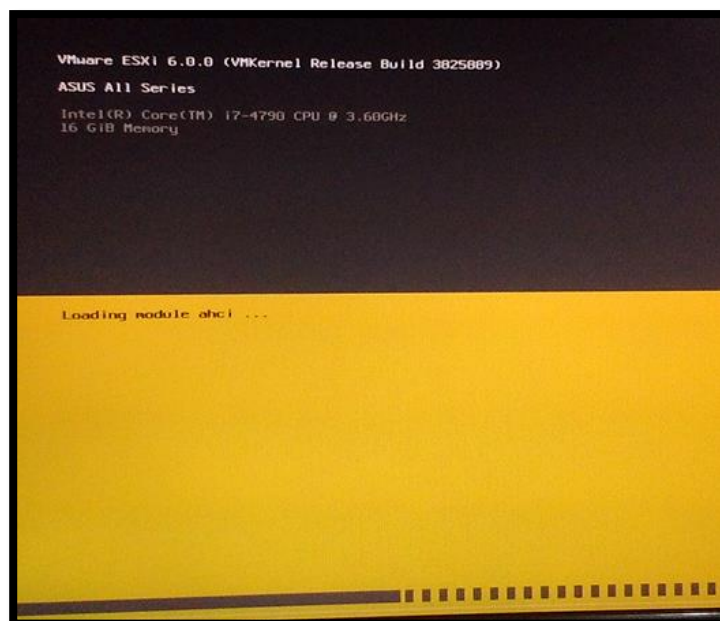


Imagen 17 – Cargando Módulos

4. Cuando aparezca el cartel de bienvenida, presionar la tecla **enter** para continuar y luego presionar la tecla **F11** para aceptar el contrato de la licencia.

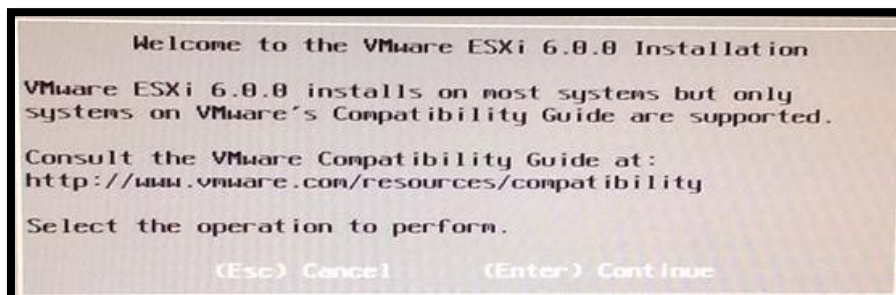


Imagen 18 – Pantalla de bienvenida ESXi

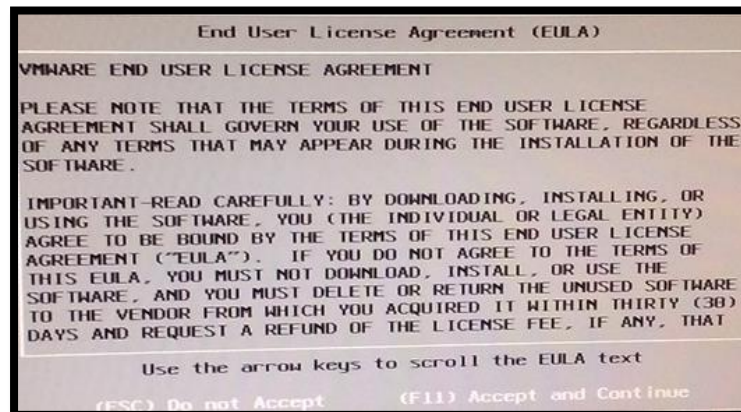


Imagen 19 – Contrato de licencia

5. Luego aparecerá un cuadro donde se deberá seleccionar la unidad de almacenamiento en donde se va a instalar, en este caso se elegirá el pendrive de 8GB y a continuación se presionará **enter**.

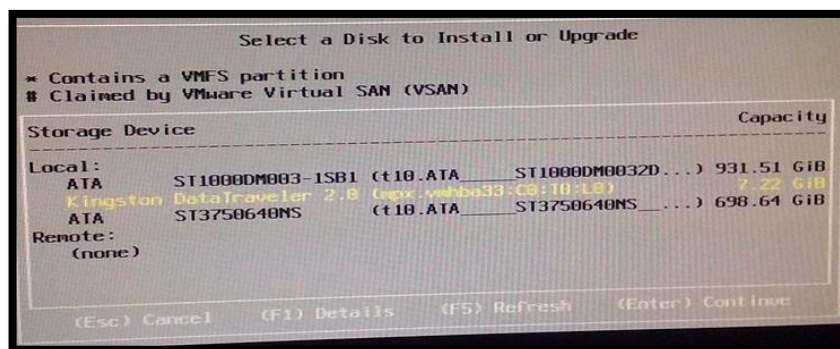


Imagen 20 – Selección del dispositivo para instalación

6. Empezará a escanear el dispositivo seleccionado, en este caso se realizó una instalación previa, motivo por el cual aparece un mensaje indicando si se desea instalar o mejorar el software, en ese caso se debe escoger la primera opción y presionar **enter**.



Imagen 21 – Instalar/Mejorar

7. A continuación aparecerá un mensaje para escoger el idioma del teclado, tener mucho cuidado al escogerlo ya que de esto depende el siguiente paso, se sugiere escoger según el idioma del teclado físico y presionar la tecla **enter**.

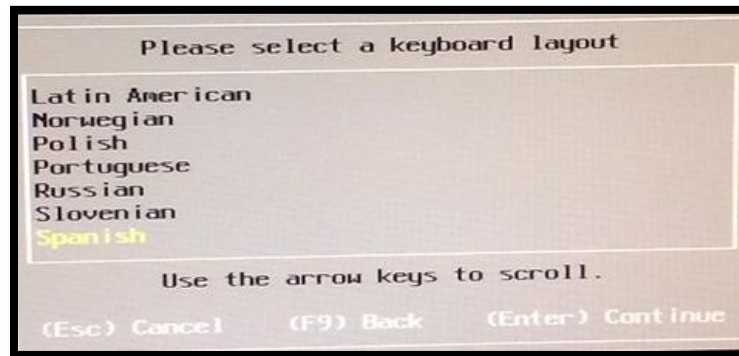


Imagen 22 – Idioma del teclado

8. En este paso se deberá colocar la contraseña para el root, al tratarse de un servidor se debe utilizar números, caracteres especiales, mayúsculas y minúsculas todo con miras de la seguridad, para continuar presionar la tecla **enter**.

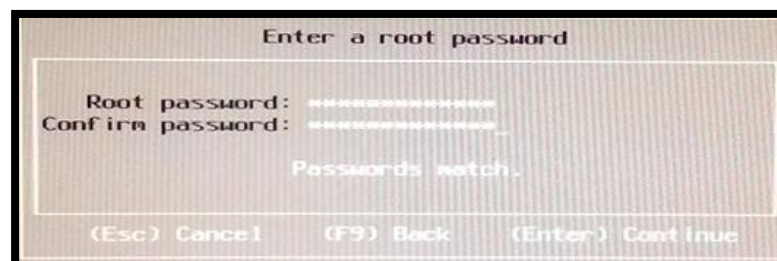


Imagen 23 – Contraseña del root

9. A continuación aparecerá un mensaje donde se debe confirmar la instalación, para lo cual se debe presionar la tecla **enter**, y se deberá esperar unos minutos a que culmine la instalación.

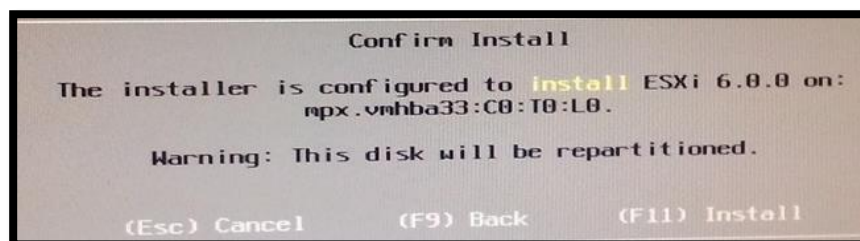


Imagen 24 – Confirmación de la Instalación

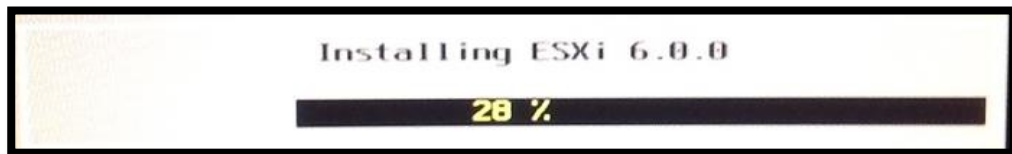


Imagen 25 – Progreso de la instalación 28%

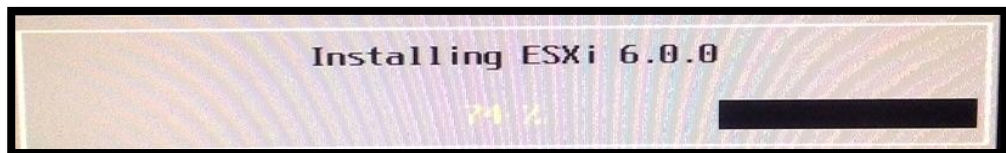


Imagen 26 – Progreso de la instalación 74%

10. Finalmente aparecerá un mensaje donde indica que la instalación se completó, para lo cual se debe presionar enter para reiniciar el equipo.



Imagen 27 – Instalación Completa

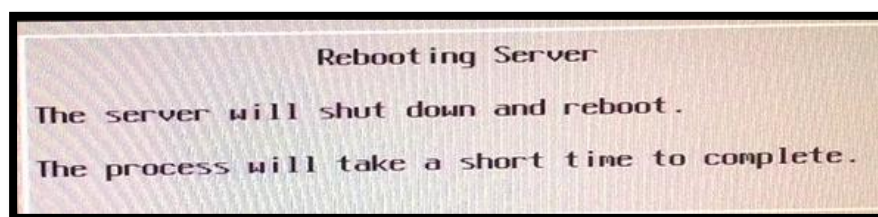


Imagen 28 – Reinicio del servidor

11. Cuando se reinicie el equipo se deberá verificar en la BIOS que como prioridad de booteo se encuentre el dispositivo USB. Esperar a que cargue el hypervisor para que aparezca la pantalla con la información del equipo.

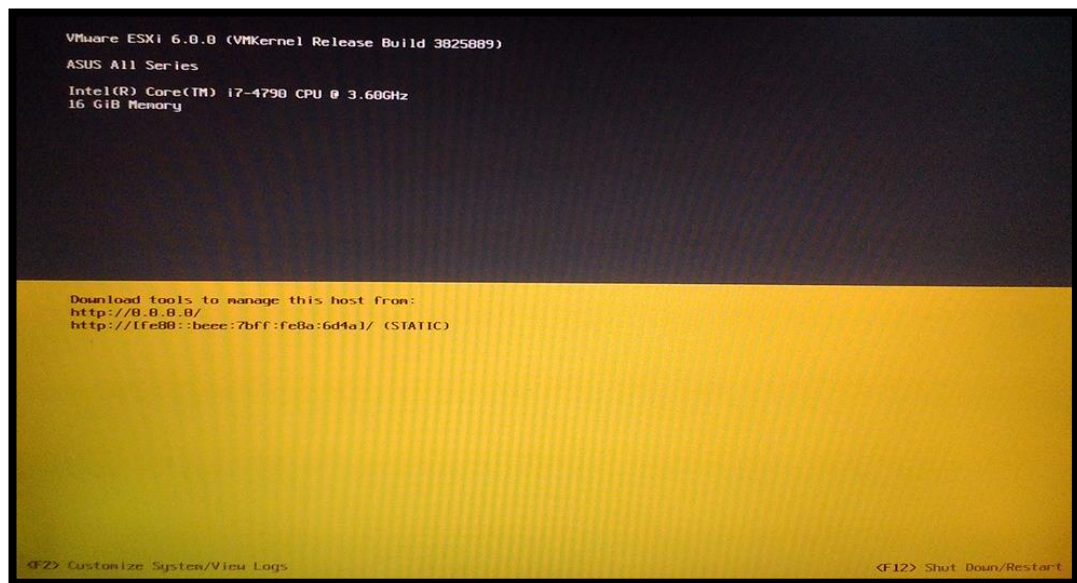


Imagen 29 – Pantalla principal ESXi

12. Se deberá configurar la dirección IP de administración, para lo cual se debe presionar la tecla F2, aparecerá un cuadro para colocar las credenciales del root y presionar **enter**, una vez realizado esto se mostrará el panel de control.

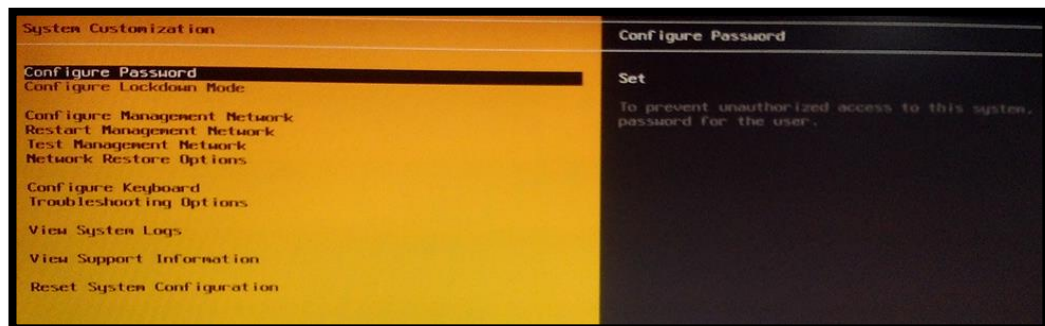


Imagen 30 – Personalización del sistema

13. Dirigirse a la opción **Configure Management Network** y presionar **enter**, luego escoger la opción **IPv4 Configuration**, y aparecerá un cuadro en donde debemos escoger la opción estática y colocar la dirección IP y a continuación presionar **enter**.

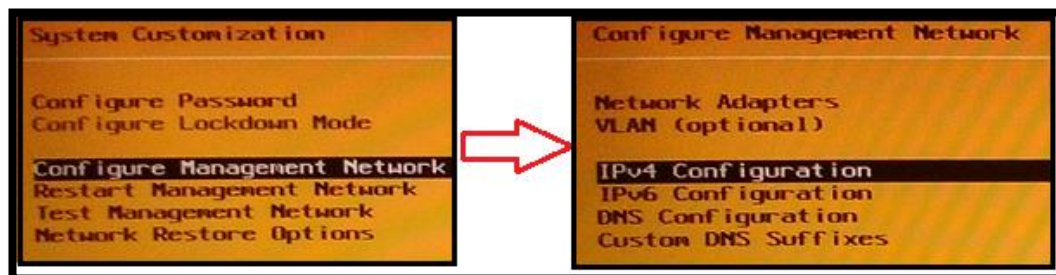


Imagen 31 – Configuración interfaz de red

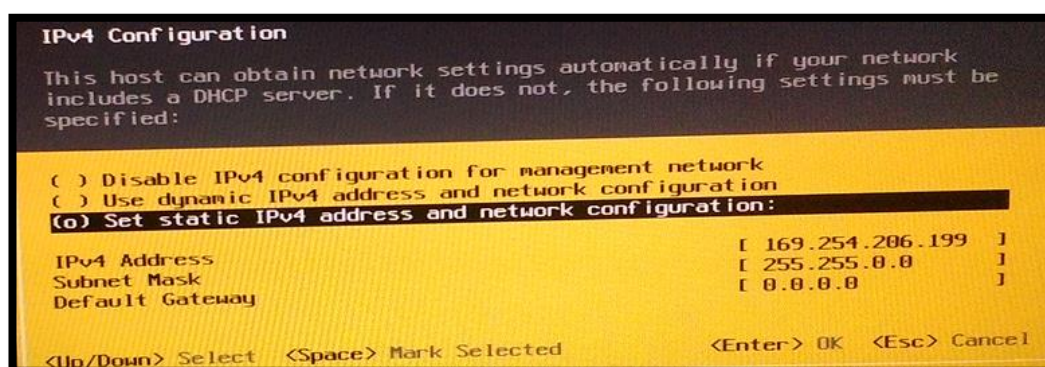


Imagen 32 – Asignación de IP

14. Para retornar al panel principal se debe presionar la tecla **ESC**, inmediatamente aparecerá un cuadro preguntando si se desean aplicar los cambios, a lo cual se elige que sí presionando la tecla **Y**.

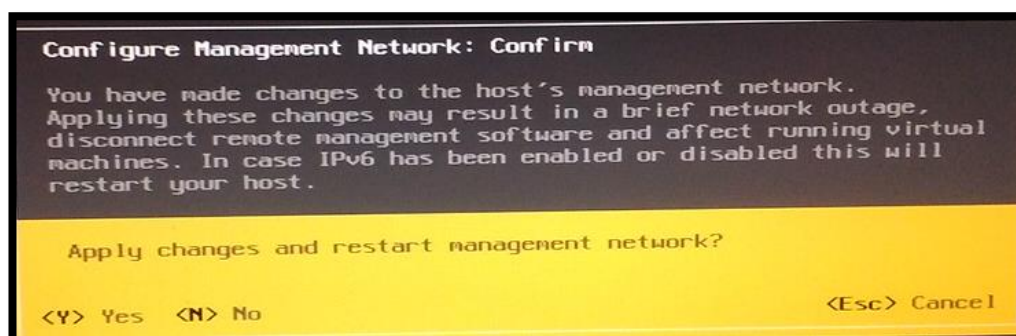


Imagen 33 – Confirmación de cambio de IP

INSTALACIÓN DE VMWARE VSPHERE CLIENT

Este programa se lo puede instalar en cualquier computadora para administrar el hypervisor, siempre y cuando se encuentre dentro de la misma red.



Imagen 34 – Instalador VMware client

1. Ejecutar como administrador el programa, y este empezará a extraer todo lo necesario para la instalación.

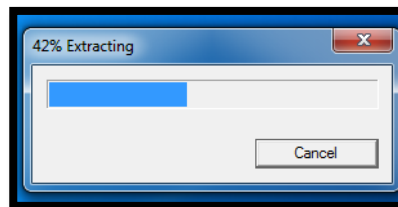


Imagen 35 – Extracción de paquetes

2. Aparecerá una ventana en donde indicará en que idioma se desea instalar.

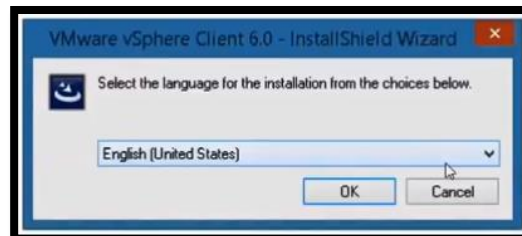


Imagen 36 – Elección Idioma

3. Se deberá esperar unos minutos a que cargue.

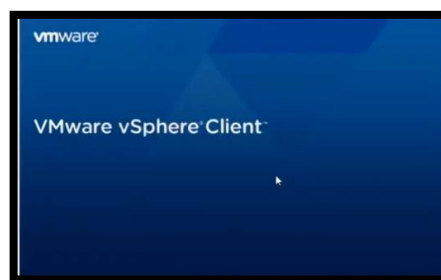


Imagen 37 – Pantalla de espera vSphere Client



Imagen 38 – Preparando la instalación

4. Aparecerá la ventana de bienvenida, dar click en siguiente.

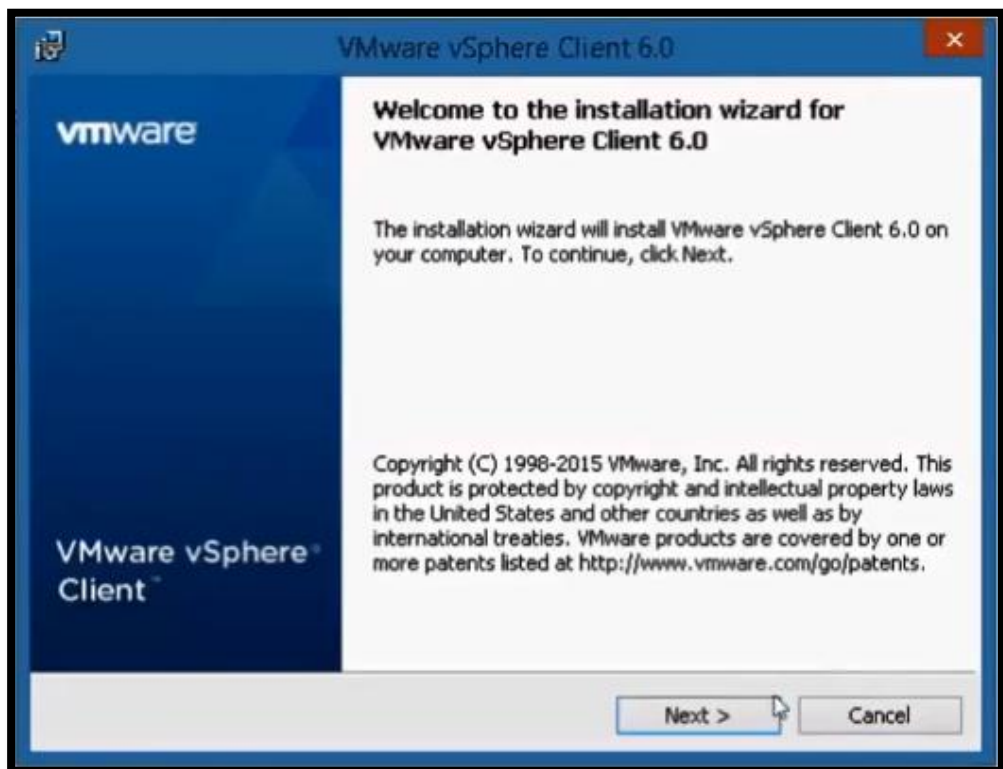


Imagen 39 – Ventana de bienvenida

5. En la siguiente ventana se deberá aceptar los términos y condiciones, dar click en siguiente



Imagen 40 – Aceptar términos de la licencia

6. En la siguiente ventana, se debe escoger la ruta en donde se instalará, se recomienda dejar la que viene por defecto y dar click en siguiente.

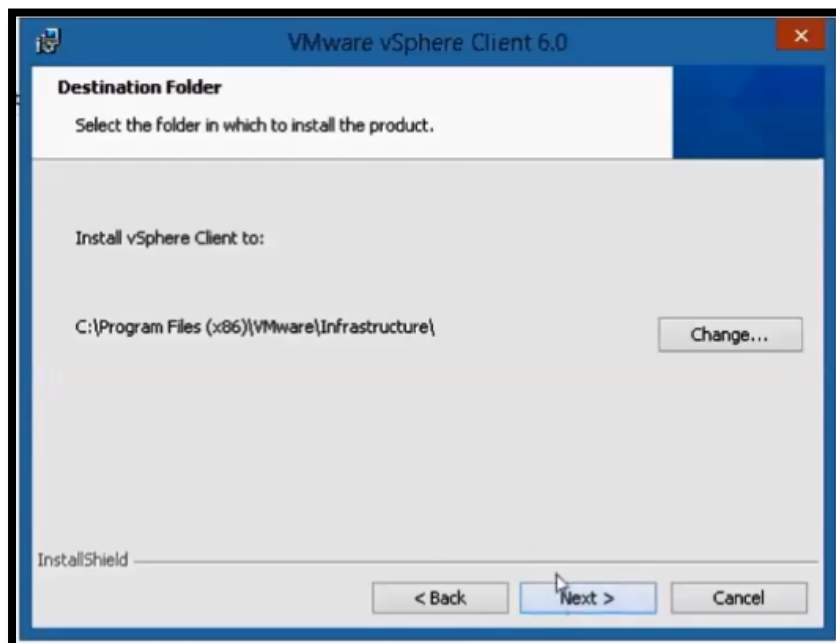


Imagen 41 – Ruta de instalación

7. Finalmente aparecerá la ventana para instalar.

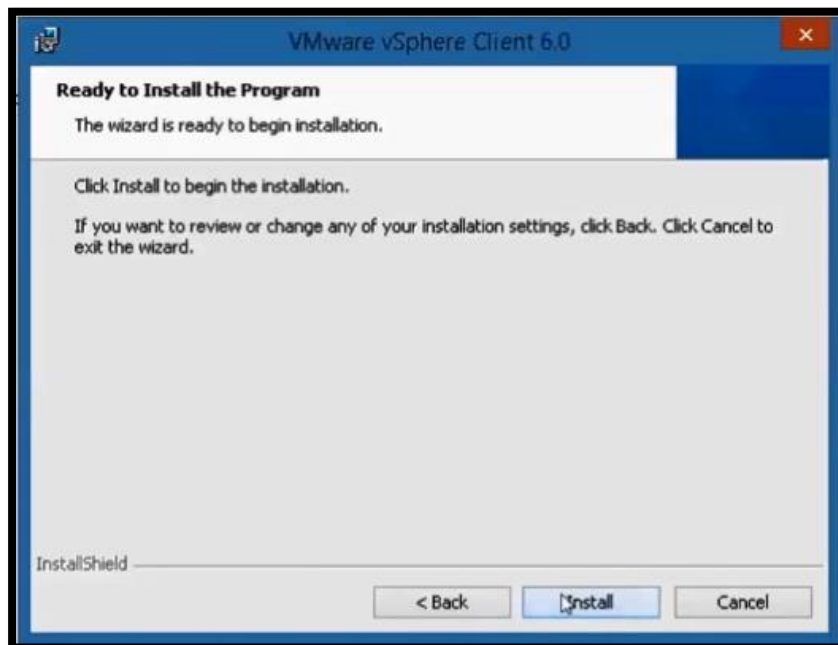


Imagen 42 – Iniciar instalación

8. Esperar unos minutos a que termine de instalarse el programa y aparezca la ventana de finalización.

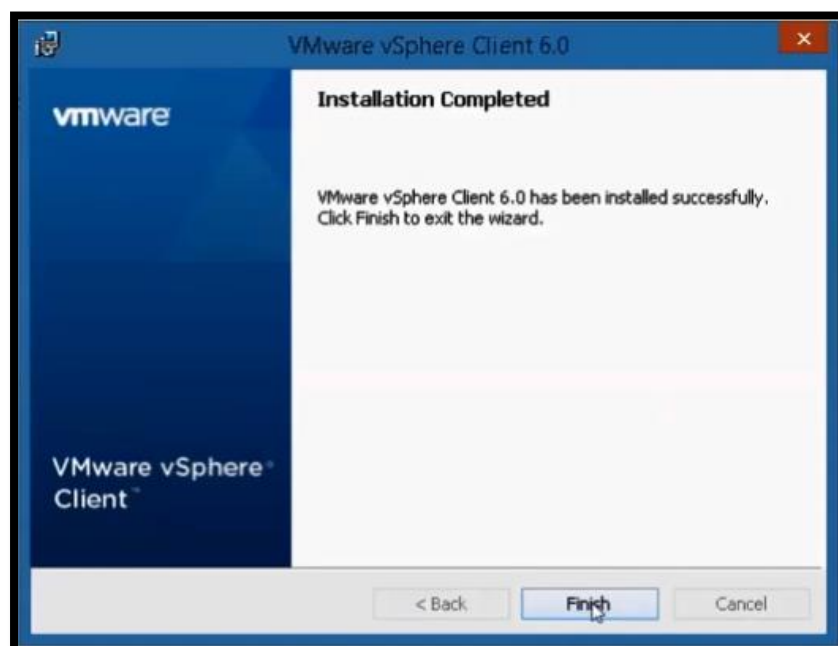


Imagen 43 – Instalación Completa

Configuración del vSphere Client

Una vez instalado el programa, este detectará todos los componentes físicos del equipo, pero no se encuentran configurados para lo cual es necesario realizar este paso antes de empezar a crear máquinas virtuales.

1. Ingresar al vSphere Client, se abrirá una ventana en donde se deberá loguearse colocando la dirección IP del servidor, el nombre de usuario en este caso root y la contraseña, presionar conectar, si todo está correcto aparecerá una ventana sobre el certificado de seguridad, presionar en el botón omitir.

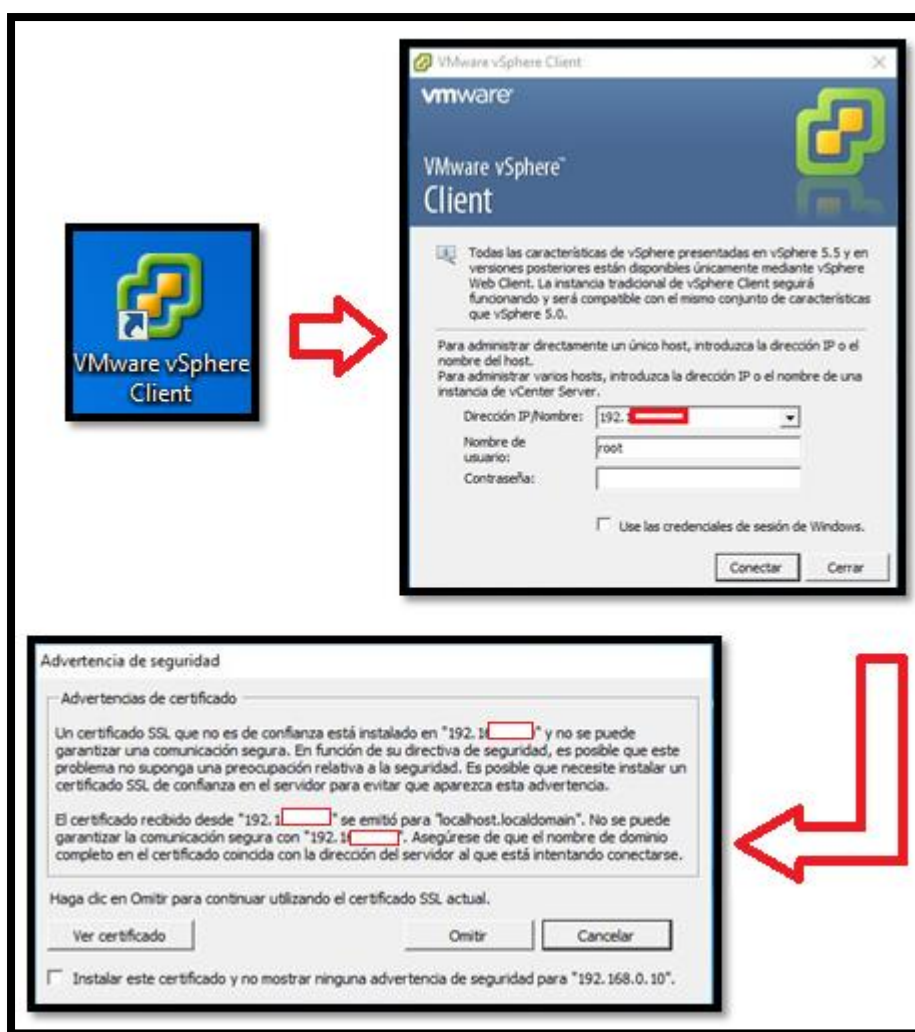


Imagen 44– Ingreso al vSphere Client

2. Una vez terminado de cargar aparecerá la ventana de administración, donde mostrará una introducción al programa.

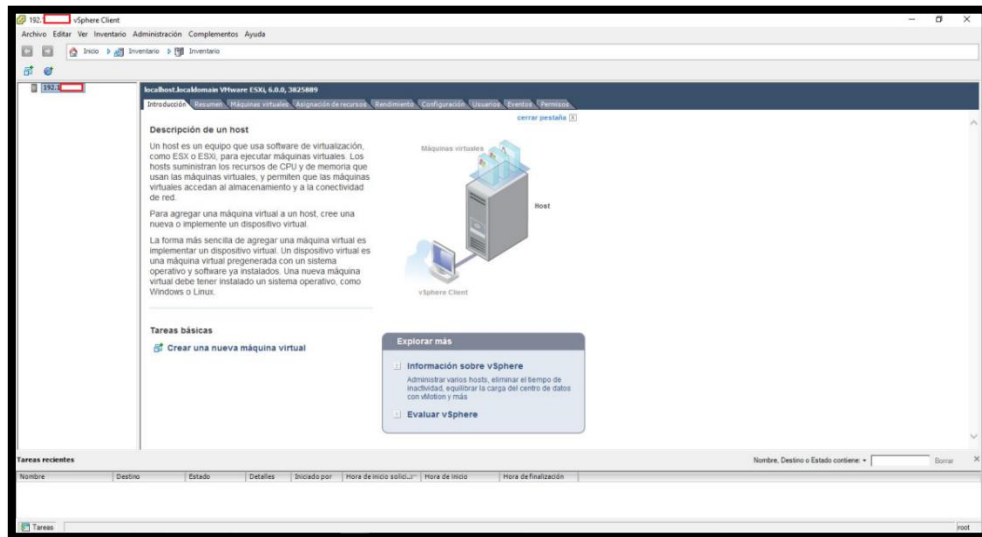


Imagen 45 – Ventana Principal vSphere Client

3. Este programa viene con un periodo de prueba de 60 días, para lo cual es necesario introducir una licencia, la misma que se la puede obtener en la página de vmware sin costo. Para introducir la licencia, hay que dirigirse a la pestaña de **Configuración**, en el panel de la izquierda seleccionar la opción **Características con licencia** y en la parte derecha presionar sobre la opción **Editar**.

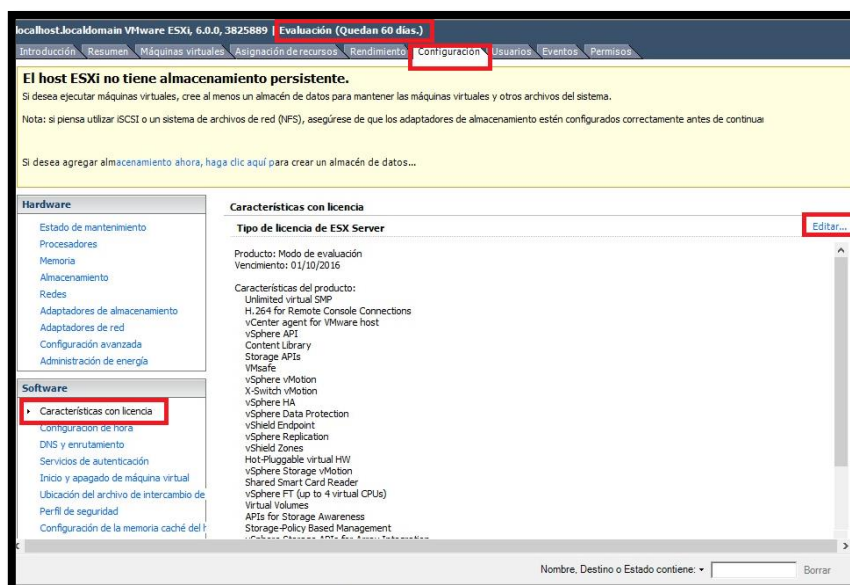


Imagen 46 – Configuración de la licencia

4. Se abrirá una ventana donde se debe seleccionar la opción **Asignar una clave de licencia nueva a este host**, se abrirá un cuadro en donde se introducirá la licencia obtenida, presionar el botón Aceptar para concluir con este paso. Hay que mencionar que estas licencias gratuitas solo permiten utilizar un máximo de 32GB para memoria RAM, si se requiere más se debe adquirir la versión pagada.

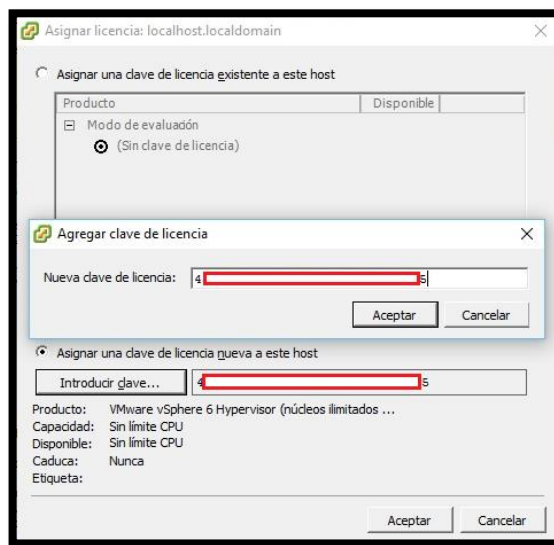


Imagen 47 – Ingreso de la licencia

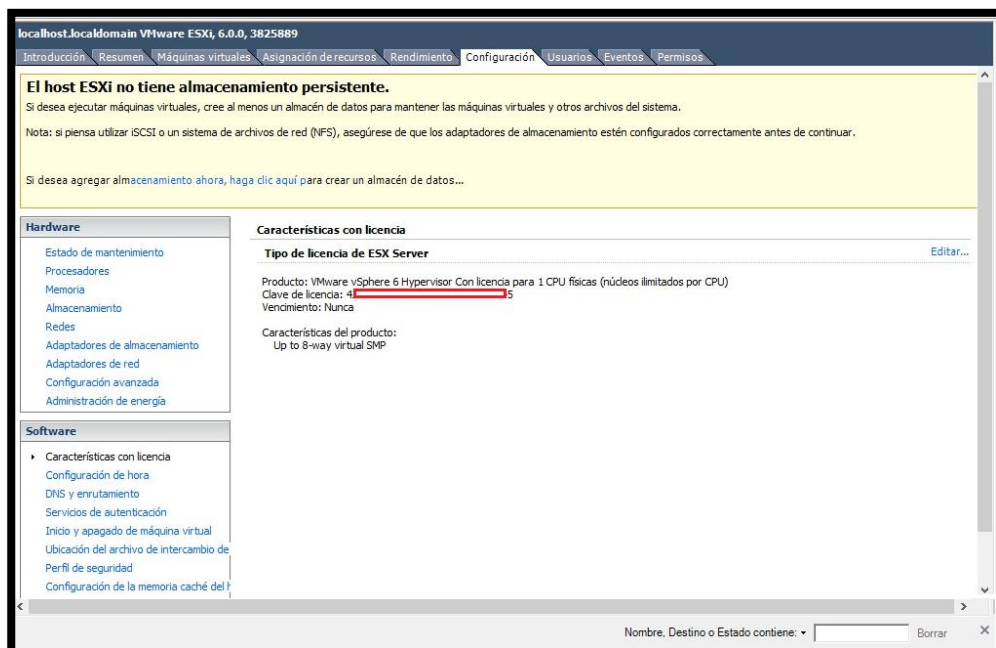


Imagen 48 – Producto Registrado

5. Para agregar los HDD e identificarlos con un nombre, en la misma pestaña de Configuración se debe seleccionar la opción **Almacenamiento** y dar click en **Agregar almacenamiento** en las opciones de la parte derecha para que abra una ventana, en la cual se debe seleccionar la **Disco/LUN** y presionar siguiente.

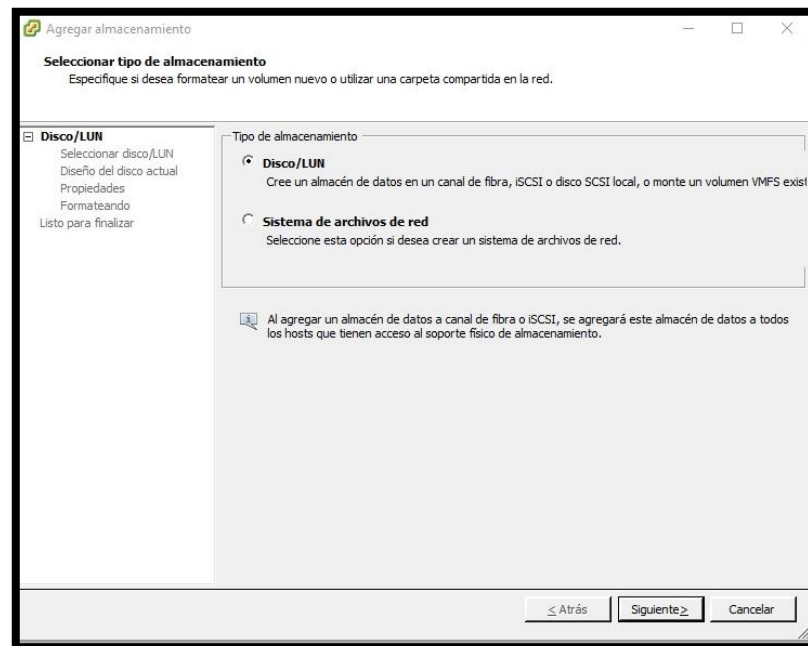


Imagen 49 – Agregar unidades de almacenamiento

6. Aparecerán los HDD disponibles, se debe seleccionar uno por uno para darles el nombre, en este caso se lo configurará de la siguiente manera:
- HDD 750GB tendrá el nombre HDD-FW
 - HDD 1TB tendrá el nombre HDD-MAIL
 - HDD 1TB tendrá el nombre HDD-MAIL2

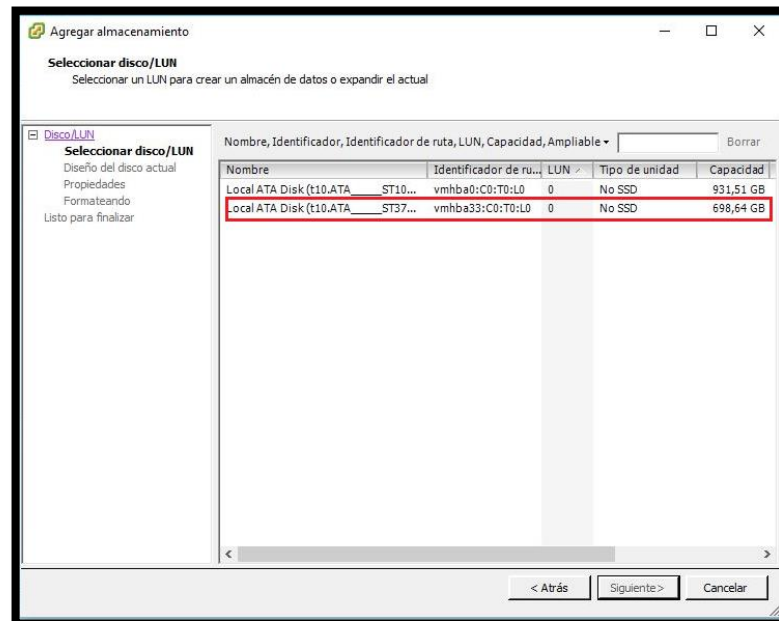


Imagen 50 – Elección del disco duro

- Una vez seleccionado el disco presionar el botón siguiente para luego escribir el nombre del disco, elegir el espacio disponible y finalizar con la creación del HDD.

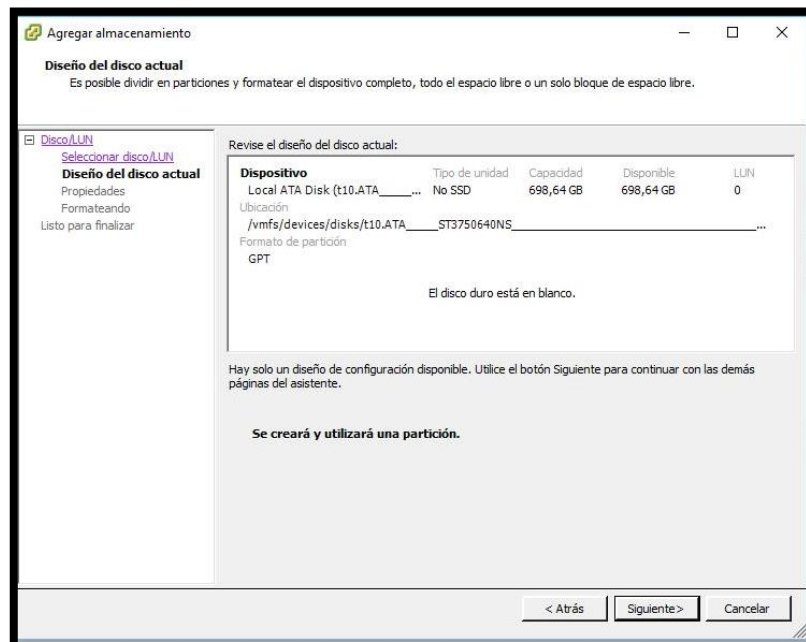


Imagen 51 – Diseño del disco seleccionado

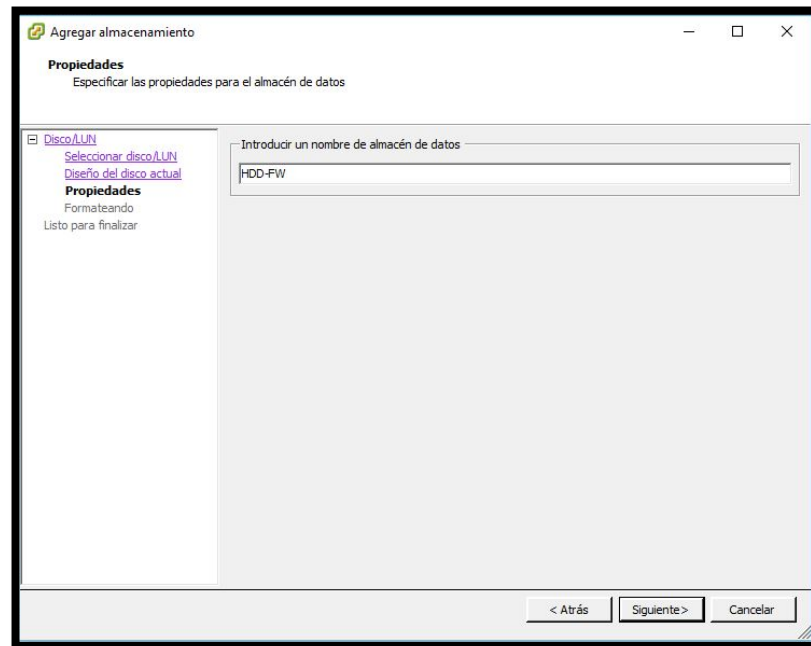


Imagen 52 – Nombre del Disco Duro

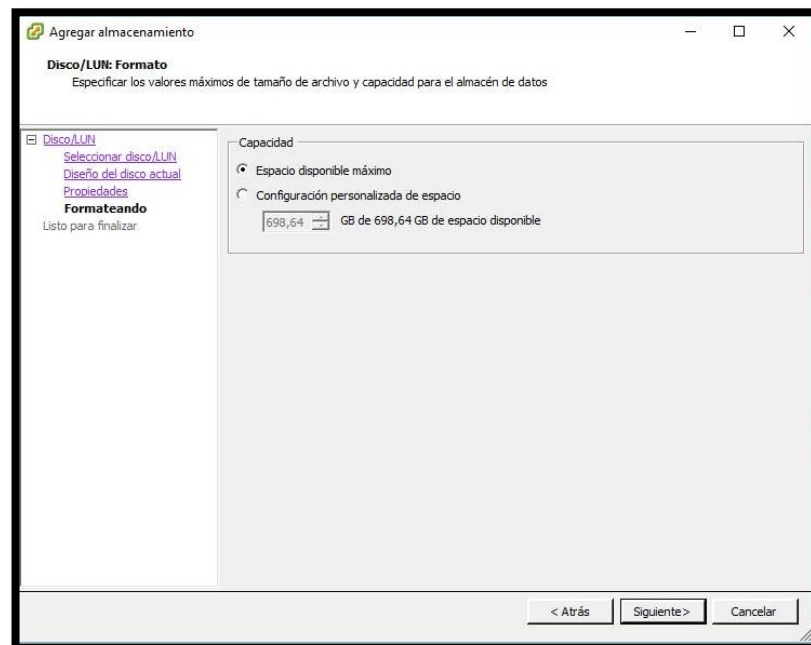


Imagen 53 – Elección de capacidad del Disco Duro

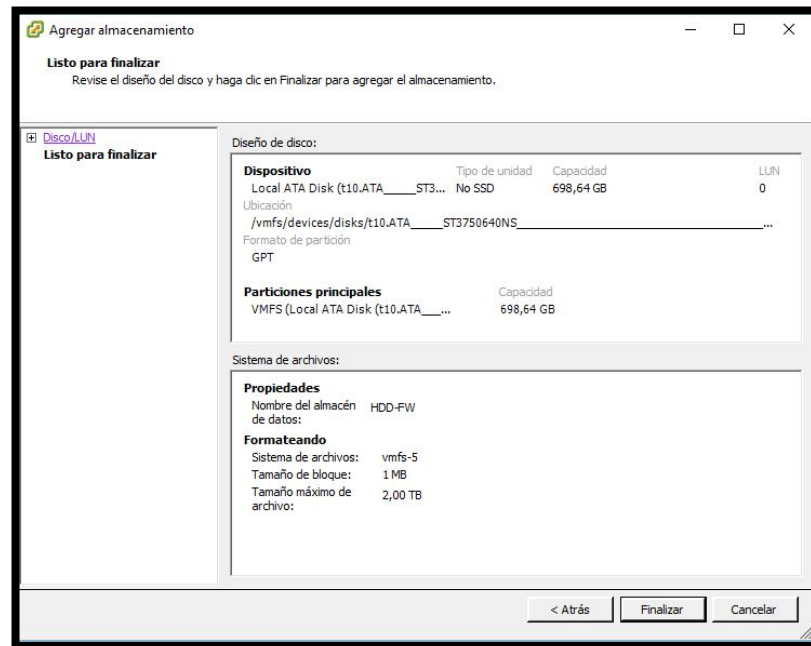


Imagen 54 – Finalización del proceso

8. Realizar los mismos pasos para los otros HDD y finalmente se tendrá lo siguiente.

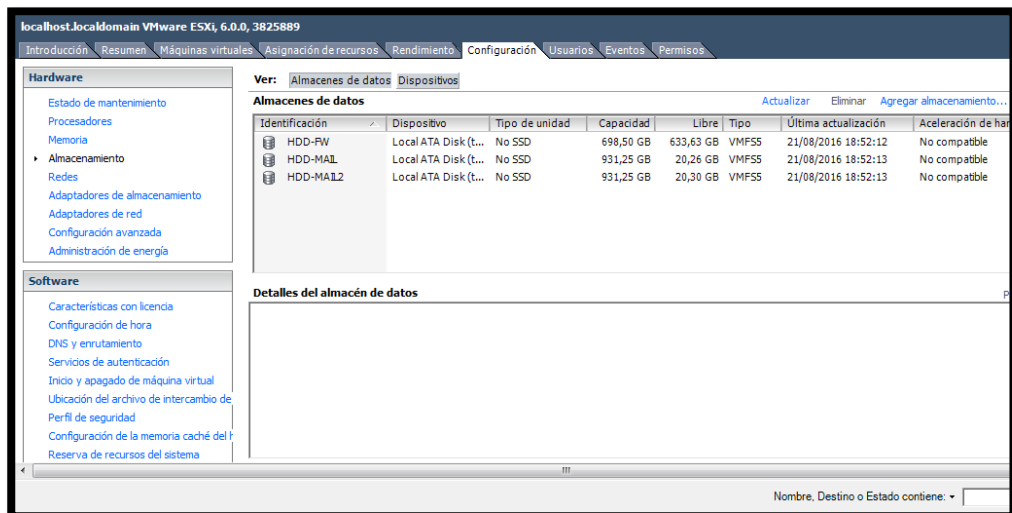


Imagen 55 – Lista de unidades de almacenamiento

9. Para configurar las interfaces de red se debe ir a la opción de **Redes**, actualmente se tiene 4 interfaces las cuales estarán repartidas de la siguiente forma:
 - Interfaz 1: Hypervisor y Servidor Web
 - Interfaz 2: Servidor Firewall Entrada

- Interfaz 3: Servidor Firewall Salida
 - Interfaz 4: Servidor de Correo
10. En la parte derecha seleccionar la opción **Agregar Redes**, esta abrirá la una ventana donde se escogerá la opción **Máquina Virtual**, dar click en siguiente, seleccionar una interfaz y dar click en siguiente.

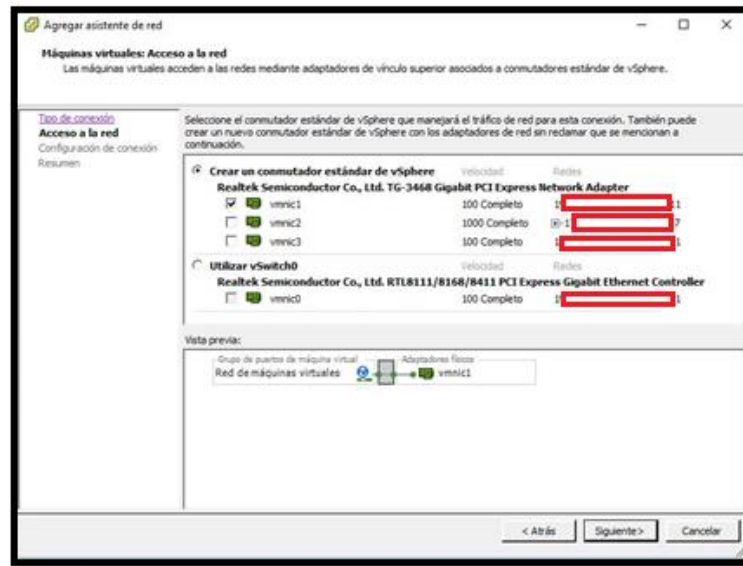


Imagen 56 – Agregar interfaces de red

11. En la parte de Etiqueta de Red colocar el nombre que tendrá la interfaz, presionar siguiente y luego finalizar en el siguiente cuadro.

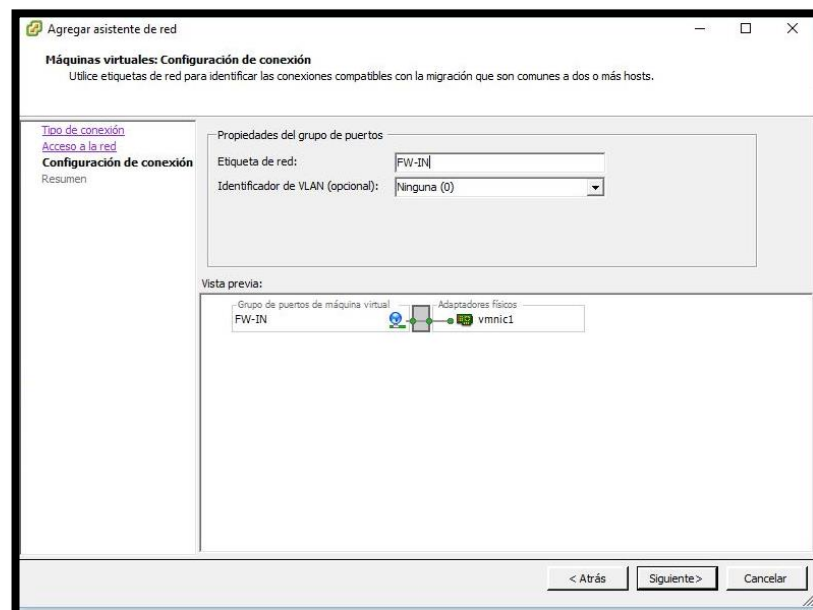


Imagen 57 – Nombre de la interfaz de red

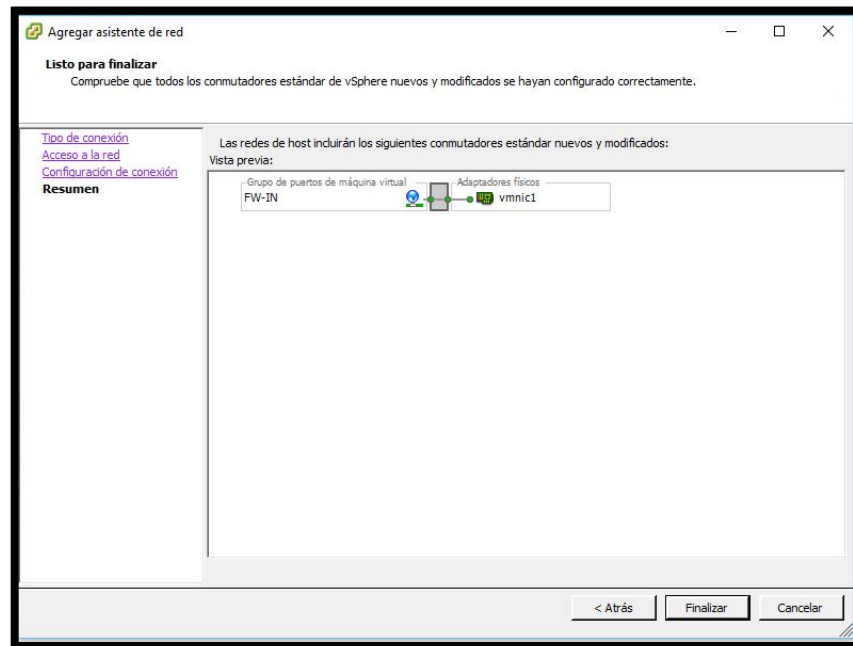


Imagen 58 – Interfaz agregada

12. Repetir el mismo proceso con las otras interfaces.
13. Finalmente se tendrá configuradas las interfaces de la siguiente manera:

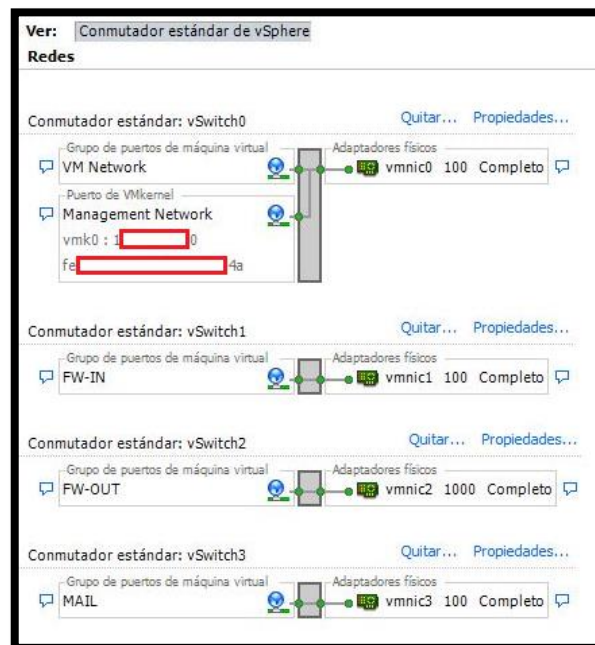


Imagen 59 – Resto de Interfaces agregadas

Creación del Data Store

El Data Store, será el lugar donde se almacenarán todos los ISO de los diferentes sistemas operativos con la finalidad de que al crear las máquinas virtuales no exista la necesidad de instalarlas desde un CD/DVD.

En este caso se subirá el ISO de CenOS7 minimal.

1. En la parte de almacenamiento se debe elegir que HDD tendrá el Data Store, darle click derecho y seleccionar la opción **Examinar Almacén de Datos**.

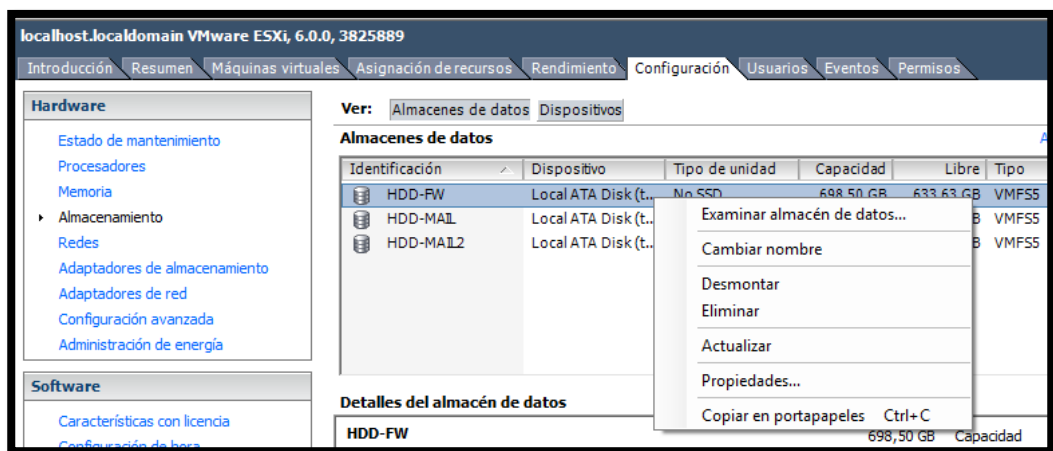


Imagen 60 – Examinar almacén de datos

2. Se abrirá una nueva ventana en donde se creará una nueva carpeta llamada **isos**

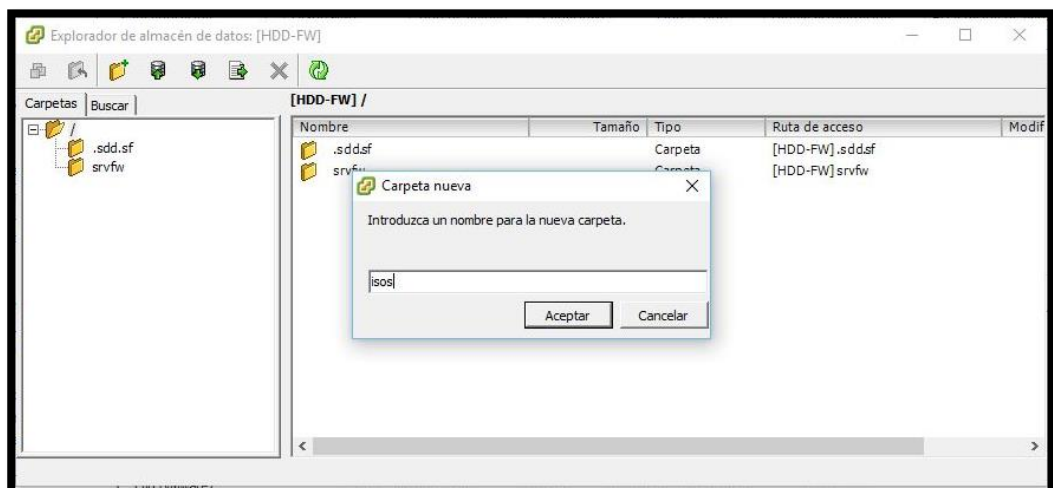


Imagen 61 – Nueva carpeta en almacén de datos



Imagen 62 – Carpeta isos creada

- Ahora se debe presionar la opción **cargar archivo**, se abrirá una ventana para seleccionar la ubicación del ISO, una vez seleccionado aparecerá un cuadro de advertencia indicando que si existe algún archivo con el mismo nombre se reemplazará, presionar **Si** y esperar a que se suba el ISO.

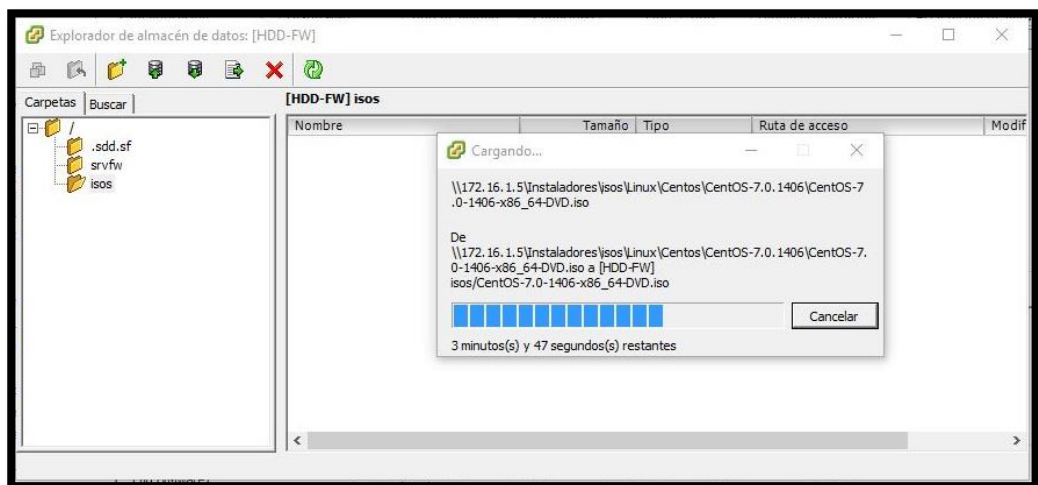


Imagen 63 – Subiendo ISO CentOS 7 minimal

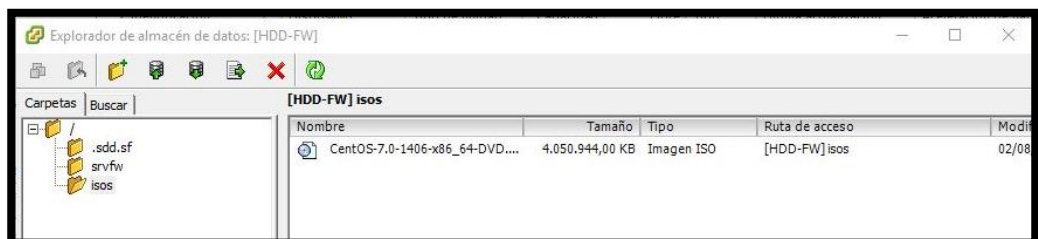


Imagen 64 – ISO en el data store

INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES

Creación del Servidor Firewall

Antes de crear la virtual se deberá definir sus recursos físicos, estos se detallan a continuación:

- HDD 30 GB, RAM 3 GB, 2 Interfaces de Red
1. Presionar la combinación de teclas Control + N, esto abrirá la ventana para crear una nueva máquina virtual, seleccionar la opción **Personalizada** y presionar siguiente.

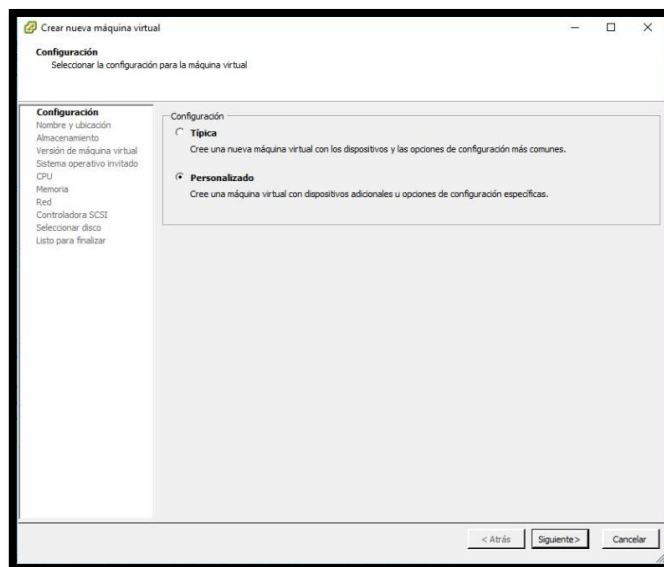


Imagen 65 – Instalación personalizada – máquina virtual FW

2. Colocar el nombre para la máquina virtual (srvfw) y presionar siguiente.

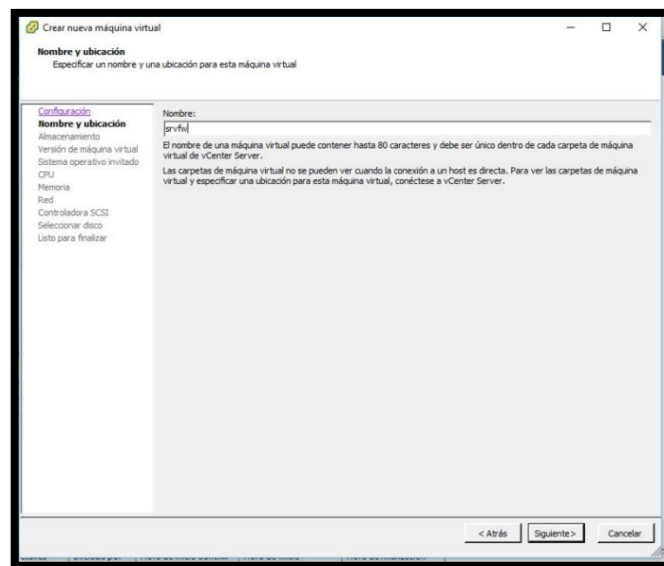


Imagen 66 – Nombre de máquina virtual

3. Escoger el disco donde se instalará.

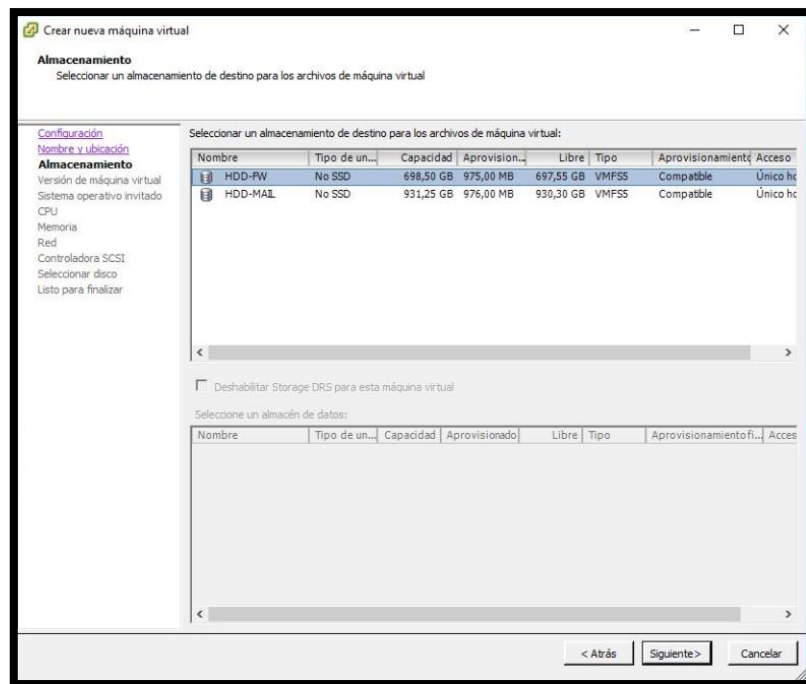


Imagen 67 – Instalación personalizada – máquina virtual FW

4. Escoger la Versión de máquina virtual 11 ya que el ESXi que tiene el servidor instalado es el 6.

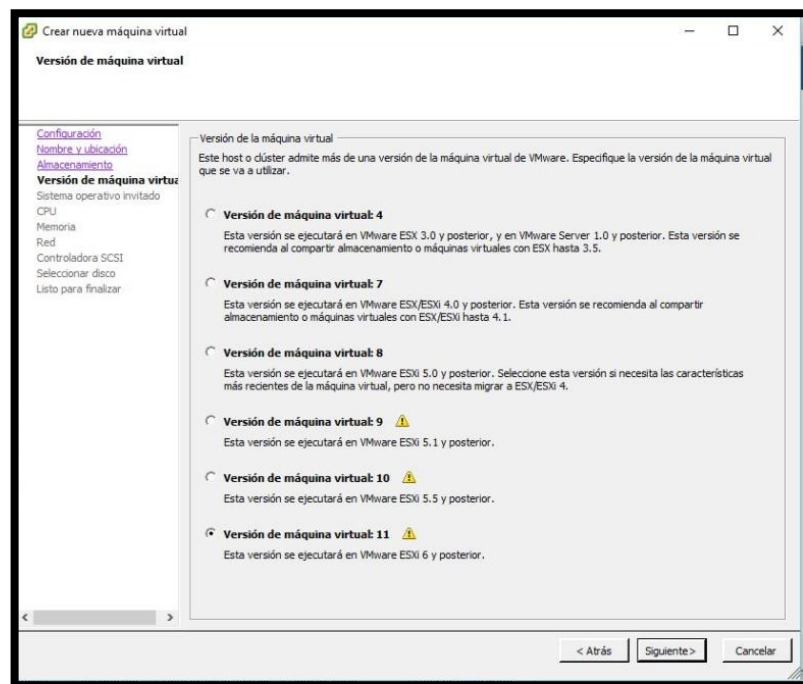


Imagen 68 – Versión de máquina virtual

5. Para el Sistema Operativo se debe elegir Linux y la versión CentOS 4/5/6/7 (64bit)

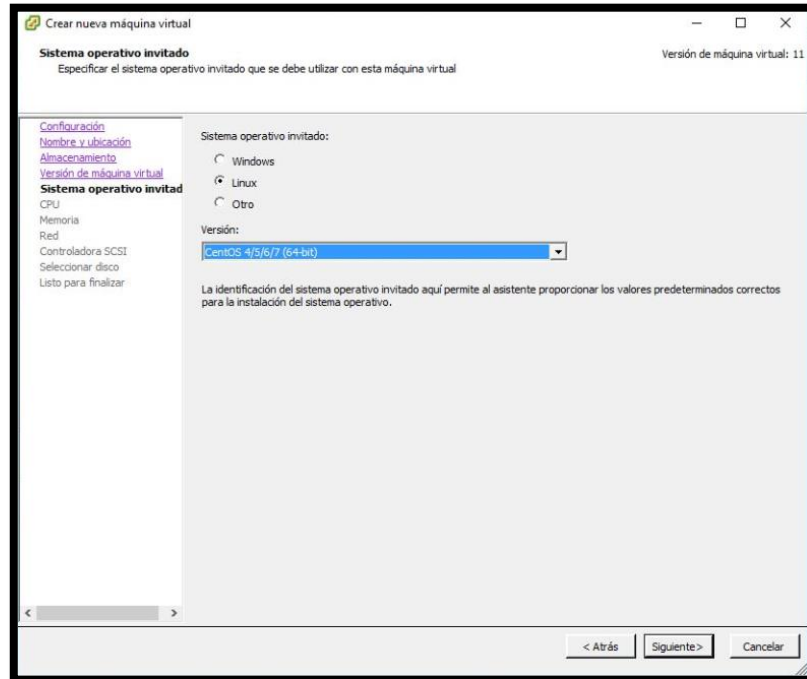


Imagen 69 – Elección del Sistema Operativo

6. En la ventana del CPU dejarla por defecto con el número de sockets virtuales en 1 y el número de núcleos por socket virtual en 1.

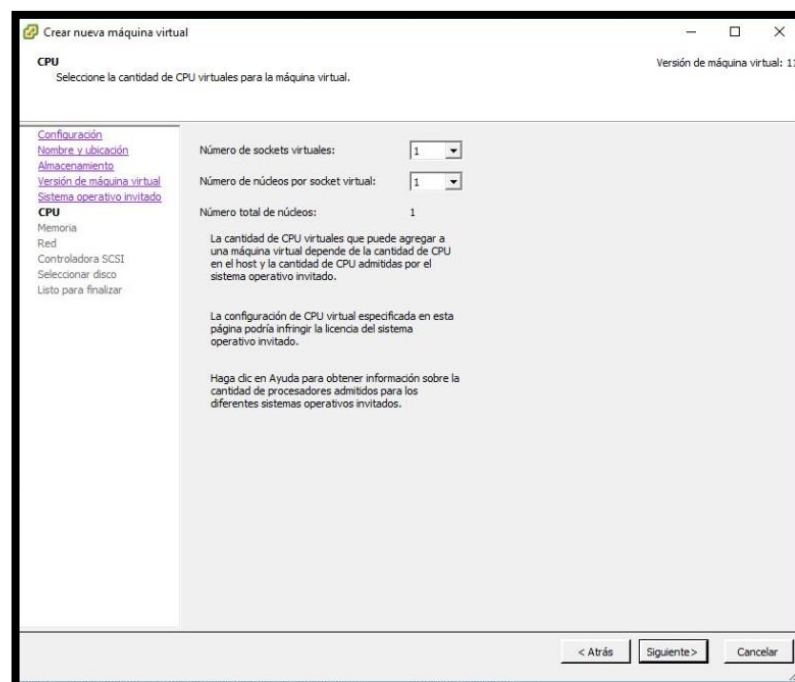


Imagen 70 – Elección de la cantidad de CPU virtuales

7. Elegir el tamaño de la memoria RAM que ya se mencionó al principio (3GB).

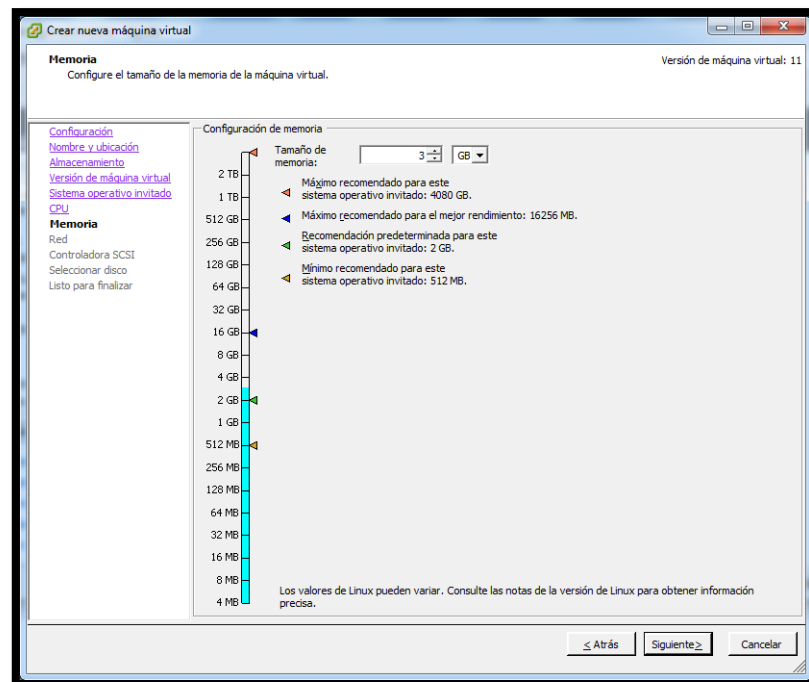


Imagen 71 – Elección de la cantidad de memoria RAM

8. Para las tarjetas de red escoger 2 y seleccionar las que se crearon anteriormente para este servidor FW-IN y FW-OUT.

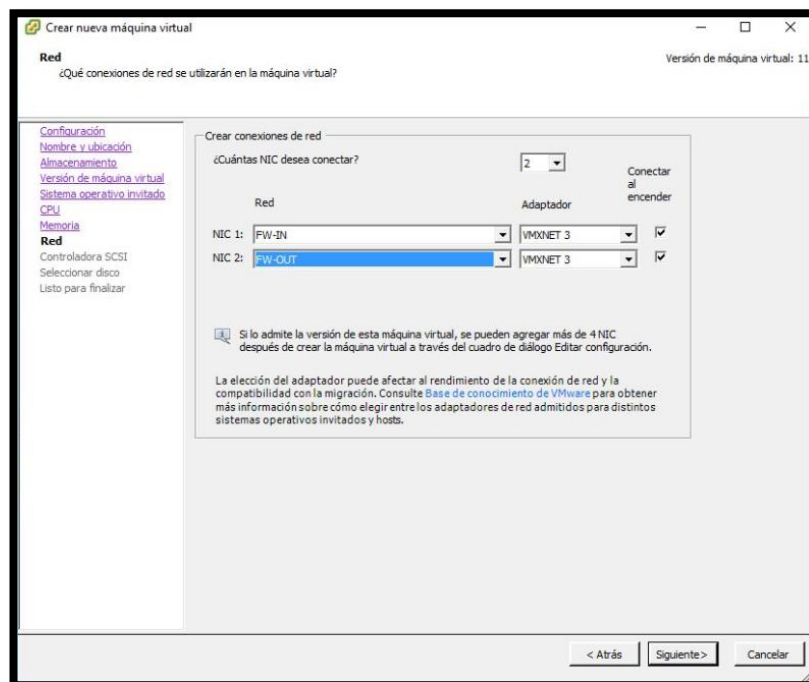


Imagen 72 – Elección de la cantidad de interfaces de red

9. Para la controladora SCSI dejar la opción que viene por defecto **LSI Logic Paralel**.

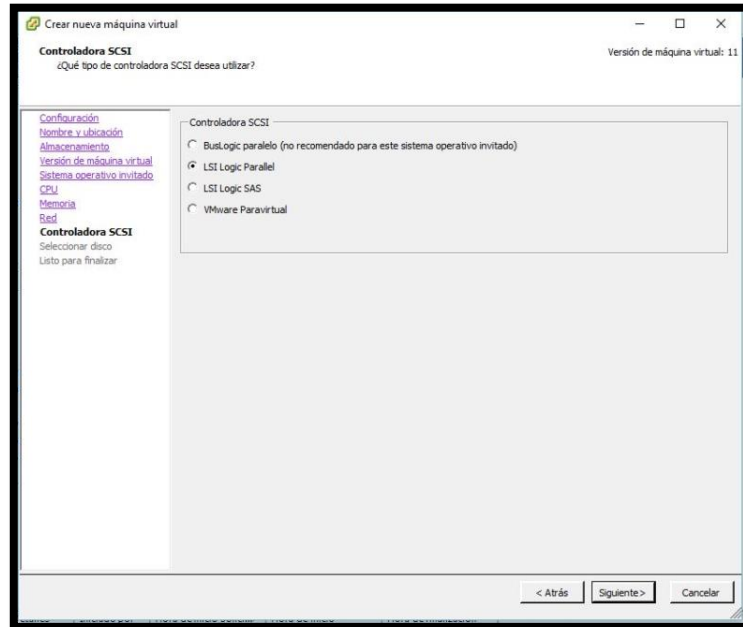


Imagen 73 – Elección de la controladora SCSI

10. En la opción Seleccionar disco escoger **Crear un disco virtual nuevo** y dar click en siguiente, ahora se deberá elegir el tamaño especificado al principio (30GB), en la ventana de **Opciones avanzadas** dejarla como está y presionar siguiente.

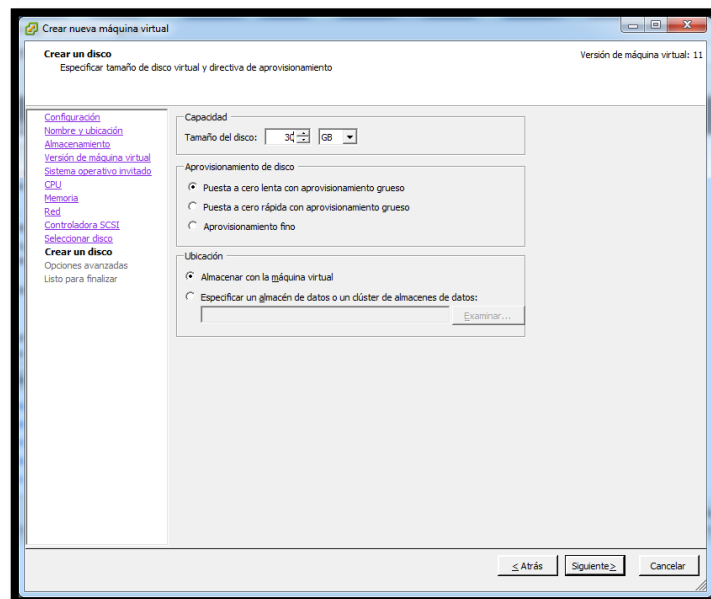


Imagen 74 – Elección de la cantidad de interfaces de red

11. En la última ventana marcar la casilla **Editar configuración de la máquina virtual antes de finalizar** y presionar el botón continuar, se abrirá una nueva ventana en donde se escogerá el ISO de CentOS7 del data store creado anteriormente, seleccionar la casilla **Conectar al encender** y presionar el botón aceptar.

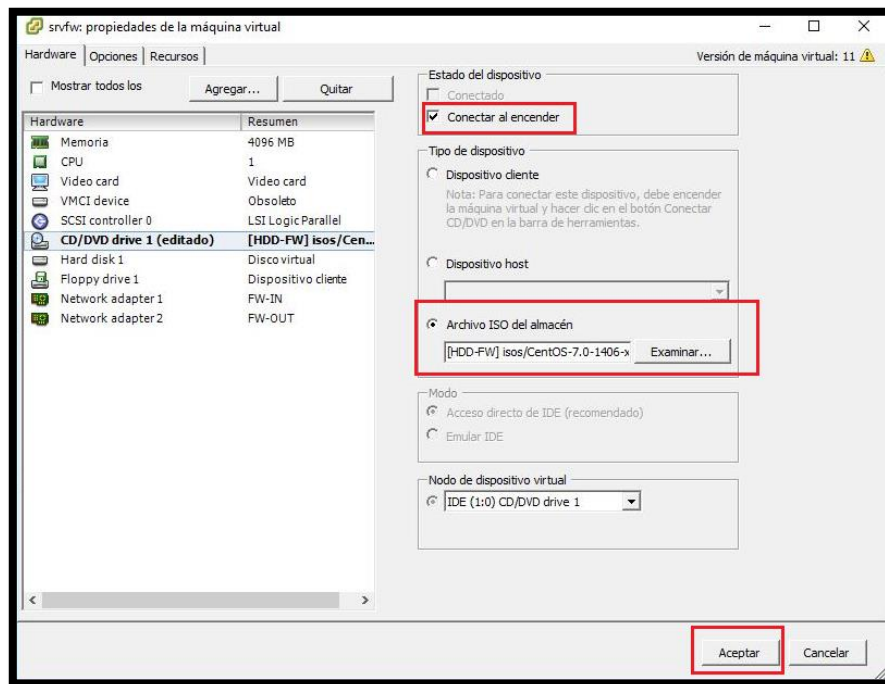


Imagen 75 – Selección del ISO para booteo

12. Una vez creada la máquina virtual, dar click derecho sobre la misma y elegir la opción **Abrir consola**, se abrirá una nueva ventana que sería una especie de “monitor” donde veremos el entorno gráfico.

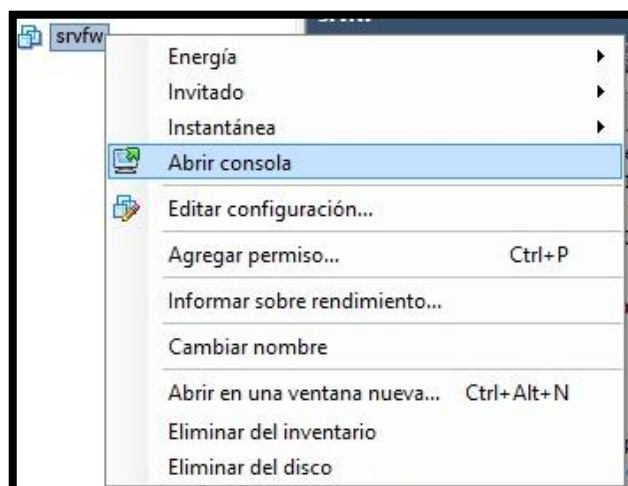


Imagen 76 – Abriendo la consola

13. Ya en la consola presionar el botón encender y esperar a que cargue el ISO y el menú de instalación de CentOS 7, escoger la primera opción **Install CentOS 7**.

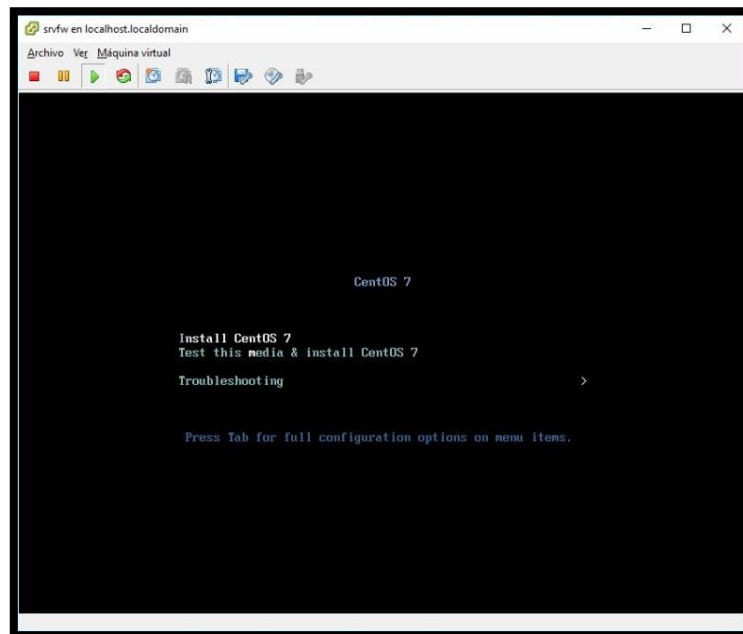


Imagen 77 – Instalación de CenOS7

14. De preferencia seleccionar el idioma inglés, ya que la mayoría de soluciones se encuentran en este idioma y es más fácil hallarlas.

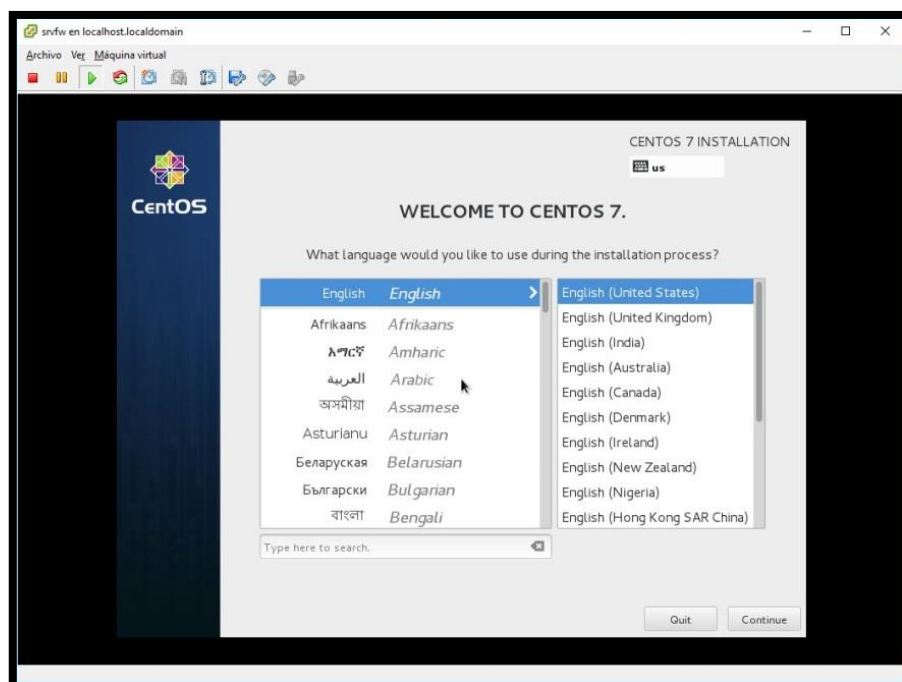


Imagen 78 – Idioma del sistema operativo

15. En la siguiente pantalla se podrá observar el resumen de lo que se va a instalar, se empezará por la zona horaria para esto seleccionamos la opción **DATE & TIME**, en donde ubicaremos la ciudad de Guayaquil y se deberá observar que la fecha y la hora sean las correctas, para finalizar presionar el botón **Done**

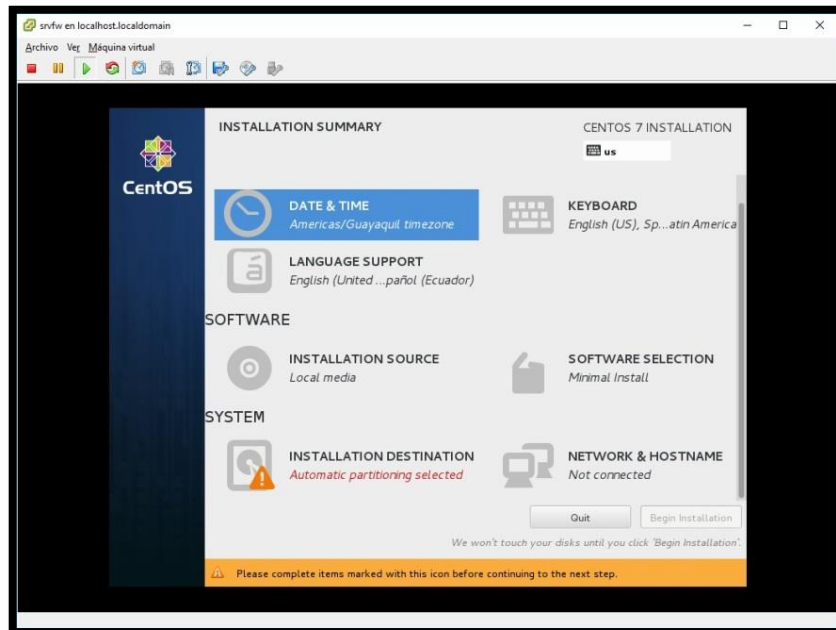


Imagen 79 – Configuración del uso horario

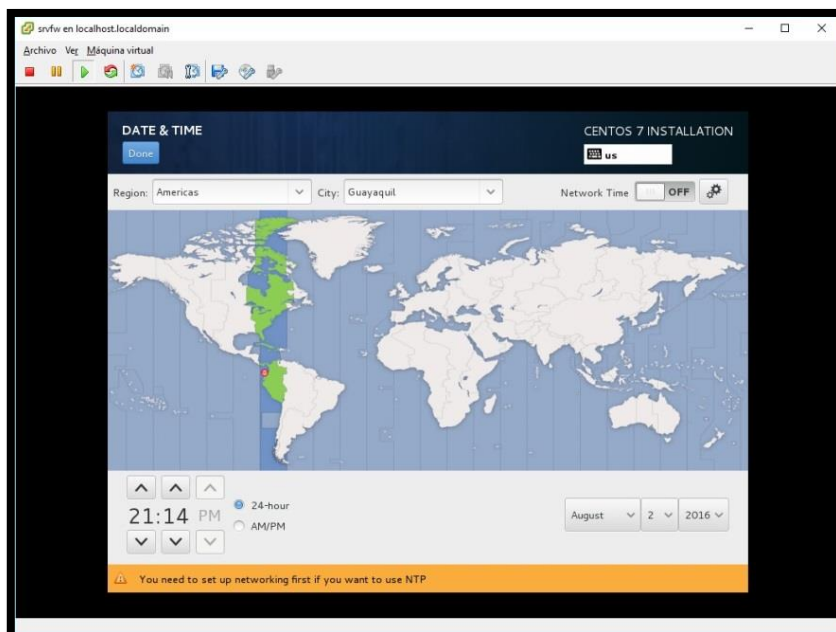


Imagen 80 – Selección de la Ciudad y la hora

16. En la siguiente opción del Teclado, dejar la versión que viene en inglés por defecto y añadir el idioma del teclado físico que se tenga.

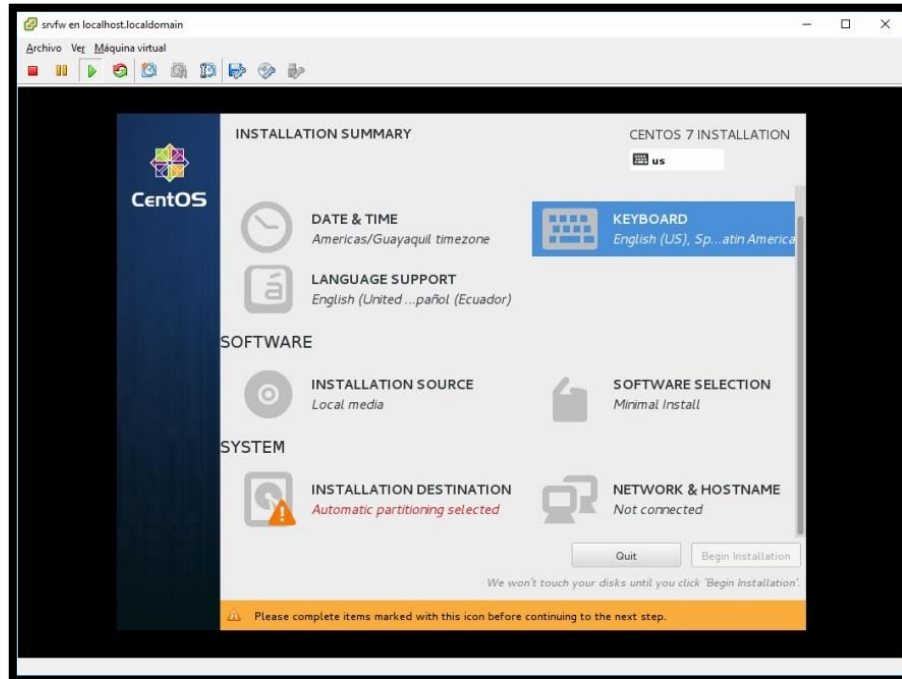


Imagen 81 – Configuración idioma del teclado

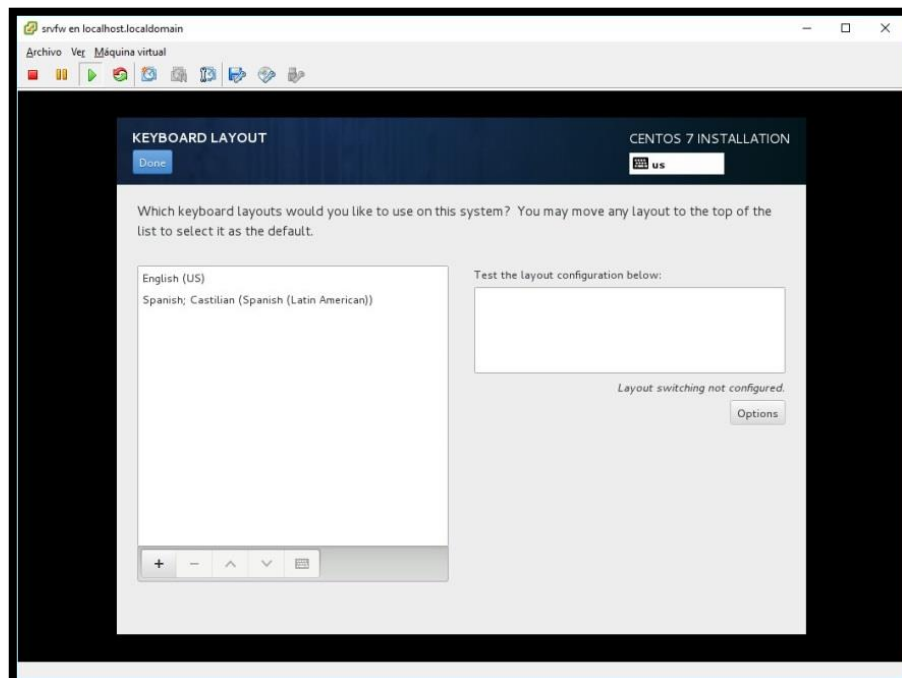


Imagen 82 – Agregar nuevo idioma del teclado

17. Al igual que en el paso anterior, dejar el idioma por defecto y añadir un segundo idioma en este caso Español.

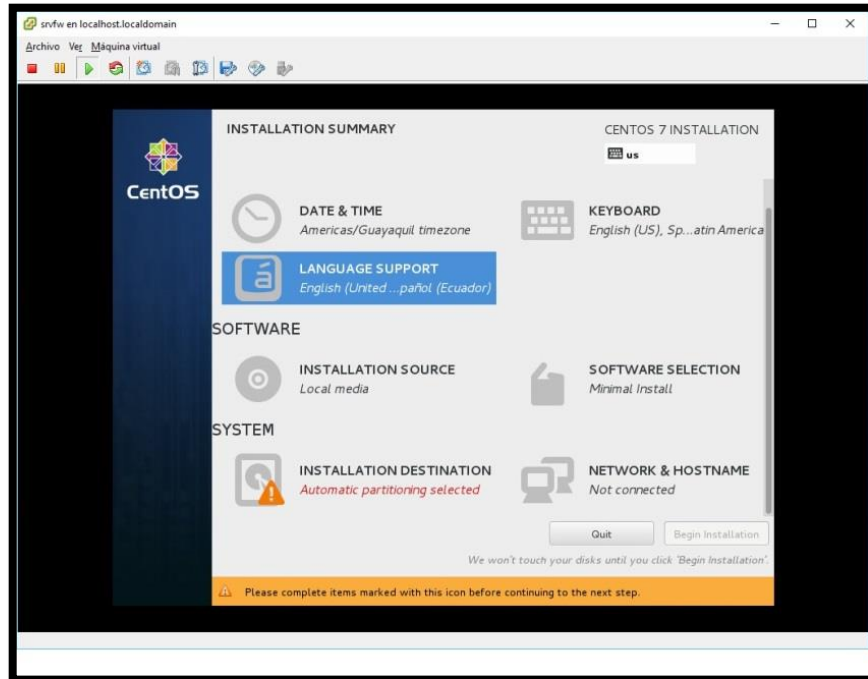


Imagen 83 – Configuración idioma del sistema operativo

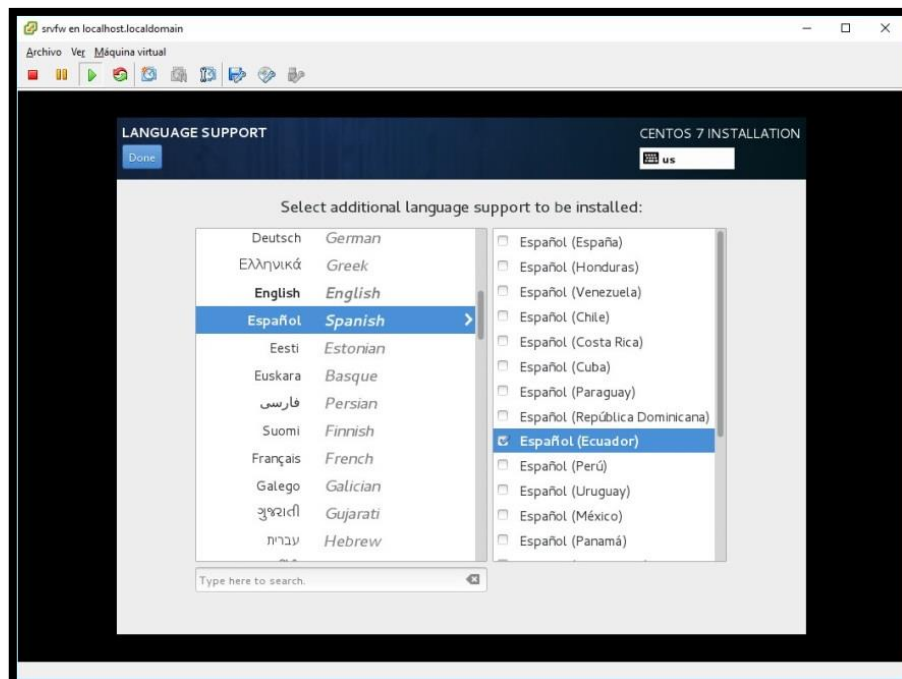


Imagen 84 – Agregar nuevo idioma al sistema operativo

18. En la opción de las tarjetas de red, asignar las direcciones IP teniendo en cuenta las conexiones físicas, una interfaz debe estar conectada al proveedor y otra debe estar conectada a la LAN.

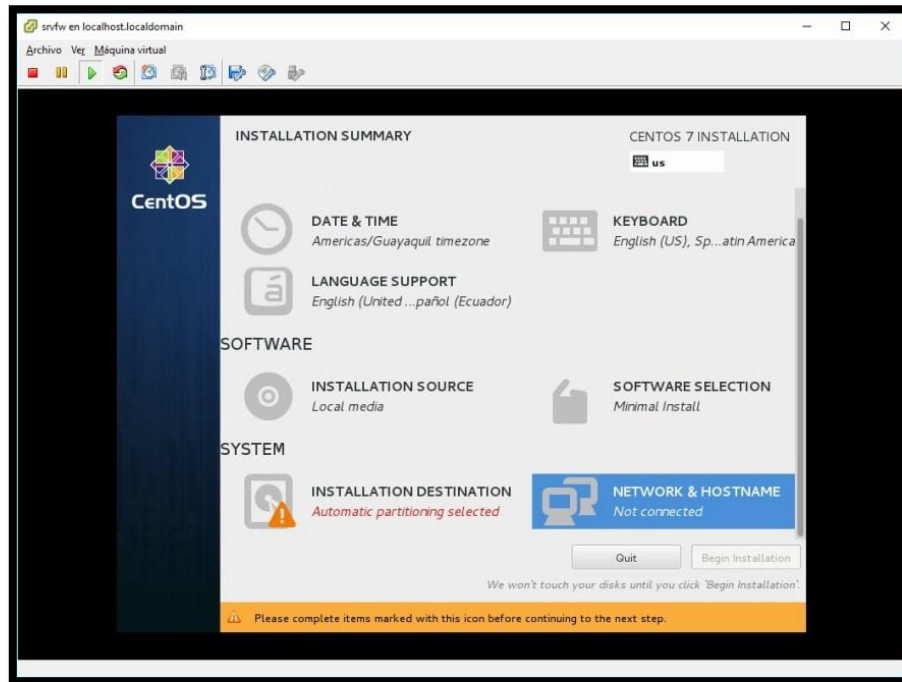


Imagen 85 – Configuración interfaces de red

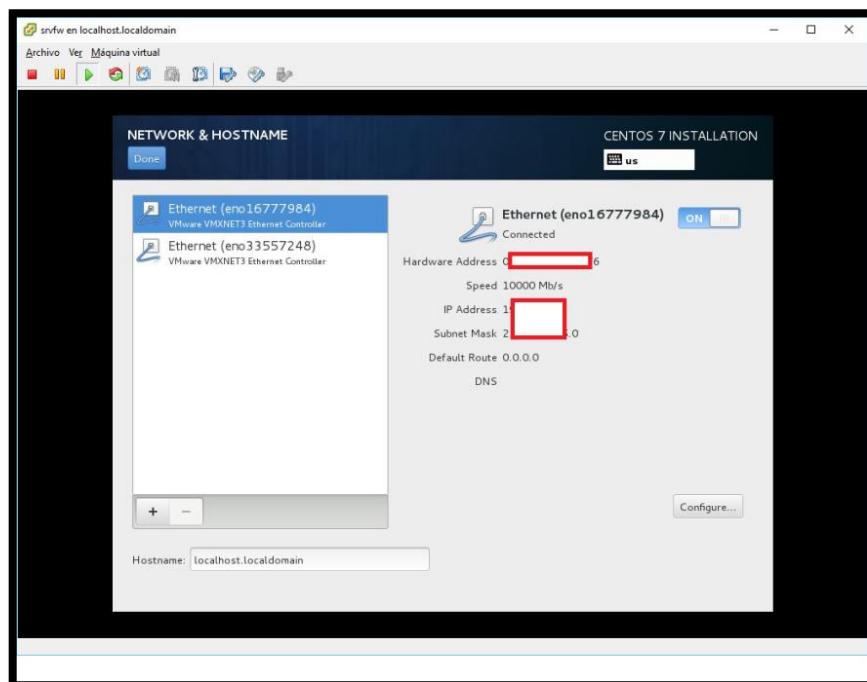


Imagen 86 – Añadir direcciones IP a las interfaces de red

19. En la configuración del disco duro hay que definir las particiones, primero se deberá seleccionar la opción **I will configure partitioning**, presionar Done y crear el particionamiento.

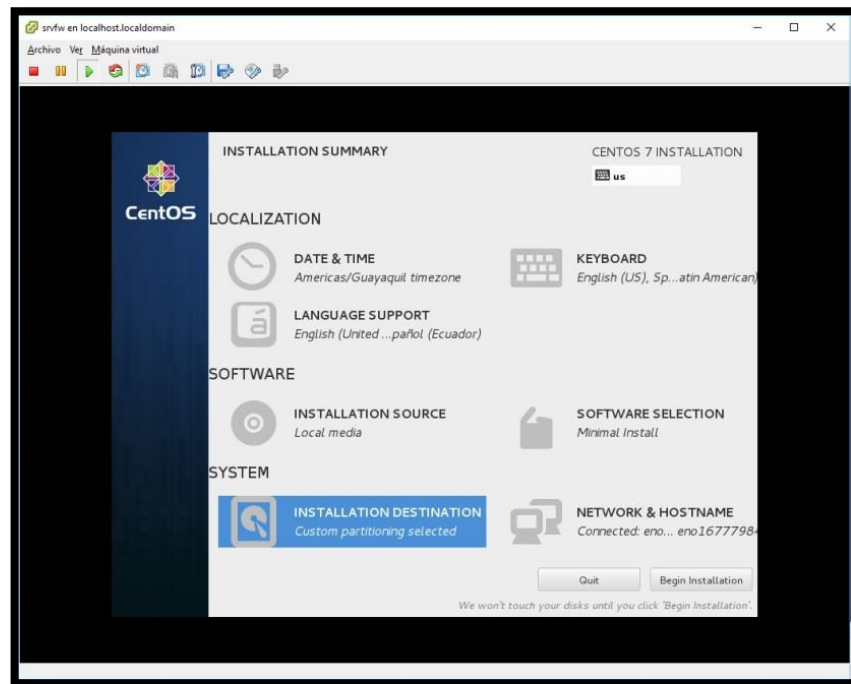


Imagen 87 – Configurar destino de instalación

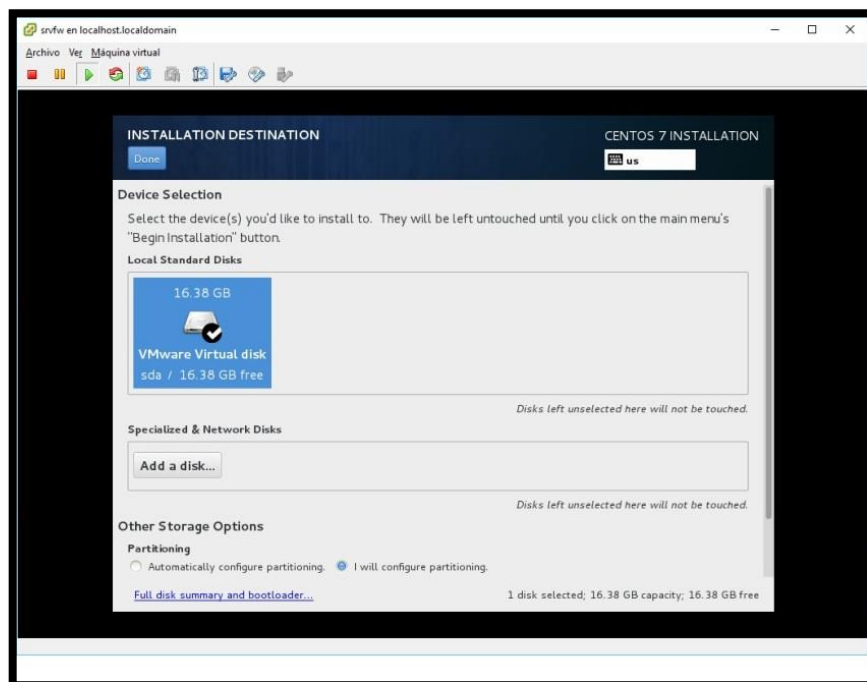


Imagen 88 – Selección del disco para particionarlo

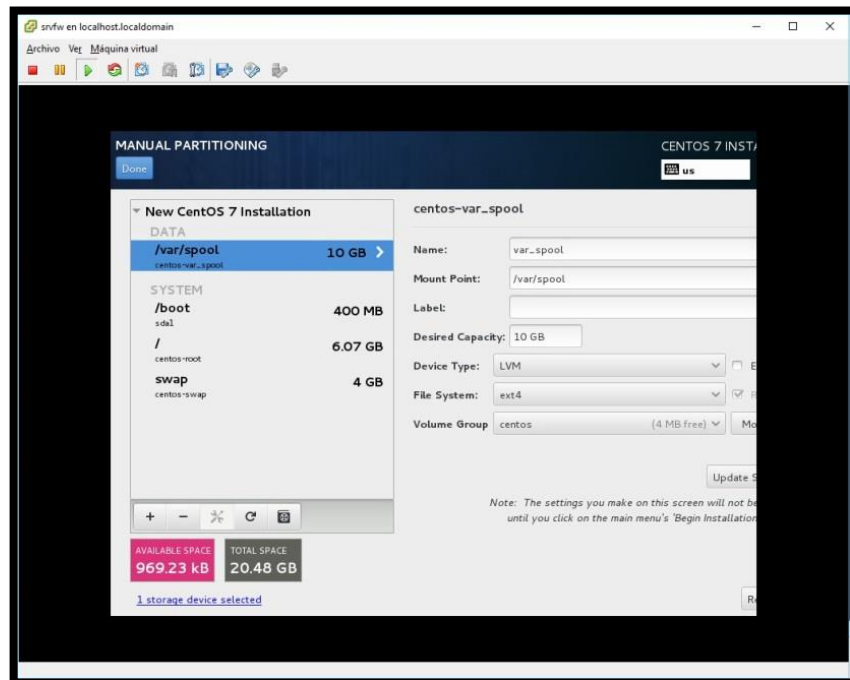


Imagen 89 – Particiones del disco duro

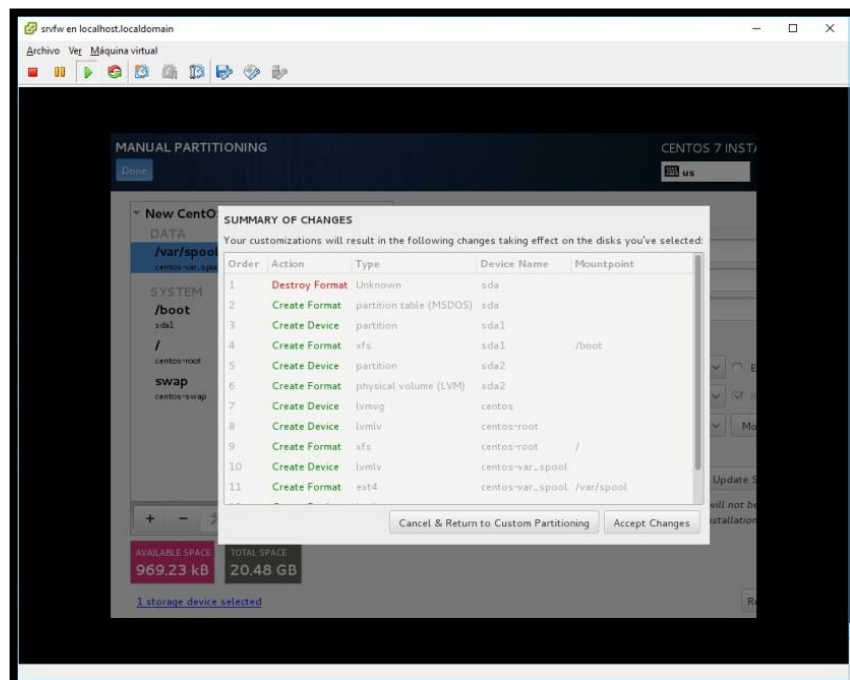


Imagen 90 – Resumen del particionamiento

20. Empezará con la instalación del sistema operativo, pero se debe crear una contraseña para root, es recomendable colocar contraseñas robustas como ya se explicó anteriormente.

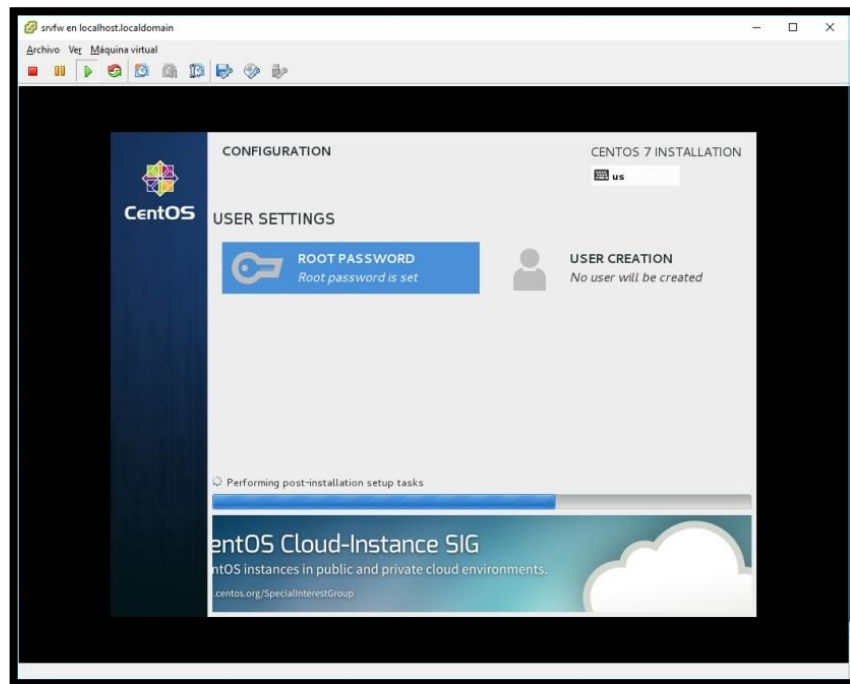


Imagen 91 – Instalación del sistema operativo

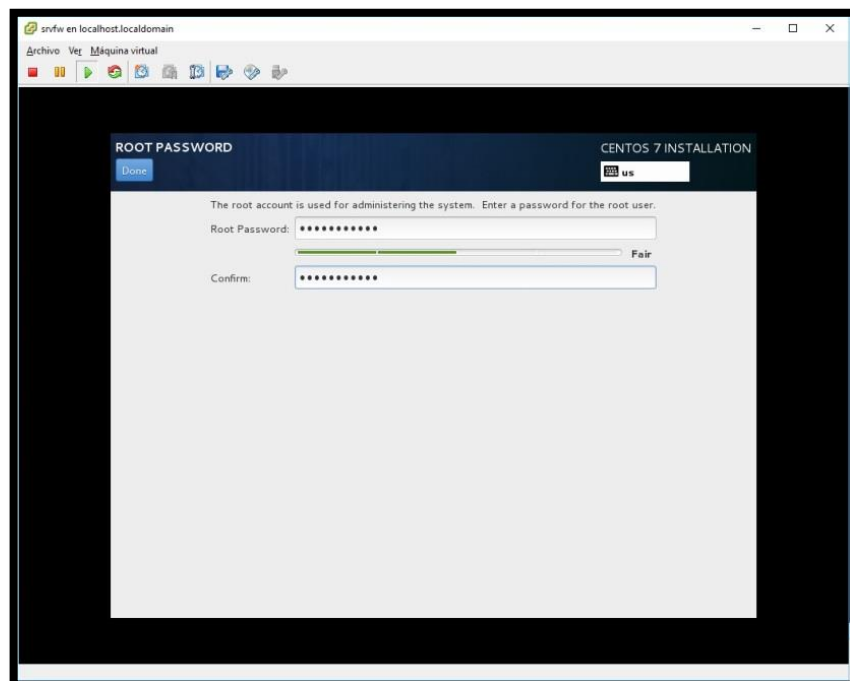


Imagen 92 – Contraseña del root

21. Cuando haya culminado la instalación, presionar en el botón Reboot para reiniciar la virtual.

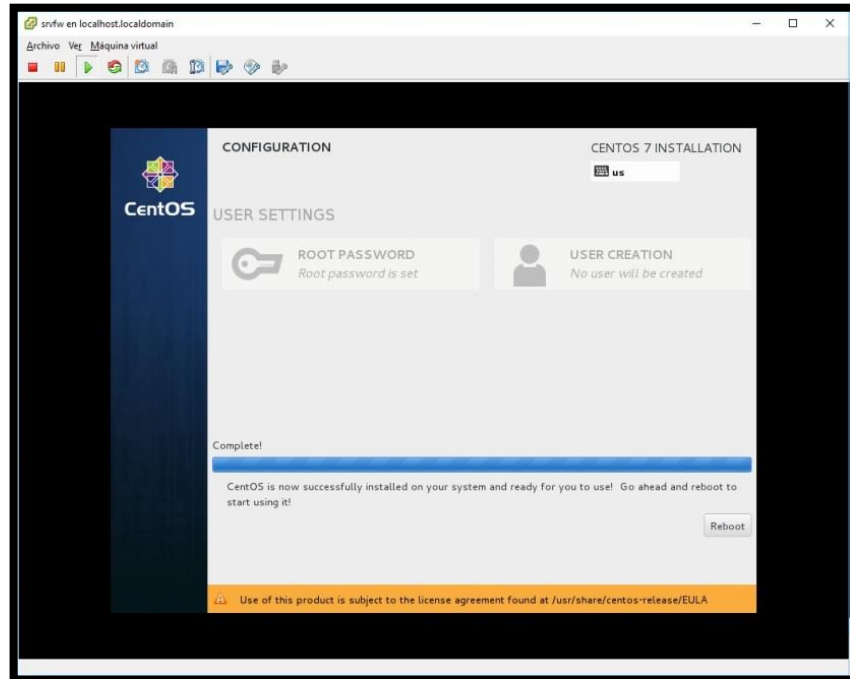


Imagen 93 – Finalización y reinicio del servidor

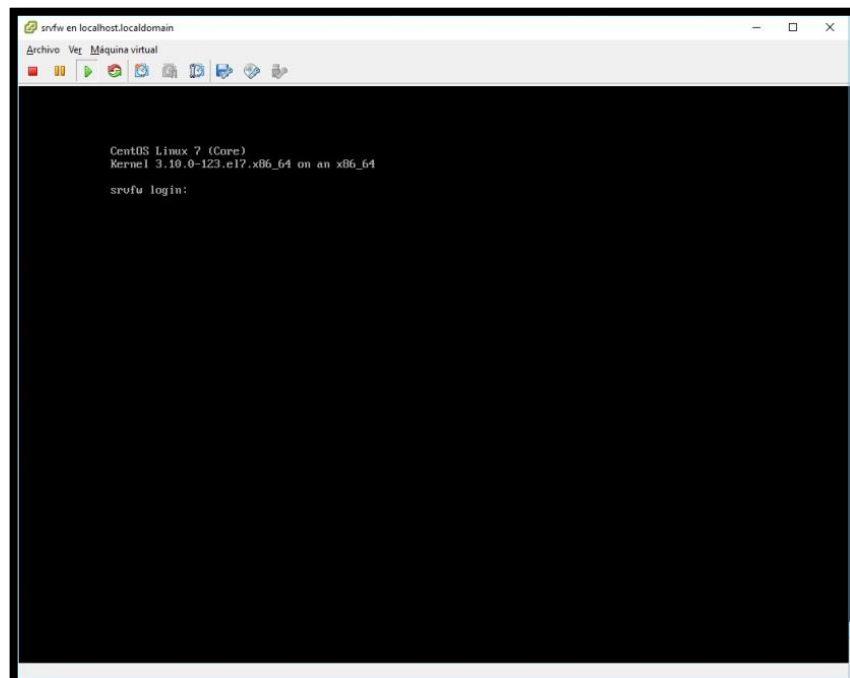


Imagen 94 – Pantalla principal de CentOS 7 minimal

22. Para mayor comodidad se recomienda utilizar programas para conectarse por SSH a la virtual, ya que se pueden copiar, pegar comandos y desde la consola solo se puede escribir.

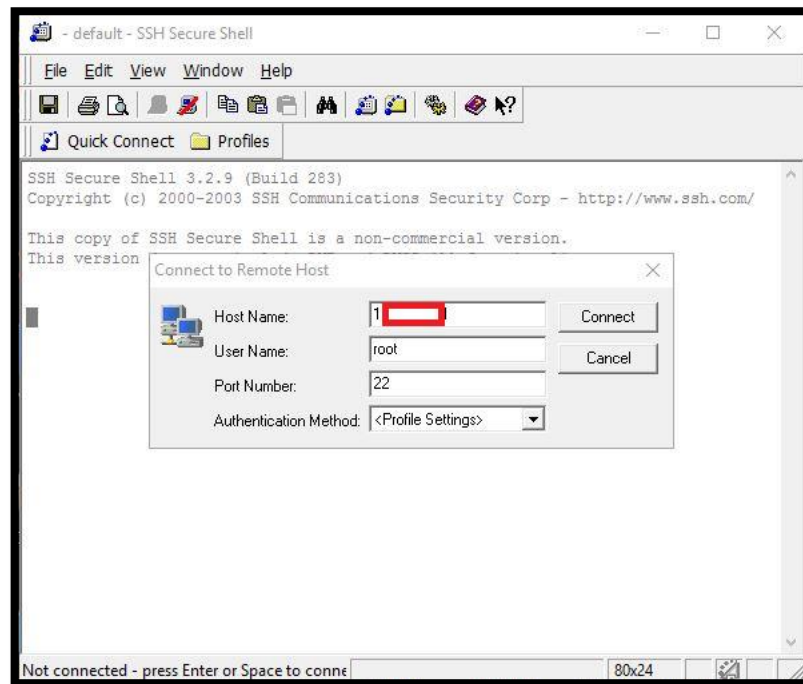


Imagen 95 – uso de SSH secure Shell

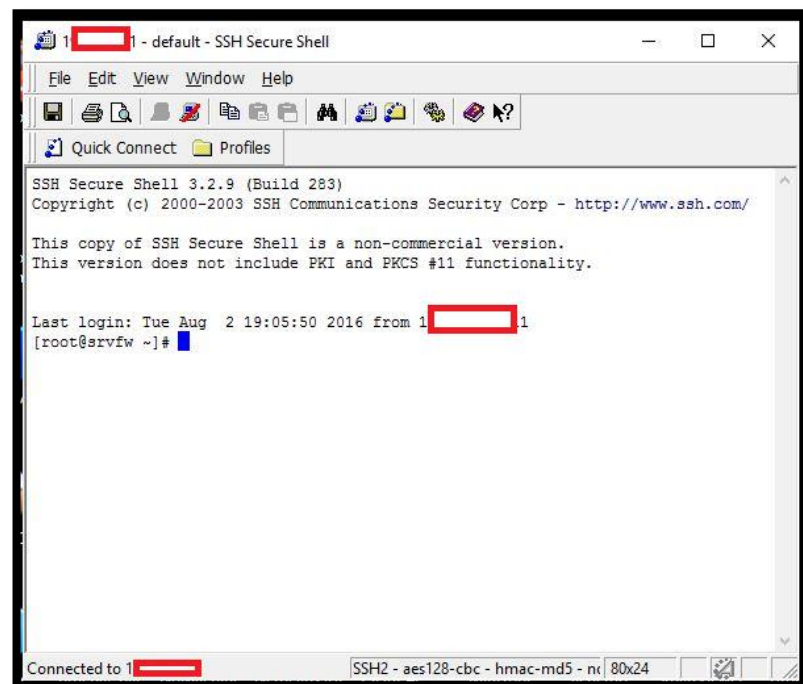


Imagen 96 – Consola ssh servidor FW

23. Una vez instalado, hay que configurar las interfaces de red, para lo cual es necesario ingresar como root, para dirigirse a la carpeta de configuración de la tarjeta de red ejecutar los siguientes comandos.

```
# cd /etc/sysconfig/network-script/  
# ls
```

```
ifcfg-eno16777984  ifdown-eth  ifdown-ppp  ifdown-tunnel  ifup-ppp  ifup-post  ifup-teamport  network-functions-ipv6  
ifcfg-eno33557248  ifdown-ppp  ifdown-routes  ifup  ifup-ipv6  ifup-ppp  ifup-tunnel  route-enp5s2  
ifcfg-lo  ifdown-ipv6  ifdown-sit  ifup-aliases  ifup-isdn  ifup-routes  ifup-wireless  
ifdown  ifdown-isdn  ifdown-team  ifup-bnep  ifup-plip  ifup-sit  init.ipv6-global  
ifdown-bnep  ifdown-post  ifdown-teamport  ifup-eth  ifup-plusb  ifup-team  network-functions
```

Imagen 97 – Interfaces de red servidor FW

Se puede apreciar que los archivos a modificar son los siguientes:

- ifcfg-eno16777984 – Interfaz para la LAN
- ifcfg-eno33557248 – Interfaz para la WAN

24. Ingresar a la interfaz de la red WAN

```
# vi ifcfg-eno33557248
```

25. Una vez dentro configurar lo siguiente:

- IPADDR0= La IP estática que asignada por el proveedor de internet.
- PREFIX0= El prefijo de la máscara de Subred.
- GATEWAY0= La puerta de enlace signada por el proveedor de internet.
- DNS1= El DNS principal del proveedor de internet.
- DNS2= El DNS secundario del proveedor de internet.

```
TYPE=Ethernet  
BOOTPROTO=none  
DEFROUTE=yes  
IPV4_FAILURE_FATAL=no  
IPV6INIT=no  
IPV6_AUTOCONF=yes  
IPV6_DEFROUTE=yes  
IPV6_PEERDNS=yes  
IPV6_PEERROUTES=yes  
IPV6_FAILURE_FATAL=no  
NAME=  
UUID=  
ONBOOT=yes  
HWADDR=  
IPADDR0=  
PREFIX0=29  
GATEWAY0=  
DNS1=200.  
DNS2=200.
```

Imagen 98 – Contenido Interfaz WAN

26. Ingresar a la interfaz de la red LAN

```
# vi ifcfg-eno16777984
```

27. Al igual que la interfaz anterior configurar lo siguiente:

- ONBOOT= Escribir yes para que arranque cada que el servidor se reinicie
- IPADDR0= La IP que se haya asignado a este servidor
- PREFIX0= El prefijo de la máscara de Subred.
- DOMAIN= El nombre de dominio de la red

```
TYPE="Ethernet"
BOOTPROTO="none"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="no"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_PEERDNS="yes"
IPV6_PEERROUTES="yes"
IPV6_FAILURE_FATAL="no"
NAME=
UUID=
ONBOOT="yes"
IPADDR0=
PREFIX0="24"
HWADDR=
DOMAIN="esnualsa.edu.ec"
```

Imagen 99 – Contenido Interfaz LAN

28. Modificar el archivo /etc/sysconfig/network, y agregar lo siguiente:

- GATEWAY= La puerta de enlace del proveedor de internet

```
# Created by anaconda
GATEWAY=
```

Imagen 100 – Contenido archivo network

29. Modificar el archivo /etc/selinux/config

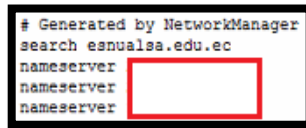
- Modificar la línea selinux: SELINUX=disabled

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Imagen 101 – Contenido archivo selinux

30. Configurar el archivo /etc/resolv.conf

- search esnualsa.edu.ec
- nameserver Las IP de los DNS

A screenshot of a terminal window showing the content of the /etc/resolv.conf file. The text is: # Generated by NetworkManager, search esnualsa.edu.ec, nameserver [redacted], nameserver [redacted], nameserver [redacted]. The redacted areas are highlighted with red rectangles.

```
# Generated by NetworkManager
search esnualsa.edu.ec
nameserver 
nameserver 
nameserver 
```

Imagen 102 – Contenido resolv.conf

31. Deshabilitar servicios

Existen ciertos servicios que se deben deshabilitar ya que no son necesarios para la configuración de este servidor. A continuación se detallará ciertos comandos que van a ser necesarios a partir de ahora.

- Para ver los servicios activos ejecutar:
`systemctl list-unit-files --type=service`
- Para detener un servicio ejecutar:
`systemctl stop nombredeservicio.service`
- Para iniciar un servicio ejecutar:
`systemctl start nombredeservicio.service`
- Para reiniciar un servicio ejecutar:
`systemctl restart nombredeservicio.service`
- Para deshabilitar un servicio ejecutar:
`systemctl disable nombredeservicio.service`
- Para habilitar un servicio ejecutar:
`systemctl enable nombredeservicio.service`

32. Utilizando los comandos del paso **solo dejar habilitados** los siguientes servicios:

- auditd
- crond
- getty
- irqbalance
- kdump
- lv2-monitor
- microcode
- rsyslog
- sshd

33. Reiniciar el servidor.

34. Probar si hay salida a internet para proceder a instalar paquetes.

```
PING www.google.com (74.125.21.104) 56(84) bytes of data.
64 bytes from yv-in-f104.1e100.net (74.125.21.104): icmp_seq=1 ttl=44 time=69.0 ms
64 bytes from yv-in-f104.1e100.net (74.125.21.104): icmp_seq=2 ttl=44 time=68.6 ms
64 bytes from yv-in-f104.1e100.net (74.125.21.104): icmp_seq=3 ttl=44 time=68.5 ms
64 bytes from yv-in-f104.1e100.net (74.125.21.104): icmp_seq=4 ttl=44 time=68.5 ms
64 bytes from yv-in-f104.1e100.net (74.125.21.104): icmp_seq=5 ttl=44 time=68.5 ms
64 bytes from yv-in-f104.1e100.net (74.125.21.104): icmp_seq=6 ttl=44 time=69.4 ms
64 bytes from yv-in-f104.1e100.net (74.125.21.104): icmp_seq=7 ttl=44 time=68.5 ms
^C
--- www.google.com ping statistics ---
```

Imagen 103 – Ping a google

35. Actualizar el sistema, con la finalidad de corregir posibles bugs, este proceso tardará unos minutos, una vez finalizado reiniciar el servidor.

```
# yum update -y
```

```
perl-Compress-Raw-Bzip2 x86_64 2.061-3.el7 base 32 K
perl-Compress-Raw-Zlib x86_64 1:2.061-4.el7 base 57 K
perl-DIT x86_64 1.627-4.el7 base 602 K
perl-Data-Dumper x86_64 2.145-3.el7 base 47 K
perl-Digest x86_64 1.17-245.el7 base 29 K
perl-Digest-HMAC x86_64 2.52-3.el7 base 30 K
perl-Encode x86_64 2.51-7.el7 base 1.5 M
perl-Exporter x86_64 5.68-3.el7 base 26 K
perl-File-Fetch x86_64 2.08-2.el7 base 26 K
perl-File-Temp x86_64 0.23-01-3.el7 base 56 K
perl-Filters x86_64 1.49-3.el7 base 76 K
perl-Getopt-Long x86_64 2.40-2.el7 base 56 K
perl-HTTP-Libwww x86_64 0.020-3.el7 base 38 K
perl-IO-Compress x86_64 2.060-2.el7 base 260 K
perl-Mail-Daemon x86_64 0.48-6.el7 base 51 K
perl-MailTools x86_64 3.40-5.el7 base 92 K
perl-Pod-Parse x86_64 0.2020-14.el7 base 36 K
perl-Pod-Parser x86_64 1.11.04-286.el7 base 50 K
perl-Pod-Perldoc x86_64 3.20-4.el7 base 87 K
perl-Pod-Simple x86_64 1.13.28-4.el7 base 216 K
perl-Pod-Usage x86_64 1.63-3.el7 base 27 K
perl-Scalar-List-Utils x86_64 1.27-245.el7 base 36 K
perl-Socket x86_64 2.010-3.el7 base 49 K
perl-Storable x86_64 2.45-3.el7 base 77 K
perl-Text-ParseWords x86_64 3.29-4.el7 base 14 K
perl-Time-HiRes x86_64 4.11.0725-3.el7 base 49 K
perl-Time-Local x86_64 1.2350-2.el7 base 24 K
perl-constant x86_64 1.27-2.el7 base 19 K
perl-libe x86_64 4.10.16.3-286.el7 base 487 K
perl-macros x86_64 4.10.16.3-286.el7 base 43 K
perl-parent x86_64 1.10.225-244.el7 base 12 K
perl-podlators x86_64 2.5.1-3.el7 base 112 K
perl-threads x86_64 1.07-4.el7 base 49 K
perl-threads-shared x86_64 1.43-6.el7 base 39 K

Transaction Summary
-----
Install 1 Package (+38 Dependent packages)

Total download size: 15 M
Installed size: 48 M
Downloading packages:
(1/39): libcomp-2.0-9.el7.x86_64.rpm | 20 kB 00:00:00
(2/39): perl-Compress-Raw-Bzip2-2.061-3.el7.x86_64.rpm | 32 kB 00:00:00
(3/39): perl-Compress-Raw-Zlib-2.061-4.el7.x86_64.rpm | 19 kB 00:00:00
(4/39): libtool-ltdl-2.4.2-21.el7_2.x86_64.rpm | 49 kB 00:00:00
(5/39): perl-Compress-Raw-Zlib-2.061-4.el7.x86_64.rpm | 57 kB 00:00:00
```

Imagen 104 – Actualización de CentOS 7

36. Instalación y configuración del proxy.

```
# yum install squid -y
```

37. Una vez concluida la instalación, habilitar e iniciar el servicio squid.

```
# systemctl enable squid.service
# systemctl start squid.service
```

38. Ingresar a la carpeta de configuración y crear los diferentes archivos para controlar la red.

```
# cd /etc/squid/
```

Una vez dentro se creará una carpeta llamada **reglas**, dentro de esta carpeta se crearán los siguientes archivos:

- ip_administrativo: Direcciones IP del personal administrativo.
- ip_navegacion: Direcciones IP con ciertos permisos de navegación.
- ip_celulares: Direcciones IP para equipos móviles.
- ip_estudiantes: Direcciones IP de las PC de laboratorio de computación.

También se creará una carpeta llamada **listas**, y está tendrá los siguientes archivos:

- redes_sociales: Direcciones web de redes sociales.
- restringidas: Direcciones web de páginas que se restringirán.
- sitios-descargas: Direcciones web de servidores de descargas.
- sitios-inocentes: Direcciones web que saltarán por encima del proxy.
- updates: Direcciones web de sitios que ofrecen actualizaciones.
- videos: Direcciones web de servidores de video.

```
[root@srvfw squid]# cd reglas/
[root@srvfw reglas]# ll
total 16
-rwxr-xr-x 1 root root 70 Aug 2 19:40 ip_administrativo
-rwxr-xr-x 1 root root 59 Aug 2 19:39 ip_celulares
-rwxr-xr-x 1 root root 86 Aug 2 19:41 ip_estudiantes
-rwxr-xr-x 1 root root 50 Aug 2 19:51 ip_navegacion
drwxr-xr-x 2 root root 119 Aug 2 19:48 listas
```

Imagen 105 – Contenido Carpeta reglas

```
[root@srvfw reglas]# cd listas
[root@srvfw listas]# ll
total 24
-rwxr-xr-x 1 root root 20 Aug 2 19:45 redes-sociales
-rwxr-xr-x 1 root root 25 Aug 2 19:46 restringidas
-rwxr-xr-x 1 root root 25 Aug 2 19:46 sitios-descargas
-rwxr-xr-x 1 root root 23 Aug 2 19:45 sitios-inocentes
-rwxr-xr-x 1 root root 22 Aug 2 19:47 updates
-rwxr-xr-x 1 root root 28 Aug 2 19:48 videos
[root@srvfw listas]#
```

Imagen 106 – Contenido Carpeta listas

39. Ingresar al archivo squid.conf, el texto original del archivo contiene configuraciones generales, las cuales se modificarán para aplicar algunas políticas de control de acceso (ACL).

El archivo original contiene lo siguiente:

```
# Recommended minimum configuration:

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8      # RFC1918 possible internal network
acl localnet src 172.16.0.0/12   # RFC1918 possible internal network
acl localnet src 192.168.0.0/16  # RFC1918 possible internal network
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # waits
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-agent
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

# Recommended minimum Access Permission configuration:

# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow localhost access from localhost
http_access allow localhost manager
http_access deny manager

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
http_access deny to_localhost

# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 3128

# Uncomment and adjust the following to add a disk cache directory.
#cache_dir ufs /var/spool/squid 100 16 256

# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid

#
# Add any of your own refresh_pattern entries above these.
#
refresh_pattern ^ftp:          1440  20% 10080
refresh_pattern ^gopher:      1440  0%  1440
refresh_pattern -i (/cgi-bin/|\?) 0  0%  0
refresh_pattern .              0 20% 4320
```

Imagen 107 – Contenido archivo squid.conf

40. Especificar las listas de control de acceso (ACL)

Por general su sintaxis es la siguiente:

`acl` [nombre de la lista] `src` [lo que compone la lista]

`acl` [nombre de la lista] `src` "[ruta de la lista]"

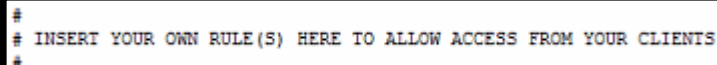
De forma predeterminada el archivo de configuración tiene listas de control de acceso para todas las redes locales, estas son:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- fcc00::/7
- fe80::/10.

Es recomendable deshabilitarlas colocando al inicio de la línea el símbolo #.

41. Especificar reglas de control de acceso

Estas definen si se permite o deniega acceso hacia squid. Estas reglas se aplican a las ACL declaradas. Se recomienda ubicarlas en la sección de reglas de control de acceso definidas, luego de la siguiente leyenda.



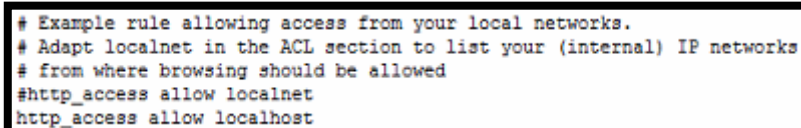
```
#  
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS  
#
```

Imagen 108 – Línea de referencia del archivo squid.conf

La sintaxis básica de una regla de control de acceso es la siguiente:

`http_access` [`deny` o `allow`] [lista de control de acceso]

Para desactivar la configuración predeterminada y poder utilizar una diferente es necesario comentar la línea que incluye `http_access allow localnet`:



```
# Example rule allowing access from your local networks.  
# Adapt localnet in the ACL section to list your (internal) IP networks  
# from where browsing should be allowed  
#http_access allow localnet  
http_access allow localhost
```

Imagen 109 –Control de Acceso

42. Aplicar las listas y reglas de control de acceso

- Declarar las ACL

```

acl ip_administrativo src "/etc/squid/reglas/ip_administrativo"
acl ip_estudiantes src "/etc/squid/reglas/ip_estudiantes"
acl ip_celulares src "/etc/squid/reglas/ip_celulares"
acl ip_navegacion src "/etc/squid/reglas/ip_navegacion"

acl videos dstdom_regex "/etc/squid/reglas/listas/videos"
acl redes-sociales dstdom_regex "/etc/squid/reglas/listas/redes-sociales"
acl restringidas dstdom_regex "/etc/squid/reglas/listas/restringidas"
acl sitios-descargas dstdom_regex "/etc/squid/reglas/listas/sitios-descargas"
acl updates url_regex "/etc/squid/reglas/listas/updates"
acl sitios-inocentes dstdom_regex "/etc/squid/reglas/listas/sitios-inocentes"

```

Imagen 110 – Declaración de ACL

- Crear las reglas de control de acceso

```

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
http_access allow sitios-inocentes
http_access allow ip_celulares !updates
http_access allow ip_administrativo
http_access allow ip_navegacion !restringidas !sitios-descargas !updates
http_access allow ip_estudiantes !videos !redes-sociales !restringidas !sitios-descargas !updates

```

Imagen 111 – Reglas de control de acceso

43. Modificar la opción http_port

Esta opción es la que permite indicar porque puerto va a escuchar las peticiones el squid. El valor predeterminado para este propósito es el 3128, otro puerto utilizado también es el 8080, depende de cada administrador de la red decidir qué puerto se utiliza.

```

# Squid normally listens to port 3128
http_port 3128 intercept

```

Imagen 112 – Opción http_port

44. Opciones varias a configurar

Opción cache_dir

Con este parámetro se puede definir el tamaño que va a utilizar Squid para almacenar la caché en el disco duro. De modo predeterminado Squid utilizará el formato ufs para crear el directorio en /var/spool/squid con 100Mb de caché, dividido en jerarquías de 16 subdirectorios con hasta 256 niveles cada uno:

`cache_dir ufs /var/spool/squid 100 16 256`

Se puede incrementar el tamaño del caché tanto como se lo desee, se debe de tener en cuenta que mientras más caché se almacene menos ancho de

banda se va a consumir, pero si esta caché es muy grande puede provocar que la búsqueda dentro de sus directorios sea más lenta y esto se traduzca en una navegación lenta a los ojos del usuario final.

En la siguiente línea se especificará un tamaño de caché de 2 Gb usando el sistema de ficheros aufs que es el recomendado cuando el proxy va a tener muchos clientes conectados.

```
cache_dir aufs /var/spool/squid 2048 16 256
```

Opción `maximum_object_size`

Este parámetro permite definir el tamaño máximo de los objetos del caché, se recomienda poner un tamaño de 48MB:

```
maximum_object_size 48 MB
```

Opciones `cache_swap_low` y `cache_swap_high`

Es necesario que se haga una limpieza de caché de Squid cuando éste llegue a cierta capacidad. La opción `cache_swap_low` establece el porcentaje a partir del cual se comenzará a limpiar el cache. La opción `cache_swap_high` establece el porcentaje a partir del cual se comenzará a limpiar de manera agresiva el cache.

Se recomienda ubicarlo en 90% el mínimo y 95% el máximo.

```
cache_swap_low 90
```

```
cache_swap_high 95
```

Opción `cache_mem`

Este parámetro en las nuevas versiones de Squid no viene especificado en el archivo de configuración pero su valor predeterminado es de 256 MB, este valor está bien para entornos de pocos usuarios. Si el Squid va a atender muchos clientes se recomienda disminuir el valor para que exista más espacio de la memoria disponible para objetos pequeños que son frecuentemente visitados a tener un espacio amplio para objetos grandes que son poco utilizados. El parámetro recomendado es 48 MB.

```
cache_mem 48 MB
```



```
#
# Add any of your own refresh_pattern entries above these.
#
refresh_pattern ^ftp:          1440      20%      10080
refresh_pattern ^gopher:       1440      0%       1440
refresh_pattern -i (/cgi-bin/|\?) 0       0%        0
refresh_pattern .               0         20%      4320

maximum_object_size 48 MB
cache_swap_low 90
cache_swap_high 95
cache_mem 48 MB
```

Imagen 113 – Opciones varias

45. Archivo final con las configuraciones aplicadas

```
# Recommended minimum configuration:
#
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed.
#cl localnet src 10.0.0.0/8      # RFC1918 possible internal network
#cl localnet src 172.16.0.0/12   # RFC1918 possible internal network
#cl localnet src 192.168.0.0/16  # RFC1918 possible internal network
#cl localnet src fe80::/7        # RFC 4193 local private network range
#cl localnet src fe80::/10       # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 20          # ftp
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280          # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl CONNECT method CONNECT

acl ip_administrative src "/etc/squid/regex/ip_administrative"
acl ip_estudiantes src "/etc/squid/regex/ip_estudiantes"
acl ip_celulares src "/etc/squid/regex/ip_celulares"
acl ip_navegacion src "/etc/squid/regex/ip_navegacion"

acl videos dstdom_regex "/etc/squid/regex/listas/videos"
acl redes-sociales dstdom_regex "/etc/squid/regex/listas/redes-sociales"
acl restringidas dstdom_regex "/etc/squid/regex/listas/restringidas"
acl sitios-descargas dstdom_regex "/etc/squid/regex/listas/sitios-descargas"
acl updates url_regex "/etc/squid/regex/listas/updates"
acl sitios-inocentes dstdom_regex "/etc/squid/regex/listas/sitios-inocentes"

ftp_passive on

# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachegr access from localhost
http_access allow localhost manager
http_access deny manager

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#

http_access allow sitios-inocentes
http_access allow ip_celulares !updates
http_access allow ip_administrative
http_access allow ip_navegacion !restringidas !sitios-descargas !updates
http_access allow ip_estudiantes !videos !redes-sociales !restringidas !sitios-descargas !updates

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 3128 intercept

# Uncomment and adjust the following to add a disk cache directory.
#cache_dir ufs /var/spool/squid 100 16 256
#cache_dir aufs /var/spool/squid 2048 16 256

# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid

#
# Add any of your own refresh_pattern entries above these.
#
refresh_pattern ^ftp:          1440      20%      10080
refresh_pattern ^gopher:       1440      0%       1440
refresh_pattern -i (/cgi-bin/|\?) 0       0%        0
refresh_pattern .               0         20%      4320

maximum_object_size 48 MB
cache_swap_low 90
cache_swap_high 95
cache_mem 48 MB
```

Imagen 114 – Archivo squid.conf editado

46. Reiniciar el servicio squid para que se apliquen los cambios.

```
# systemctl reload squid.service
```

47. Instalación y configuración de iptables

En la instalación del tipo Minimal ya viene por defecto instalado el paquete de iptables, pero es recomendable ejecutar el comando para buscar actualizaciones e instalar el agente que permite manipularlo como servicio.

```
# yum install iptables iptables-services -y
```

48. Habilitar e iniciar el servicio de iptables

```
# systemctl enable iptables.service
# systemctl start iptables.service
```

Para configurar las iptables se puede ejecutar individualmente las instrucciones o crear un script para su posterior ejecución.

En este manual se creará un script detallando uno a uno los parámetros que se irán configurando.

Se planteará un escenario donde el firewall va a tener políticas de todo negado y se irán abriendo los puertos necesarios para el funcionamiento del proxy con Squid.

49. Crear un archivo llamado firewall.sh dentro de cualquier directorio del disco duro. Se recomienda ubicarlo dentro /etc/sysconfig para tener una mejor organización de los directorios.

```
# cd /etc/sysconfig/  
# vi firewall.sh
```

```
#!/bin/bash  
#####  
##### Ecabezado #####  
  
##### UNIVERSIDAD DE GUAYAQUIL  
##### FACULTAD DE MATEMATICAS Y FISICAS  
##### CARRERA DE INGENIERIA EN NETWORKING Y TELECOMUNICACIONES  
##### AUTORES:  
##### Andres Del Pozo Espin  
##### Johanna Hernandez Paramo  
##### Puesto en produccion: 15/08/2016  
  
##### Fin Ecabezado #####  
#####  
##### Variables #####  
#####  
IP_WAN1=XXX.XXX.XXX.XXX      #IP proveedor  
RED_WAN=XXX.XXX.XXX.XXX/29   #Segmento de RED WAN  
IP_MAIL=YYY.YYY.YYY.YYY     #IP servidor de correo  
IP_WEB=YYY.YYY.YYY.YYY      #IP servidor web  
IP_DNS=YYY.YYY.YYY.YYY      #IP DNS creado  
IF_LAN=eno16777984           #nombre de la interfaz LAN  
IF_WAN=eno33557248           #nombre de la interfaz WAN  
RED_LOCAL=YYY.YYY.YYY.YYY/24 #Segmento de RED LAN  
IP_ADMIN1=YYY.YYY.YYY.YYY    #IP para el usuario administrador  
  
DNS1=XXX.XXX.XXX.XXX         #DNS principal del proveedor  
DNS2=XXX.XXX.XXX.XXX         #DNS secundario del proveedor  
##### Fin Variables #####  
#####  
##### Cargar modulos adicionales  
modprobe ip_nat_ftp  
modprobe nf_conntrack_pptp  
modprobe nf_nat_pptp  
##### Fin de cargar modulos adicionales  
#####
```

```

##### Flush de Reglas #####
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables -t mangle -F
iptables -t filter -F
##### Fin Flush de Reglas #####
#####
##### Politicas por Defecto #####
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
##### Fin Politicas por Defecto #####
#####
##### Definimos las políticas Como el firewall es DROP
##### empezamos a abrir los puertos necesarios
## *****
# Al localhost le damos full acceso
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
## *****

# Damos acceso full a un ip de administracion de Internet
#
iptables -A INPUT -s $IP_ADMIN1 -j ACCEPT
iptables -A FORWARD -s $IP_ADMIN1 -j ACCEPT
iptables -t nat -A PREROUTING -s $IP_ADMIN1 -p tcp --dport 80 -j ACCEPT
iptables -t nat -A POSTROUTING -s $IP_ADMIN1 -o $IF_WAN -j SNAT --to-source $IP_WAN2
iptables -A OUTPUT -d $IP_ADMIN1 -j ACCEPT

#####
# Damos salida a internet a esta pc
# Puerto 80
iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --sport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT

iptables -A INPUT -p tcp -m tcp --sport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT

#Puerto 443
iptables -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --sport 443 -m state --state RELATED,ESTABLISHED -j ACCEPT

iptables -A INPUT -p tcp -m tcp --sport 443 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT
## *****

# Damos acceso a que consulte a los DnS
# Servidor DNS
iptables -A INPUT -s $IP_DNS -p udp -m udp --sport 53 -j ACCEPT
iptables -A OUTPUT -d $IP_DNS -p udp -m udp --dport 53 -j ACCEPT

# DNS1
iptables -A INPUT -s $DNS1 -p udp -m udp --sport 53 -j ACCEPT
iptables -A OUTPUT -d $DNS1 -p udp -m udp --dport 53 -j ACCEPT

# DNS2
iptables -A INPUT -s $DNS2 -p udp -m udp --sport 53 -j ACCEPT
iptables -A OUTPUT -d $DNS2 -p udp -m udp --dport 53 -j ACCEPT
## *****

```

```

# Damos acceso para que esta PC haga ping
iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -p icmp --icmp-type any -j ACCEPT

# Damos acceso para que esta PC haga traceroute
iptables -I OUTPUT -o $IF_WAN -p udp --dport 33434:33524 -m state --state NEW -j ACCEPT
iptables -I INPUT -p udp --sport 33434:33524 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
#####

# Damos acceso para que la red local pueda hacer ping y tracert
iptables -A INPUT -i $IF_LAN -s $RED_LOCAL -p ICMP -j ACCEPT
iptables -A OUTPUT -o $IF_LAN -d $RED_LOCAL -p ICMP -j ACCEPT
iptables -A FORWARD -i $IF_LAN -s $RED_LOCAL -p ICMP -j ACCEPT
#####

### Enmascaramos la red local
#
iptables -t nat -A POSTROUTING -s $RED_LOCAL -o $IF_WAN -j MASQUERADE
#

### Activamos el bit de forward
echo 1 > /proc/sys/net/ipv4/ip_forward
###
#####

#####
### Damos acceso a algunas IPs para que puedan navegar en todas las paginas por https
#
IP_CELULARES=$(egrep -v "^#" /etc/squid/reglas/ip_celulares)
for ip_celulares in $IP_CELULARES
do
    iptables -t filter -A FORWARD -i $IF_LAN -s $ip_celulares -p tcp --dport 443 -j ACCEPT
done

IP_ADMINISTRATIVO=$(egrep -v "^#" /etc/squid/reglas/ip_administrativo)
for ip_administrativo in $IP_ADMINISTRATIVO
do
    iptables -A INPUT -i $IF_LAN -s $ip_administrativo -j ACCEPT
    iptables -t nat -A PREROUTING -s $ip_administrativo -p tcp --dport 443 -j ACCEPT
    iptables -t filter -A FORWARD -i $IF_LAN -s $ip_administrativo -p tcp --dport 443 -j ACCEPT
    iptables -A OUTPUT -o $IF_LAN -d $ip_administrativo -j ACCEPT
done

#####
### Bloqueamos por nombre a ciertas paginas
#
SITES_REDES_SOCIALES=$(egrep -v "^#" /etc/squid/reglas/listas/redes-sociales)
for sites_redes_sociales in $SITES_REDES_SOCIALES
do
    iptables -t filter -A FORWARD -i $IF_LAN -s $RED_LOCAL -p tcp --dport 443 -m string --string $sites_redes_sociales --algo bm -j DROP
done

SITES_VIDEOS=$(egrep -v "^#" /etc/squid/reglas/listas/videos)
for sites_videos in $SITES_VIDEOS
do
    iptables -t filter -A FORWARD -i $IF_LAN -s $RED_LOCAL -m string --string $sites_videos --algo bm -j DROP
done

SITES_RESTRINGIDAS=$(egrep -v "^#" /etc/squid/reglas/listas/restringidas)
for sites_restringidas in $SITES_RESTRINGIDAS
do
    iptables -t filter -A FORWARD -i $IF_LAN -s $RED_LOCAL -p tcp --dport 443 -m string --string $sites_restringidas --algo bm -j DROP
done
###

```

```
#####
### Damos acceso a las ips para trafico https pero con el bloqueo de las reglas superiores
#
IP_NAVEGACION=$(egrep -v "^#" /etc/squid/reglas/ip_navegacion)
for ip_navegacion in $IP_NAVEGACION
do
    iptables -t filter -A FORWARD -i $IF_LAN -s $ip_navegacion -p tcp --dport 443 -j ACCEPT
done

###
#####

#####
### Damos acceso a paginas que salgan por otros puertos
#
iptables -t nat -A PREROUTING -s $RED_LOCAL -d 200.7.221.145 -j ACCEPT
iptables -t filter -A FORWARD -s $RED_LOCAL -p tcp -m tcp -d 200.7.221.145 --dport 8833 -j ACCEPT
iptables -t filter -A FORWARD -s $RED_LOCAL -p tcp -m tcp -d 200.7.221.145 --dport 8834 -j ACCEPT
iptables -t filter -A FORWARD -s $RED_LOCAL -p tcp -m tcp -d 200.7.221.145 --dport 443 -j ACCEPT
#
###
#####

#####
### Bloqueamos el trafico https a toda la red

iptables -t filter -A FORWARD -i $IF_LAN -s $RED_LOCAL -p tcp --dport 443 -j DROP

###
#####

#####
### Permitimos el forward desde y hacia la red local
#
iptables -t filter -A FORWARD -i $IF_LAN -o $IF_WAN -s $RED_LOCAL -d 0/0 -j ACCEPT
iptables -t filter -A FORWARD -i $IF_WAN -o $IF_LAN -d $RED_LOCAL -s 0/0 -m state --state RELATED,ESTABLISHED
-j ACCEPT
iptables -t filter -A FORWARD -i $IF_LAN -s $RED_LOCAL -d $RED_LOCAL -j ACCEPT
#####iptables -t filter -A FORWARD -i tun+ -o $IF_LAN -d $RED_LOCAL -j ACCEPT

#####
### Configuracion necesaria para el proxy
# Trafico puerto 80
iptables -t filter -A INPUT -p tcp --dport 8080 -i $IF_LAN -s $RED_LOCAL -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --sport 8080 -o $IF_LAN -d $RED_LOCAL -m state --state RELATED,ESTABLISHED
-j ACCEPT
iptables -t nat -A PREROUTING -i $IF_LAN -s $RED_LOCAL -p tcp --dport 80 -j REDIRECT --to-port 8080

# Trafico puerto 80
#iptables -t filter -A INPUT -p tcp --dport 3128 -i $IF_LAN -s $RED_LOCAL -j ACCEPT
#iptables -t filter -A OUTPUT -p tcp --sport 3128 -o $IF_LAN -d $RED_LOCAL -m state --state RELATED,ESTABLISHED
-j ACCEPT
#iptables -t nat -A PREROUTING -i $IF_LAN -s $RED_LOCAL -p tcp --dport 80 -j REDIRECT --to-port 3128

##### Servidor de paginas web
##Puerto 80
iptables -t nat -A PREROUTING -i $IF_WAN -d $IP_WAN2 -p tcp --dport 80 -j DNAT --to $IP_WEB
iptables -A FORWARD -i $IF_WAN -o $IF_LAN -d $IP_WEB -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i $IF_LAN -o $IF_WAN -s $IP_WEB -p tcp --dport 80 -j ACCEPT
iptables -t nat -A POSTROUTING -s $IP_WEB -o $IP_WAN2 -j MASQUERADE
```

```
#####
## Redireccionamos trafico hacia el servidor de correos
##### Servidor de correos
##Puerto 25 SMTP
iptables -t nat -A PREROUTING -i $IF_WAN -d $IP_WAN1 -p tcp --dport 25 -j DNAT --to $IP_MAIL
iptables -A FORWARD -i $IF_LAN -d $IP_MAIL -p tcp --dport 25 -j ACCEPT
iptables -A FORWARD -i $IF_WAN -o $IF_LAN -d $IP_MAIL -p tcp --dport 25 -j ACCEPT
iptables -A FORWARD -i $IF_LAN -o $IF_WAN -s $IP_MAIL -p tcp --dport 25 -j ACCEPT

##Puerto 110 POP3
iptables -t nat -A PREROUTING -i $IF_WAN -d $IP_WAN1 -p tcp --dport 110 -j DNAT --to $IP_MAIL
iptables -A FORWARD -i $IF_LAN -d $IP_MAIL -p tcp --dport 110 -j ACCEPT
iptables -A FORWARD -i $IF_WAN -o $IF_LAN -d $IP_MAIL -p tcp --dport 110 -j ACCEPT
iptables -A FORWARD -i $IF_LAN -o $IF_WAN -s $IP_MAIL -p tcp --dport 110 -j ACCEPT

##Puerto 143 IMAP
iptables -t nat -A PREROUTING -i $IF_WAN -d $IP_WAN1 -p tcp --dport 143 -j DNAT --to $IP_MAIL
iptables -A FORWARD -i $IF_LAN -d $IP_MAIL -p tcp --dport 143 -j ACCEPT
iptables -A FORWARD -i $IF_WAN -o $IF_LAN -d $IP_MAIL -p tcp --dport 143 -j ACCEPT
iptables -A FORWARD -i $IF_LAN -o $IF_WAN -s $IP_MAIL -p tcp --dport 143 -j ACCEPT

##Puerto 81 Web
iptables -t nat -A PREROUTING -i $IF_WAN -d $IP_WAN1 -p tcp --dport 81 -j DNAT --to $IP_MAIL
iptables -A FORWARD -i $IF_LAN -d $IP_MAIL -p tcp --dport 81 -j ACCEPT
iptables -A FORWARD -i $IF_WAN -o $IF_LAN -d $IP_MAIL -p tcp --dport 81 -j ACCEPT
iptables -A FORWARD -i $IF_LAN -o $IF_WAN -s $IP_MAIL -p tcp --dport 81 -j ACCEPT

##Puerto 8443 Web SSL
iptables -t nat -A PREROUTING -i $IF_WAN -d $IP_WAN1 -p tcp --dport 8443 -j DNAT --to $IP_MAIL
iptables -A FORWARD -i $IF_LAN -d $IP_MAIL -p tcp --dport 8443 -j ACCEPT
iptables -A FORWARD -i $IF_WAN -o $IF_LAN -d $IP_MAIL -p tcp --dport 8443 -j ACCEPT
iptables -A FORWARD -i $IF_LAN -o $IF_WAN -s $IP_MAIL -p tcp --dport 8443 -j ACCEPT

##Puerto 465 SMTPS SSL
iptables -t nat -A PREROUTING -i $IF_WAN -d $IP_WAN1 -p tcp --dport 465 -j DNAT --to $IP_MAIL
iptables -A FORWARD -i $IF_LAN -d $IP_MAIL -p tcp --dport 465 -j ACCEPT
iptables -A FORWARD -i $IF_WAN -o $IF_LAN -d $IP_MAIL -p tcp --dport 465 -j ACCEPT
iptables -A FORWARD -i $IF_LAN -o $IF_WAN -s $IP_MAIL -p tcp --dport 465 -j ACCEPT

##Puerto 995 POP3S SSL
iptables -t nat -A PREROUTING -i $IF_WAN -d $IP_WAN1 -p tcp --dport 995 -j DNAT --to $IP_MAIL
iptables -A FORWARD -i $IF_LAN -d $IP_MAIL -p tcp --dport 995 -j ACCEPT
iptables -A FORWARD -i $IF_WAN -o $IF_LAN -d $IP_MAIL -p tcp --dport 995 -j ACCEPT
iptables -A FORWARD -i $IF_LAN -o $IF_WAN -s $IP_MAIL -p tcp --dport 995 -j ACCEPT

##Puerto 993 IMAPS SSL
iptables -t nat -A PREROUTING -i $IF_WAN -d $IP_WAN1 -p tcp --dport 993 -j DNAT --to $IP_MAIL
iptables -A FORWARD -i $IF_LAN -d $IP_MAIL -p tcp --dport 993 -j ACCEPT
iptables -A FORWARD -i $IF_WAN -o $IF_LAN -d $IP_MAIL -p tcp --dport 993 -j ACCEPT
iptables -A FORWARD -i $IF_LAN -o $IF_WAN -s $IP_MAIL -p tcp --dport 993 -j ACCEPT

##Puerto 587 MSA SMTP
iptables -t nat -A PREROUTING -i $IF_WAN -d $IP_WAN1 -p tcp --dport 587 -j DNAT --to $IP_MAIL
iptables -A FORWARD -i $IF_LAN -d $IP_MAIL -p tcp --dport 587 -j ACCEPT
iptables -A FORWARD -i $IF_WAN -o $IF_LAN -d $IP_MAIL -p tcp --dport 587 -j ACCEPT
iptables -A FORWARD -i $IF_LAN -o $IF_WAN -s $IP_MAIL -p tcp --dport 587 -j ACCEPT

##Puerto TCP 2703 Ryzor Zimbra
iptables -t nat -A PREROUTING -i $IF_WAN -d $IP_WAN1 -p tcp --dport 2703 -j DNAT --to $IP_MAIL
iptables -A FORWARD -i $IF_LAN -d $IP_MAIL -p tcp --dport 2703 -j ACCEPT
iptables -A FORWARD -i $IF_WAN -o $IF_LAN -d $IP_MAIL -p tcp --dport 2703 -j ACCEPT
iptables -A FORWARD -i $IF_LAN -o $IF_WAN -s $IP_MAIL -p tcp --dport 2703 -j ACCEPT
```

```

##Puerto UDP 2703 Pyzor Zimbra
iptables -t nat -A PREROUTING -i $IF_WAN -d $IP_WAN1 -p udp --dport 24441 -j DNAT --to $IP_MAIL
iptables -A FORWARD -i $IF_LAN -d $IP_MAIL -p udp --dport 24441 -j ACCEPT
iptables -A FORWARD -i $IF_WAN -o $IF_LAN -d $IP_MAIL -p udp --dport 24441 -j ACCEPT
iptables -A FORWARD -i $IF_LAN -o $IF_WAN -d $IP_MAIL -p udp --sport 24441 -j ACCEPT

##### Servidor DNS Publico
##Puerto 53
iptables -t nat -A PREROUTING -i $IF_WAN -d $IP_WAN1 -p tcp --dport 53 -j DNAT --to $IP_DNS
iptables -A FORWARD -i $IF_WAN -o $IF_LAN -d $IP_DNS -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -i $IF_LAN -o $IF_WAN -s $IP_DNS -p tcp --dport 53 -j ACCEPT
iptables -t nat -A POSTROUTING -s $IP_DNS -o $IP_WAN1 -j MASQUERADE

iptables -t nat -A PREROUTING -i $IF_WAN -d $IP_WAN1 -p udp --dport 53 -j DNAT --to $IP_DNS
iptables -A FORWARD -i $IF_WAN -o $IF_LAN -d $IP_DNS -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -i $IF_LAN -o $IF_WAN -s $IP_DNS -p udp --dport 53 -j ACCEPT
iptables -t nat -A POSTROUTING -s $IP_DNS -o $IP_WAN1 -j MASQUERADE

#####
#### Reglas adicionales

#### Proteccion adicional en caso de que cambiemos las reglas a ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 1:1024 -j DROP
iptables -A INPUT -p udp -m udp --dport 1:1024 -j DROP
iptables -A INPUT -p tcp -m tcp --dport 3306 -j DROP
iptables -A INPUT -p tcp -m tcp --dport 5432 -j DROP
## *****

#####
#### Desactivamos el trafico IPV6 sino lo necesitamos
##
echo 1 > /proc/sys/net/ipv6/conf/all/disable_ipv6
echo 1 > /proc/sys/net/ipv6/conf/default/disable_ipv6
##
####
#####

#####
#### Bloqueamos IP Dudosa
##
iptables -A INPUT -s 213.136.75.238 -j DROP
iptables -A OUTPUT -d 213.136.75.238 -j DROP
##
###
#####
####Fin de reglas adicionales
#####
#### Fin de script

```

50. Finalmente se debe dar permisos de ejecución al archivo para posteriormente ejecutarlo

```

# chmod 755 firewall.sh
# ./firewall.sh

```

51. Para comprobar que se hayan aplicado las reglas ejecutar lo siguiente:

```

# iptables -nvL

```

52. Para que se aplique el script desde el arranque es necesario agregar la siguiente línea en el archivo /etc/rc.local

`/etc/sysconfig/firewall.sh`

```
#!/bin/bash
# THIS FILE IS ADDED FOR COMPATIBILITY PURPOSES
#
# It is highly advisable to create own systemd services or udev rules
# to run scripts during boot instead of using this file.
#
# In contrast to previous versions due to parallel execution during boot
# this script will NOT be run after all other services.
#
# Please note that you must run 'chmod +x /etc/rc.d/rc.local' to ensure
# that this script will be executed during boot.

touch /var/lock/subsys/local
/etc/sysconfig/firewall.sh
```

Imagen 115 - Archivo rc.local

53. Finalmente dar permiso de ejecución al archivo rc.local y reiniciar el servidor

```
# chmod +x /etc/rc.d/rc.local
# reboot
```

54. Segmentación del ancho de banda

Se planteará un escenario donde van a existir 2 niveles de colas, detallados a continuación:

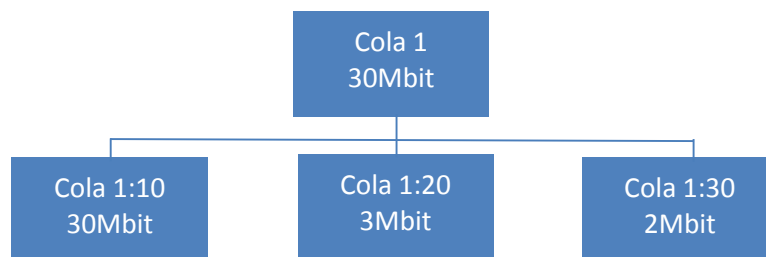


Imagen 116 - Segmentación del ancho de banda

La Cola 1: es donde se asignará todo el ancho de banda disponible, dependiendo del tipo de contrato que se posea con el proveedor de internet.

La Cola 1:10 será utilizada por un usuario TOP con todo el ancho de banda disponible.

La Cola 1:20 será utilizada por un usuario PREFERENCIAL con un ancho de banda de 3Mbits

La Cola 1:30 será utilizada por el resto de la red con un ancho de banda de 2 Mbit

55. Dentro de la ruta /etc/sysconfig crear un archivo llamado anchodebanda.sh, para tener una mejor organización de los directorios

```
# cd /etc/sysconfig/  
# vi anchodebanda.sh
```

El contenido del archivo será el siguiente

```
#!/bin/bash  
##### Ecabezado #####  
  
##### UNIVERSIDAD DE GUAYAQUIL  
##### FACULTAD DE MATEMATICAS Y FISICAS  
##### CARRERA DE INGENIERIA EN NETWORKING Y TELECOMUNICACIONES  
##### AUTORES:  
##### Andres Del Pozo Espin  
##### Johanna Hernandez Paramo  
##### Puesto en produccion: 15/08/2016  
  
##### Fin Ecabezado #####  
  
#####  
##### Variables  
# Se declara variable eth1 con el nombre de la interfaz LAN del servidor  
eth1=eno16777984  
##### Fin de Variables  
  
# #####Método para crear interfaz virtual y controlar UPLOAD  
#  
modprobe ifb  
ip link set dev ifb0 down  
ip link set dev ifb0 up  
  
##### Fin de método para UPLOAD  
## eth1 se va a llamar la interfaz para controlar el DOWNLOAD e ifb0 la interfaz para el UPLOAD  
##### Eliminamos colas presentes  
#  
tc qdisc del dev $eth1 root 2>/dev/null  
tc qdisc del dev $eth1 ingress 2>/dev/null  
tc qdisc del dev ifb0 root 2>/dev/null  
  
##### Creamos la regla para el UPLOAD  
#  
tc qdisc add dev $eth1 handle ffff: ingress  
tc filter add dev $eth1 parent ffff: protocol ip u32 match u32 0 0 action mirred egress redirect dev ifb0  
#  
#####Fin de regla del UPLOAD  
  
##### Cambiamos la tarjeta de red de método FIFO a HTB  
tc qdisc add dev $eth1 root handle 1: htb r2q 625 default 33  
tc qdisc add dev ifb0 root handle 1: htb r2q 625 default 33  
  
##### Limitamos todo el ancho de banda de subida y de bajada a 30Mbit Cola 1:  
tc class add dev $eth1 parent 1: classid 1:1 htb rate 30Mbit  
tc class add dev ifb0 parent 1: classid 1:1 htb rate 30Mbit
```

```

#### Añadimos segundo nivel de colas
#### Vamos a tener 3 colas
#### Cola 10 de Con full navegación para usuarios TOP
#### Cola 20 de 2.5Mbit con una máxima de 3Mbit para un usuario PREFERENCIALES
#### Cola 30 de 1.5Mbit con una máxima de 2Mbit (Defecto) todo lo no marcado se va por esta cola

#### Creamos las colas de download
tc class add dev $eth1 parent 1:1 classid 1:10 htb rate 30Mbit
tc class add dev $eth1 parent 1:1 classid 1:20 htb rate 2.5Mbit ceil 3Mbit
tc class add dev $eth1 parent 1:1 classid 1:30 htb rate 1.5Mbit ceil 2Mbit

#### Creamos las colas de upload
tc class add dev ifb0 parent 1:1 classid 1:10 htb rate 30Mbit
tc class add dev ifb0 parent 1:1 classid 1:20 htb rate 2.5Mbit ceil 3Mbit
tc class add dev ifb0 parent 1:1 classid 1:30 htb rate 1.5Mbit ceil 2Mbit

#### Agrupamos los paquetes del mismo tipo
tc qdisc add dev $eth1 parent 1: handle 10: sfq perturb 10
tc qdisc add dev $eth1 parent 1: handle 20: sfq perturb 10
tc qdisc add dev $eth1 parent 1: handle 30: sfq perturb 10

#####
#### Hacemos el match con la ip del usuario TOP
##Download
tc filter add dev $eth1 parent 1: protocol all prio 1 u32 match ip dst xxx.xxx.xxx.xxx classid 1:10
#Upload
tc filter add dev ifb0 parent 1: protocol all prio 1 u32 match ip src xxx.xxx.xxx.xxx classid 1:10
##
#####

#### Hacemos el match con la ip del usuario PREFERENCIAL
##Download
tc filter add dev $eth1 parent 1: protocol all prio 1 u32 match ip dst xxx.xxx.xxx.xxx classid 1:20
#Upload
tc filter add dev ifb0 parent 1: protocol all prio 1 u32 match ip src xxx.xxx.xxx.xxx classid 1:20
##
#####

#### Hacemos el match con toda la red
##Download
tc filter add dev $eth1 parent 1: protocol all prio 1 u32 match ip dst xxx.xxx.xxx.xxx/24 classid 1:30
#Upload
tc filter add dev ifb0 parent 1: protocol all prio 1 u32 match ip src xxx.xxx.xxx.xxx/24 classid 1:30
##
#####

```

57. Dar permisos de ejecución para posteriormente ejecutarlo.

```

# chmod 755 anchodebanda.sh
# ./anchodebanda.sh

```

58. Ejecutar el siguiente comando para que se apliquen las reglas.

```

# tc -s class show dev eno16777984

```

59. Agregar en el script del firewall la línea que llamará al control de ancho de banda, posteriormente reiniciar y comprobar que funcione.

```

##Aplicamos las reglas del control de ancho de banda
/etc/sysconfig/anchodebanda.sh
##Fin de script

```

60. Instalación de Webmin

Primero se debe descargar el paquete desde su web oficial, se lo puede hacer también con el siguiente comando

```
# wget http://prdownloads.sourceforge.net/webadmin/webmin-1.810-1.noarch.rpm
```

Instalar las dependencias

```
# yum -y install perl perl-Net-SSLeay openssl perl-IO-Tty
```

Instalar el paquete descargado

```
# rpm -U webmin-1.810-1.noarch.rpm
```

Finalmente ingresar al siguiente URL https://ip_servidor:10000

En caso de que salga un error de que no se tiene acceso, se deberá agregar la IP del equipo desde donde se está tratando de conectar en el archivo /etc/webmin/miniserv.conf en la penúltima línea, debe quedar de la siguiente manera:

```
allow=ip_administracion1 ip_administracion2 ip_administracion3
```

Reniciar el servicio webmin y comprobar en el navegador.

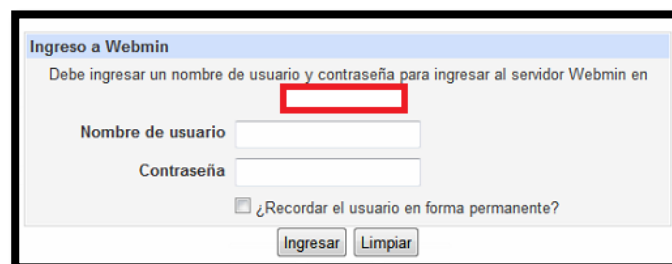


Imagen 117 – Pantalla principal Webmin

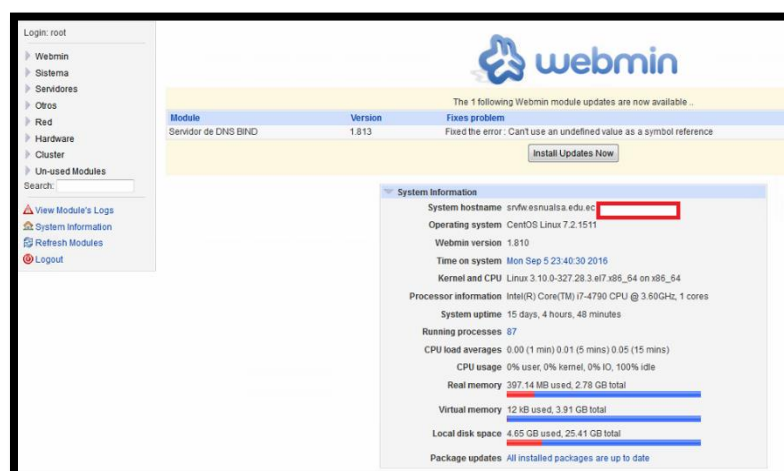


Imagen 118 – Panel de control Webmin

CREACIÓN DEL SERVIDOR DE CORREO

Antes de crear la virtual se deberá definir sus recursos físicos, estos se detallan a continuación:

- 2 HDD 1TB
- 8 GB RAM
- 1 Interfaz de red

Esta máquina virtual tendrá 2 discos asignados debido a que se aplicará RAID 1

1. Presionar la combinación Control + N para crear una nueva máquina virtual, repetir los mismo pasos del servidor firewall.

Se omitirán algunas imágenes que no tienen mayor relevancia

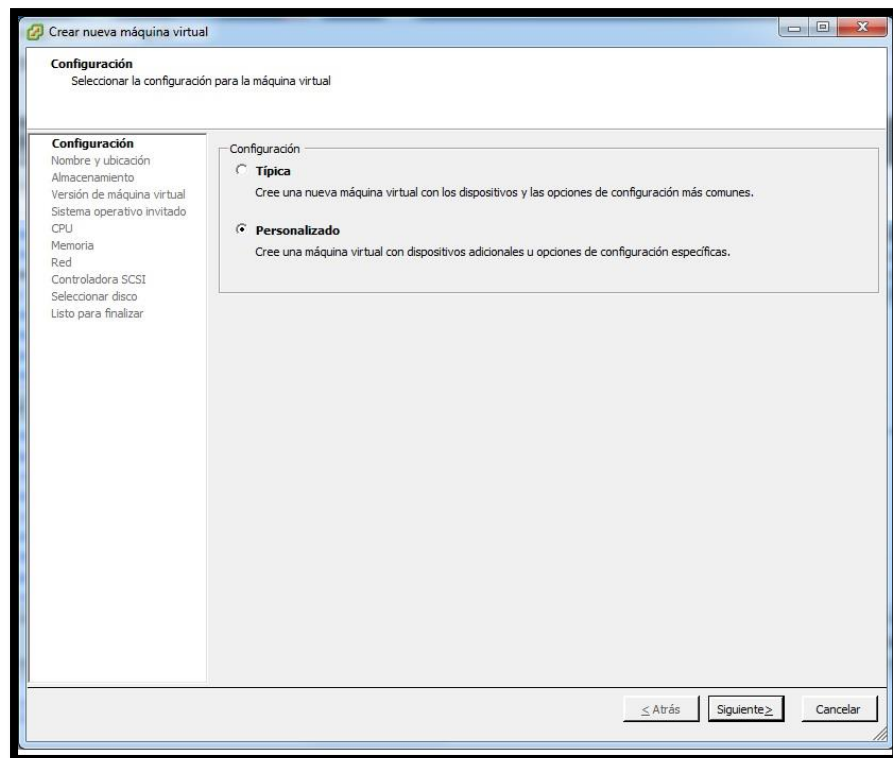


Imagen 119 – Creación de máquina virtual Servidor de Correo

2. Colocar el nombre del servidor (srvmail).

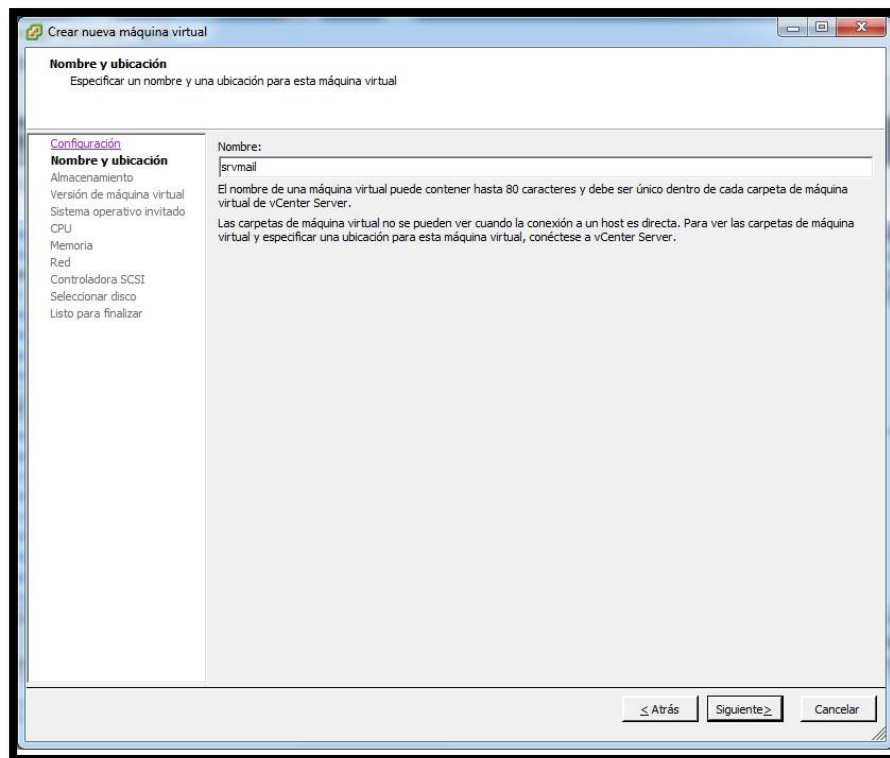


Imagen 120 – Nombre de máquina virtual

3. Elegir el disco HDD-MAIL.

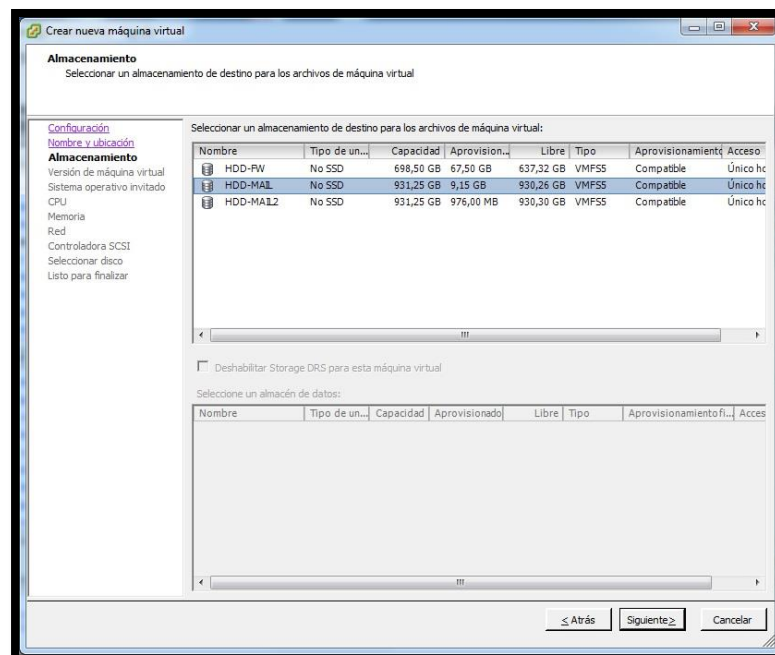


Imagen 121 – Selección del disco duro

4. Escoger el SO CentOS 4/5/6/7.

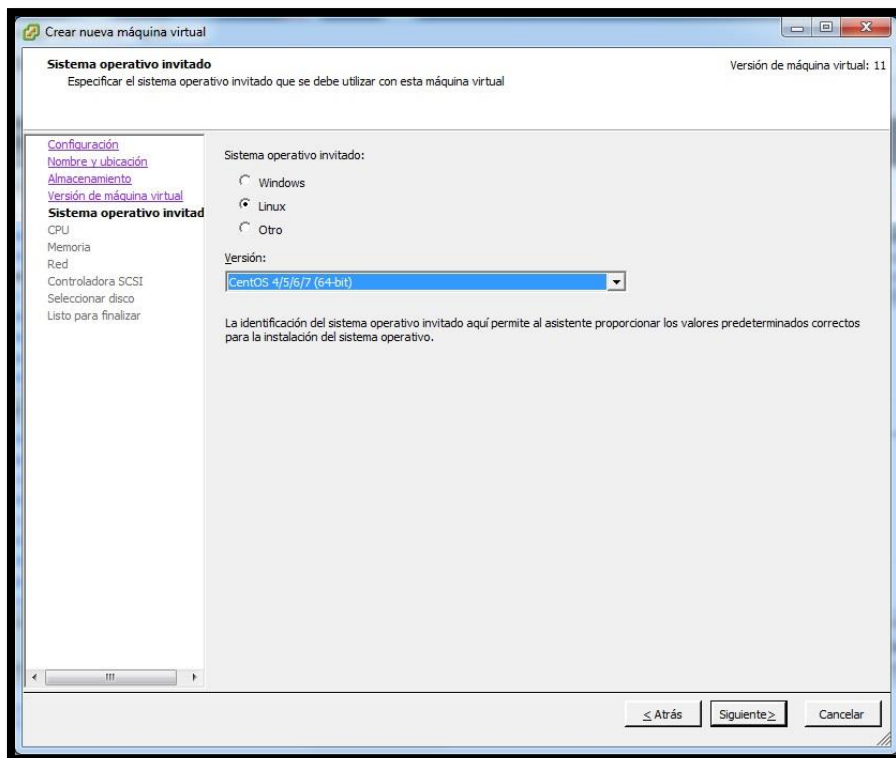


Imagen 122 – Elección del SO CentOS

5. Asignar las 8GB de memoria RAM.

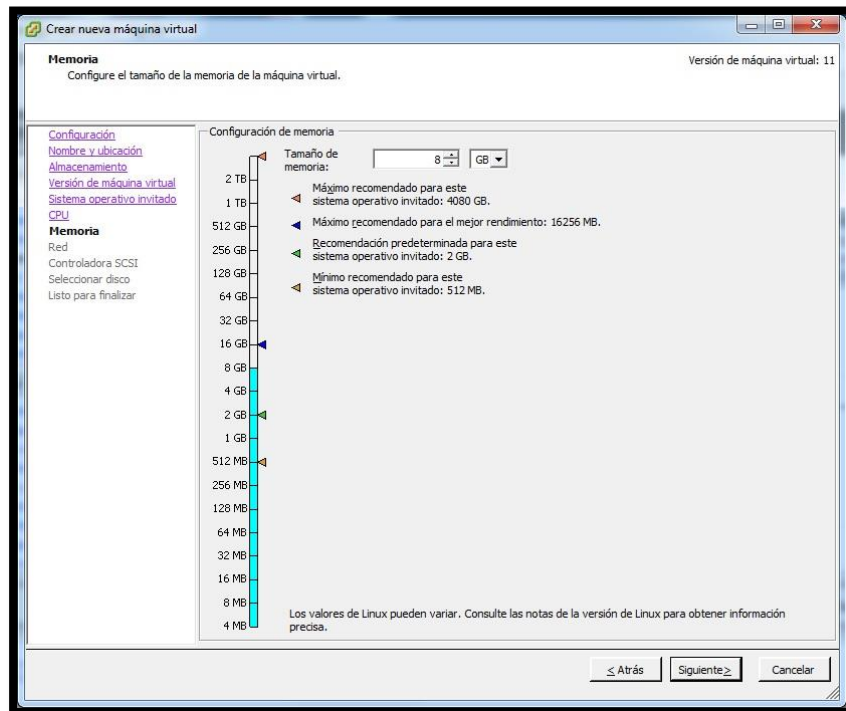


Imagen 123 – Asignación de memoria RAM

6. Escoger la interfaz de red.

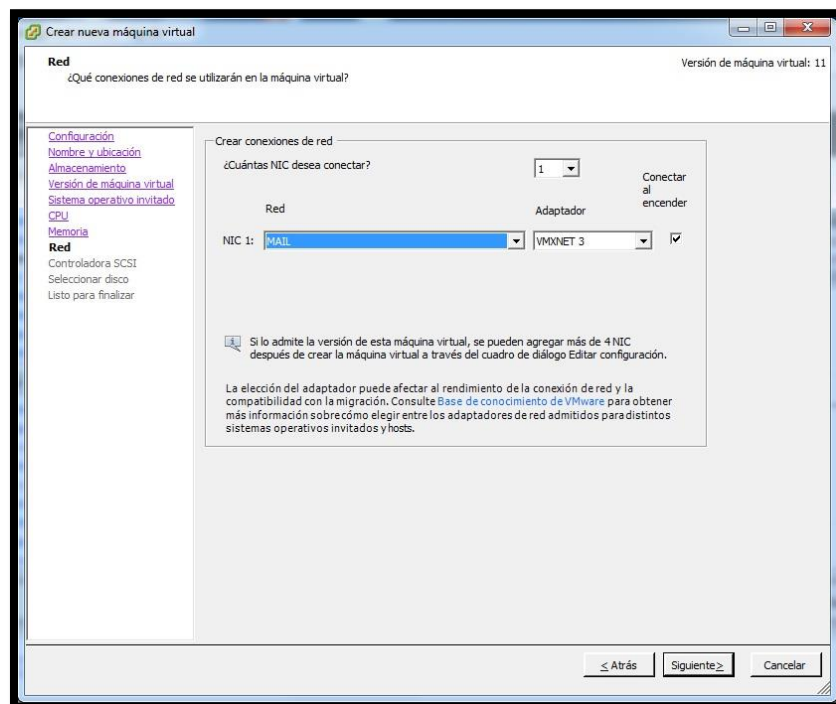


Imagen 124 – Selección de la interfaz

7. Crear un nuevo disco duro virtual, se le asignará 910 GB ya que el hypervisor toma una cierta cantidad del disco.

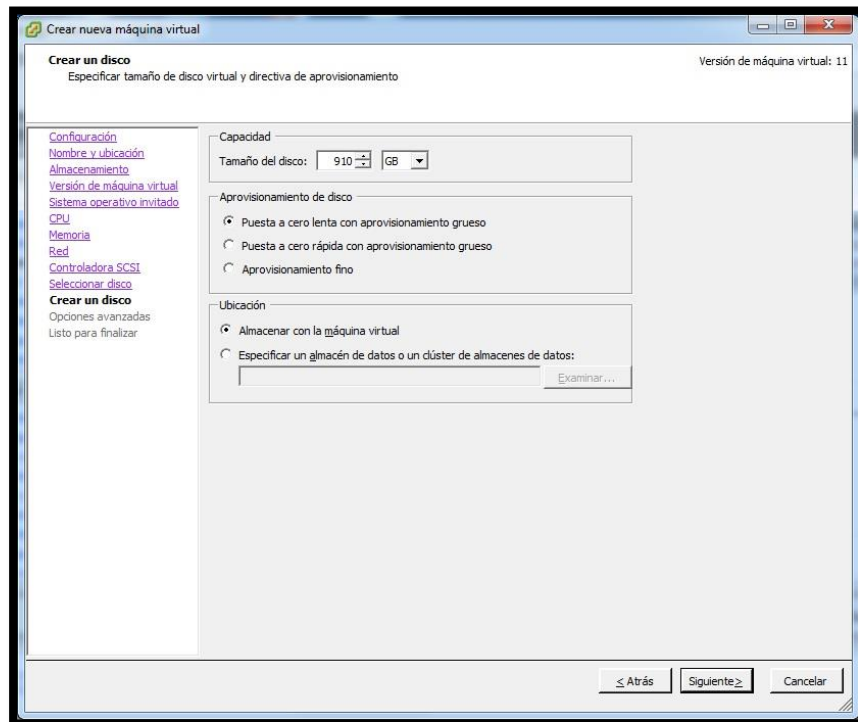


Imagen 125 – Creación de un nuevo disco

8. Antes de finalizar se agregará otro disco duro.

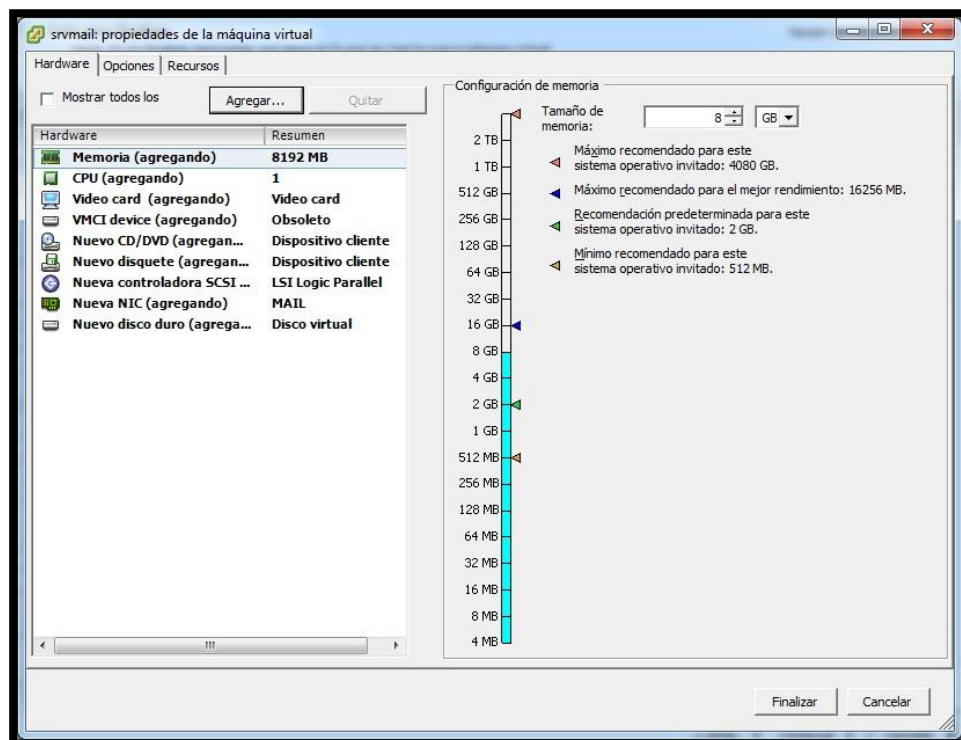


Imagen 126 – Asignación de memoria

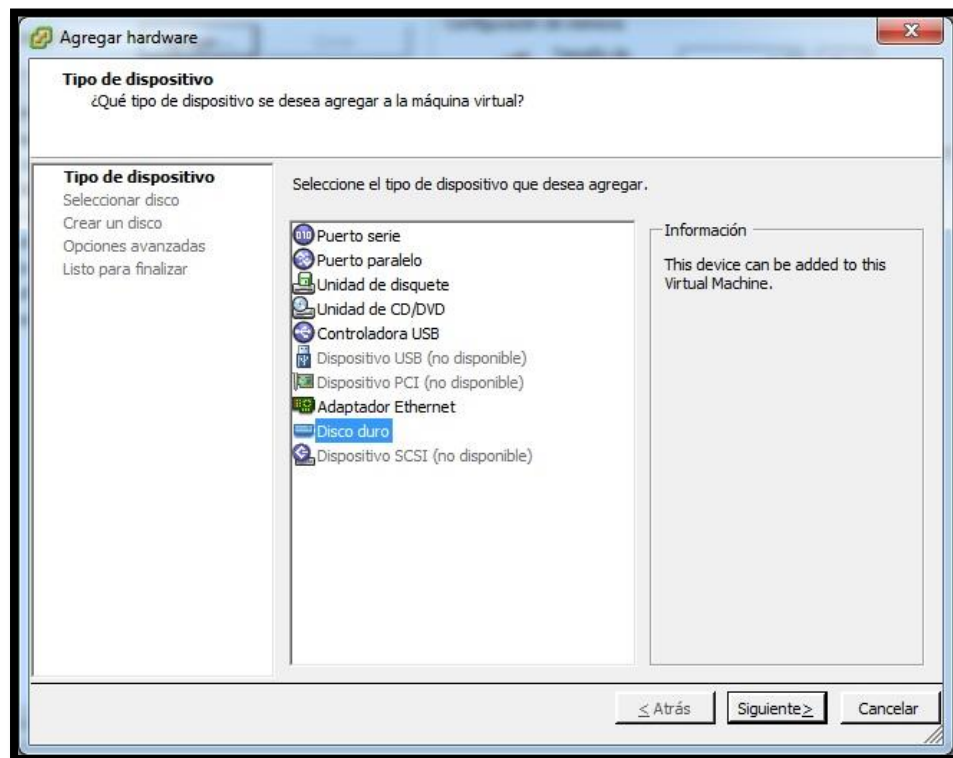


Imagen 127 – Agregación de un nuevo disco

9. En la ventana de crear un disco, elegir Especificar un almacén de datos o un clúster de almacenes de datos y elegir el HDD-MAIL2.

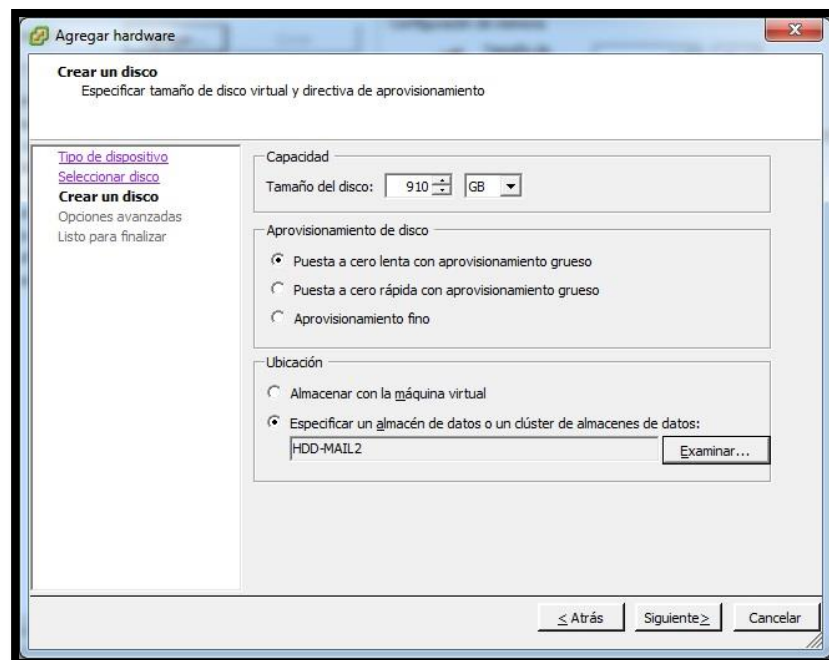


Imagen 128 – Elección del almacén de datos

10. Elegir el ISO de CentOS 7 para poder instalarlo.

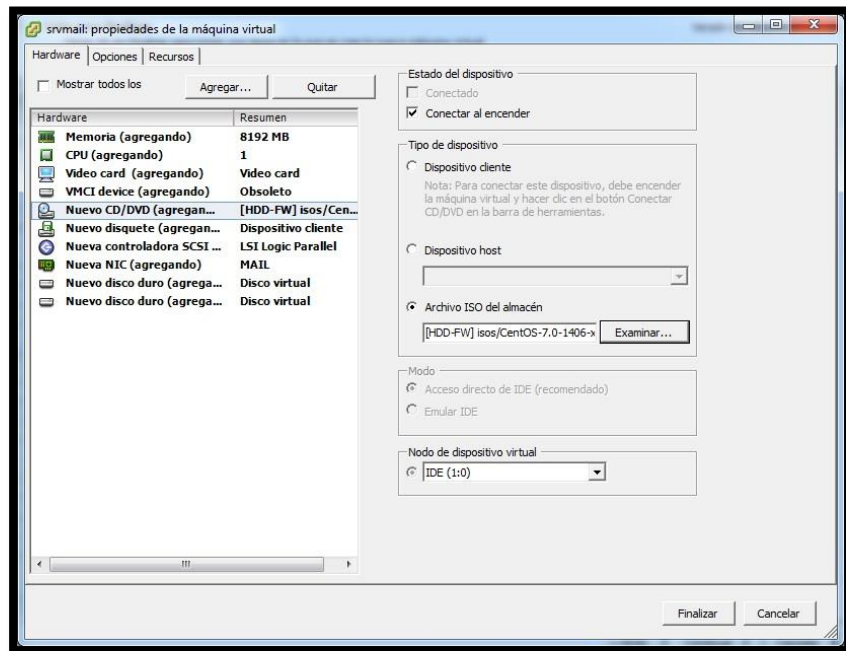


Imagen 129 – Selección del ISO CentOS 7

Se deberá esperar unos minutos hasta que se termine de crear la máquina virtual debido a los recursos que se le asignó.

11. Instalación del sistema operativo

Al igual que en el servidor anterior se deberá configurar igual la zona horaria, el idioma del teclado, el idioma de la aplicación, la interfaz de red.

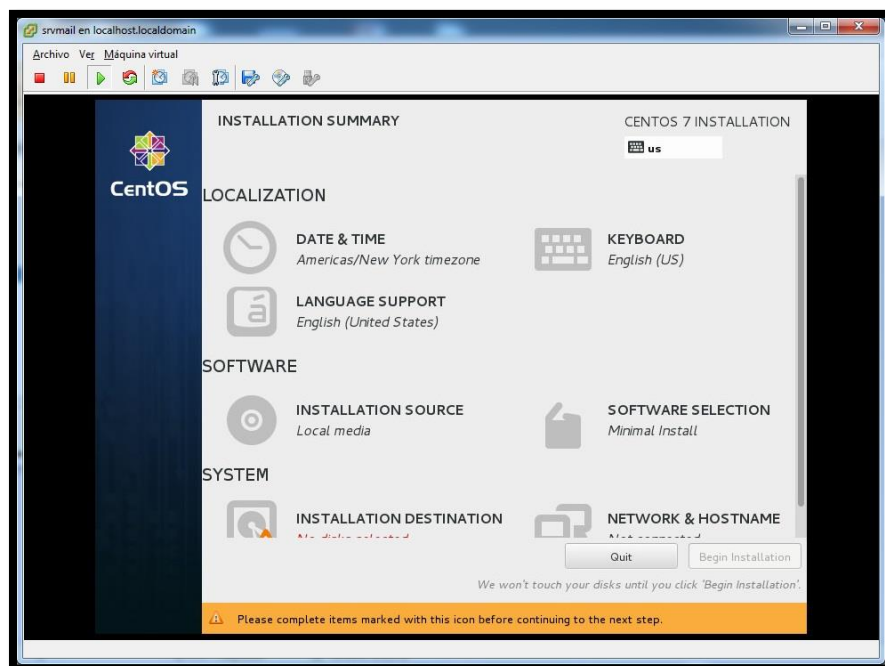


Imagen 130 – Instalación del SO

12. Para crear las particiones se debe seleccionar los dos discos.

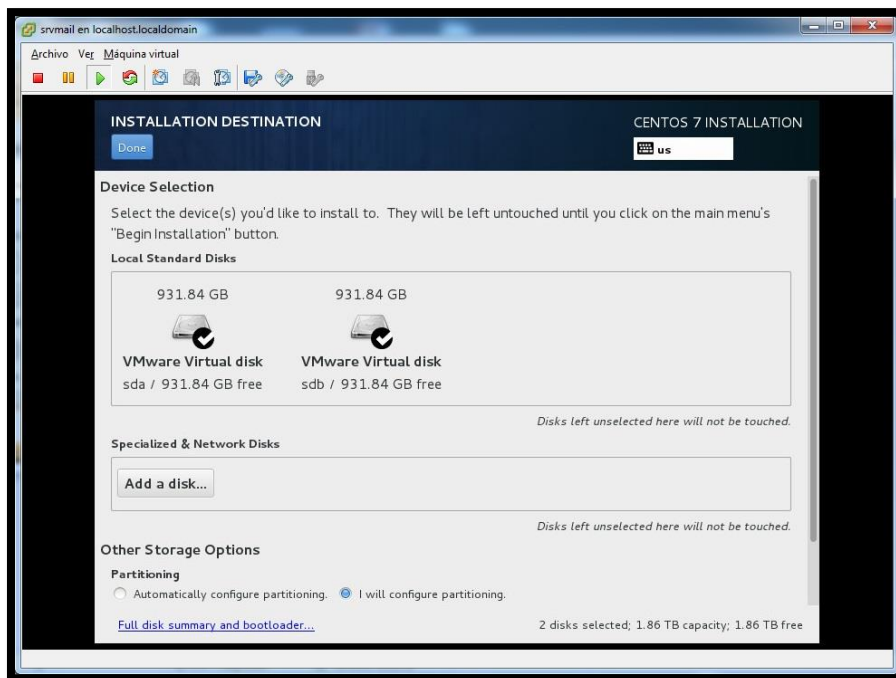


Imagen 131 – Partición de los discos

Particionar de la siguiente forma, pero teniendo en cuenta que se utilizará RAID1

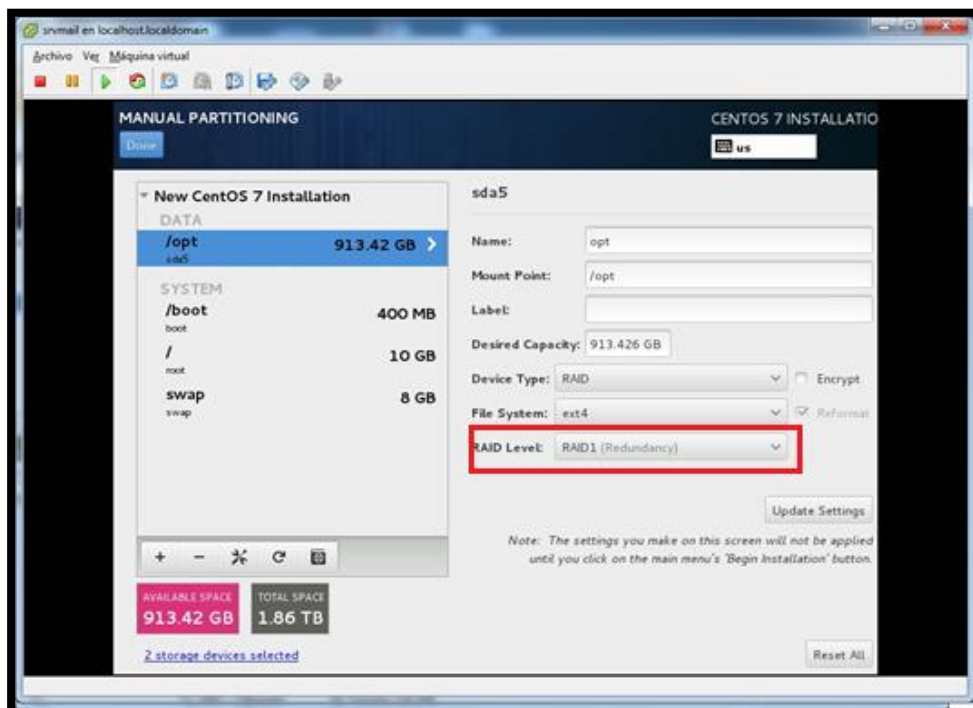


Imagen 132 – Selección del RAID1

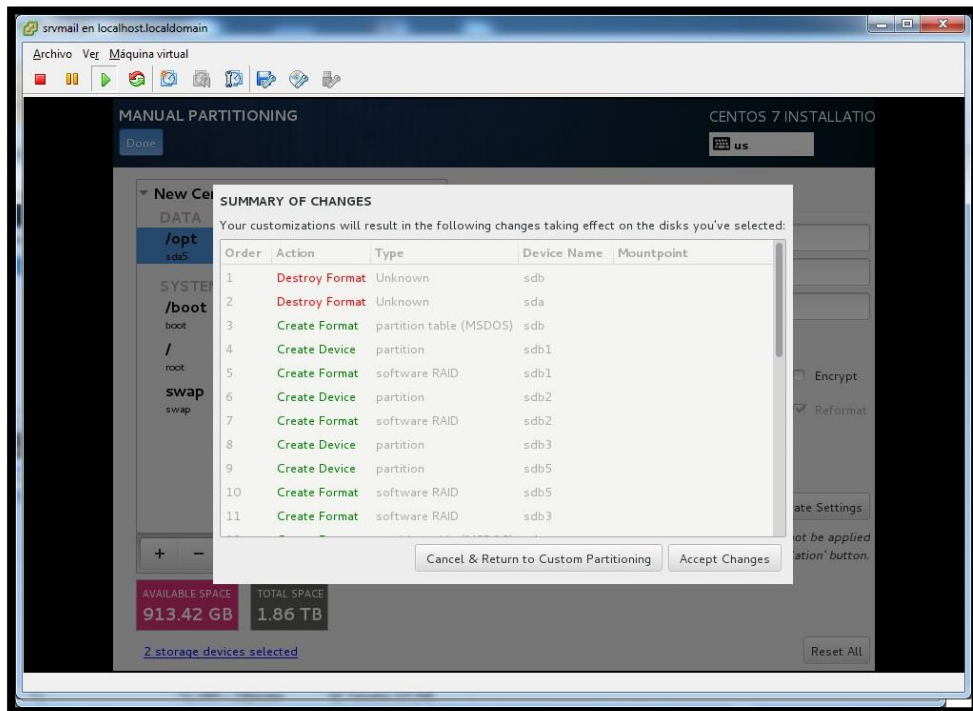


Imagen 133 – Partición del disco

13. Crear la contraseña para el root y esperar a que culmine la instalación para reiniciar el servidor.

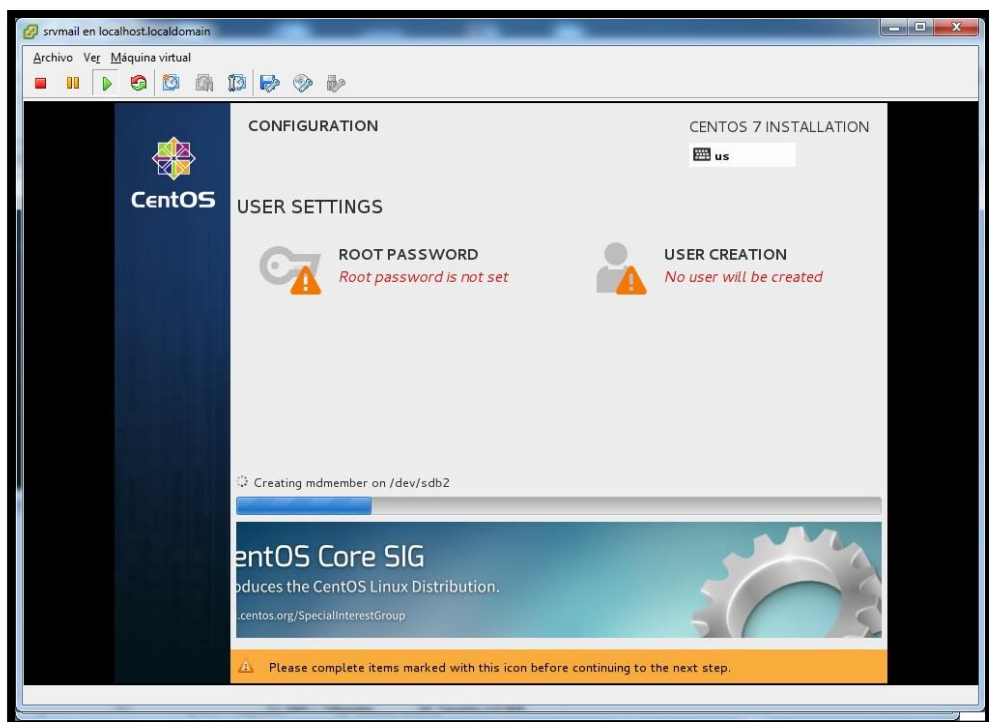


Imagen 134 – Instalación

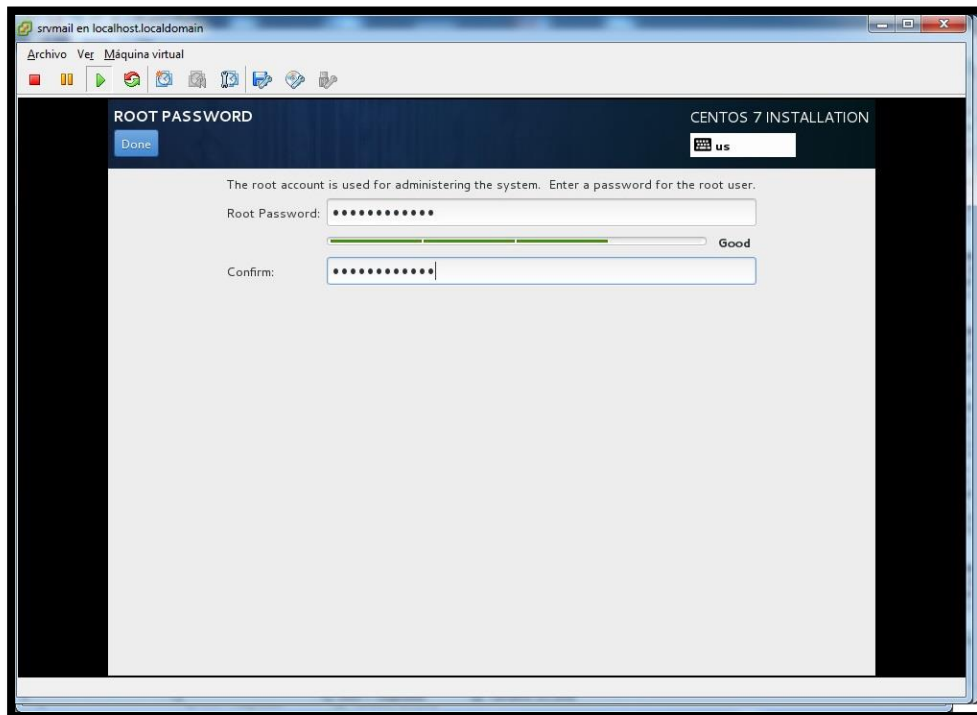


Imagen 135 – Creación de la contraseña ROOT

14. Una vez terminada la instalación configurar la interfaz de red

```
# cd /etc/sysconfig/network-script/
# vi eno16777984
```

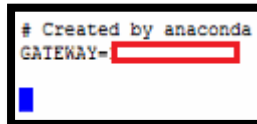
- IPV6INIT= Colocar NO para que no se inicie
- ONBOOT= Escribir yes para que arranque cada que el servidor se reinicie
- IPADDR0= La IP que se haya asignado a este servidor
- PREFIX0= El prefijo de la máscara de Subred.
- GATEWAY0= La IP del servidor firewall

```
TYPE="Ethernet"
BOOTPROTO="none"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="no"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
NAME="eno16777984"
UUID="[REDACTED]"
ONBOOT="yes"
HWADDR="[REDACTED]"
IPADDR0="[REDACTED]"
PREFIX0="24"
GATEWAY0="[REDACTED]"
DNS1="[REDACTED]"
IPV6_PEERDNS="yes"
IPV6_PEERROUTES="yes"
```

Imagen 136 – Configuración del GATEWAY

15. Modificar el archivo /etc/sysconfig/network, y agregar lo siguiente:

- GATEWAY= La IP del servidor Firewall

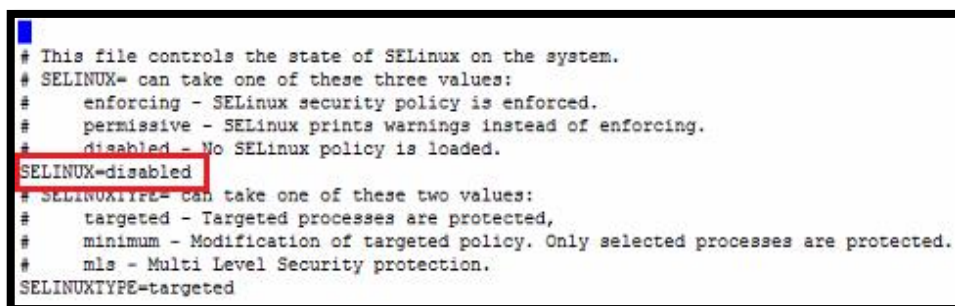


```
# Created by anaconda
GATEWAY=
```

Imagen 137 – Modificación del archivo network

16. Modificar el archivo /etc/selinux/config

- Modificar la línea selinux: SELINUX=disabled

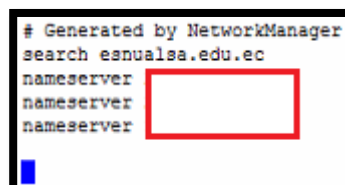


```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Imagen 138 – Configuración del archivo config

17. Configurar el archivo /etc/resolv.conf

- search esnualsa.edu.ec
- nameserver Las IP de los DNS



```
# Generated by NetworkManager
search esnualsa.edu.ec
nameserver
nameserver
nameserver
```

Imagen 139 – Configuración del archivo resolv.conf

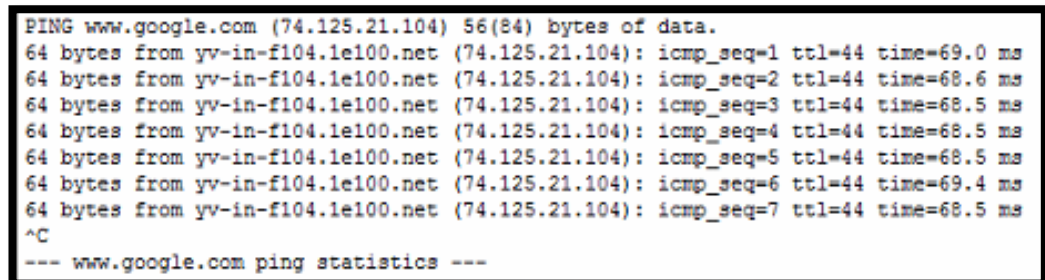
18. Al igual que en el servidor firewall **dejar solo habilitados** los siguientes servicios:

- auditd
- crond
- getty
- irqbalance
- kdump
- lv2-monitor
- microcode
- rsyslog

- sshd

19. Reiniciar el servidor.

20. Probar si hay salida a internet para proceder a instalar paquetes.

A terminal window showing the output of a ping command. The text is as follows:

```
PING www.google.com (74.125.21.104) 56(84) bytes of data:
64 bytes from yv-in-fl04.1e100.net (74.125.21.104): icmp_seq=1 ttl=44 time=69.0 ms
64 bytes from yv-in-fl04.1e100.net (74.125.21.104): icmp_seq=2 ttl=44 time=68.6 ms
64 bytes from yv-in-fl04.1e100.net (74.125.21.104): icmp_seq=3 ttl=44 time=68.5 ms
64 bytes from yv-in-fl04.1e100.net (74.125.21.104): icmp_seq=4 ttl=44 time=68.5 ms
64 bytes from yv-in-fl04.1e100.net (74.125.21.104): icmp_seq=5 ttl=44 time=68.5 ms
64 bytes from yv-in-fl04.1e100.net (74.125.21.104): icmp_seq=6 ttl=44 time=69.4 ms
64 bytes from yv-in-fl04.1e100.net (74.125.21.104): icmp_seq=7 ttl=44 time=68.5 ms
^C
--- www.google.com ping statistics ---
```

Imagen 140 – Prueba de salida a internet

21. Actualizar el sistema, con la finalidad de corregir posibles bugs, este proceso tardará unos minutos, una vez finalizado reiniciar el servidor.

```
# yum update -y
```

Configuración del DNS

22. Este servidor además de ser el de correo también cumplirá con la función de ser un servidor DNS, permitiendo resolver los nombres para la red Interna, para lo cual será necesario instalar el paquete bind.

```
# yum install bind bind-utils -y
```

23. Una vez instalado el paquete, se procederá a configurar el archivo named.conf.

```
# vi /etc/named.conf
```

Deberá quedar de la siguiente manera:

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
    listen-on port 53 { xxx.xxx.xxx.xxx; }; //ip del servidor
    //listen-on-v6 port 53 { ::1; };
    directory    "/var/named";
    dump-file     "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    version "BIND";
    forwarders {
        xxx.xxx.xxx; //DNS1 del proveedor
        xxx.xxx.xxx; //DNS2 del proveedor
    };
    forward first;

    dnssec-enable yes;
    dnssec-validation yes;
    dnssec-lookaside auto;

    bindkeys-file "/etc/named.iscdlv.key";

    managed-keys-directory "/var/named/dynamic";

    pid-file "/run/named/named.pid";
    session-keyfile "/run/named/session.key";
};

include "/etc/rndc.key";
include "/etc/named.root.key";
```



```

logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
    category lame-servers { null; };
};

controls {
    inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndc-key"; };
};

view "local" {
    match-clients {
        127.0.0.0/8;
        xxx.xxx.xxx.xxx/24; //Segmento de red LAN
    };
    allow-recursion {
        xxx.xxx.xxx.xxx/24; //Segmento de red LAN
    };
    include "/etc/named.rfc1912.zones";
    zone "." IN {
        type hint;
        file "named.ca";
    };
    zone "esnualsa.edu.ec" {
        type master;
        file "data/esnualsa-local.zone";
        allow-update { none; };
    };
    zone "xxx.xxx.xxx.in-addr.arpa" { //zona inversa LAN
        type master;
        file "data/xxx.xxx.xxx.in-addr.arpa.zone"; //archivo zona inversa LAN
        allow-update { none; };
    };
};

view "public" {
    match-clients { any; };
    recursion no;
    zone "." IN {
        type hint;
        file "named.ca";
    };
    zone "esnualsa.edu.ec" {
        type master;
        file "data/esnualsa.edu.ec.zone";
        allow-update { none; };
    };

    zone "yyy.yyy.yyy.in-addr.arpa" { //Zona Inversa WAN
        type master;
        file "data/yyy.yyy.yyy.in-addr.arpa.zone"; //archivo zona inversa WAN
        allow-update { none; };
    };
};

```

24. Se creará los archivos de las zonas en la siguiente ruta:

```
# cd /var/named/data/
```

25. Creación de la zona local

```
# vi esnualsa-local.zone
```

```

$TTL 3600
@      IN  SOA  dns.esnualsa.edu.ec.  adydel.hotmail.es. (
    20162306; serie
    1800 ; tiempo de refresco
    900 ; tiempo entre reintentos de consulta
    604800 ; tiempo tras el cual expira la zona
    3600 ; tiempo total de vida
)
@      IN  NS   dns
@      IN  MX   10  mail
@      IN  TXT  "v=spf1 a mx -all"
@      IN  A    xxx.xxx.xxx.xxx //IP del servidor local
dns    IN  A    xxx.xxx.xxx.xxx //IP del servidor local
mail   IN  A    xxx.xxx.xxx.xxx //IP del servidor local
www    IN      IN      A      www.www.www.www //IP del servidor web
srvfw  IN      IN      A      fff.fff.fff.fff //IP del servidor firewall
fw     IN      IN      CNAME  srvfw

```

26. Creación de la zona local inversa

vi xxx.xxx.xxx.in-addr.arpa.zone

```

$TTL 3600
@      IN  SOA  dns.esnualsa.edu.ec.  adydel.hotmail.es. (
    20162306; serie
    1800 ; tiempo de refresco
    900 ; tiempo entre reintentos de consulta
    604800 ; tiempo tras el cual expira la zona
    3600 ; tiempo total de vida
)
@      IN  NS   dns.esnualsa.edu.ec.
@      IN      IN      PTR      esnualsa.edu.ec.
2      IN  PTR  mail
3      IN      IN      PTR      www
1      IN  PTR  fw

```

27. Creación de la zona pública

vi esnualsa.edu.ec.zone

```

$TTL 3600
@      IN  SOA  dns.esnualsa.edu.ec.  adydel.hotmail.es. (
    20162306; serie
    1800 ; tiempo de refresco
    900 ; tiempo entre reintentos de consulta
    604800 ; tiempo tras el cual expira la zona
    3600 ; tiempo total de vida
)
@      IN  NS   dns
@      IN  MX   10  mail
@      IN  TXT  "v=spf1 a mx -all"
@      IN  A    yyy.yyy.yyy.yyy //IP proveedor internet
dns    IN  A    yyy.yyy.yyy.yyy //IP proveedor internet
mail   IN  A    yyy.yyy.yyy.yyy //IP proveedor internet
www    IN      IN      A      yyy.yyy.yyy.yyy //IP proveedor internet

```

28. Creación de la zona pública inversa

```
# vi yyy.yyy.yyy.in-addr.arpa.zone
```

```
$TTL 3600
@      IN      SOA  dns.esnualsa.edu.ec. adydel.hotmail.es. (
        20162306; serie
        1800 ; tiempo de refresco
        900 ; tiempo entre reintentos de consulta
        604800 ; tiempo tras el cual expira la zona
        3600 ; tiempo total de vida
        )
@      IN      NS   dns.esnualsa.edu.ec.
@      IN      PTR  esnualsa.edu.ec.
2      IN      PTR  mail
1      IN      PTR  fw
```

29. Habilitar e iniciar el servicio de DNS

```
# systemctl enable named
# systemctl start named
```

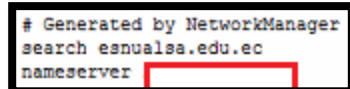
30. Configurar permisos

```
# chgrp named -R /var/named
# chown -v root:named /etc/named.conf
# restorecon -rv /var/named
# restorecon /etc/named.conf
```

31. Probar las configuraciones y la sintaxis de las zonas:

```
# named-checkconf /etc/named.conf
# named-checkzone esnualsa.edu.ec /var/named/data/esnualsa-local.zone
# named-checkzone esnualsa.edu.ec /var/named/data/esnualsa.edu.ec.zone
# named-checkzone esnualsa.edu.ec /var/named/data/ xxx.xxx.xxx.in-addr.arpa.zone
# named-checkzone esnualsa.edu.ec /var/named/data/ yyy.yyy.yyy.in-addr.arpa.zone
```

32. Editar el archivo resolv.conf y colocar la ip del servidor local y borrar las otras del proveedor de internet.



```
# Generated by NetworkManager
search esnualsa.edu.ec
nameserver [redacted]
```

Imagen 141 – Edición del archivo resolv.conf

33. Reiniciar la interfaz de red, a partir de este momento colocar en todas los equipos de la red local como DNS primario la IP del servidor de correo y comprobar que tengan salida a internet.

34. Instalación de Zimbra

Antes de proceder con la instalación se deberá verificar que se cumplan ciertos requisitos para que no aparezcan errores durante la instalación.

Verificar que no exista una instalación de postfix, en caso de existir desinstalarla.

```
# rpm -qa postfix //verificar si hay paquetes postfix
# rpm -e postfix* //eliminar cualquier versión de postfix
```

35. Verificar que estén correctamente configurados los archivos hosts y hostname.

```
# vi /etc/hosts
```

El archivo de hosts debe estar configurado de la siguiente manera:

IP_del_servidor mail.esnualsa.edu.ec

```
xxx.xxx.xxx.xxx mail.esnualsa.edu.ec
127.0.0.1      localhost localhost.localdomain localhost4 localhost4.localdomain4
::1           localhost localhost.localdomain localhost6 localhost6.localdomain6
```

Imagen 142 – Configuración del archivo hosts

```
# vi /etc/hostname
```

El archivo de hostname debe contener lo siguiente:

mail.esnualsa.edu.ec

```
mail.esnualsa.edu.ec
```

Imagen 143 – Nombre del dominio

36. Descargar la última versión disponible de Zimbra desde su sitio web <http://www.zimbra.com/>

Para este proyecto se Descargó la versión 8.7 que es la última y se encuentra estable, el paquete se llama:

zcs-8.7.0_GA_1659.RHEL7_64.20160628202714.tgz

Tiene un peso de 290MB, mediante ssh pasar el archivo a la ruta /opt/ que es donde se instalará el zimbra.

37. Descomprimir e instalar el paquete utilizando los siguientes comandos

```
# tar -xvzf zcs-8.7.0_GA_1659.RHEL7_64.20160628202714.tgz
# cd zcs-8.7.0_GA_1659.RHEL7_64.20160628202714
# ./install.sh
```

Posiblemente aparezca un error indicando que faltan ciertos paquetes de **perl** por instalar, a continuación se los instalará y tomará unos minutos.

```
# yum install perl -y
```

Ejecutar otra vez el comando de instalación, esperar a que cargue hasta que pida manualmente instalar ciertos paquetes, colocar Y a todos a excepción del zimbra-roxy para evitar problemas a futuro.

A terminal window showing the output of the Zimbra installation script. It lists found packages (zimbra-snmp, zimbra-store, zimbra-apache, zimbra-spell, zimbra-proxy) and then asks to select packages to install. For each package, it shows the installation status with a prompt in brackets and a response. zimbra-proxy is the only one with 'N' (No), while others have 'Y' (Yes). It then checks required space for zimbra-core and zimbra-store, and finally shows 'Installing: zimbra-core'.

```
Found zimbra-snmp
Found zimbra-store
Found zimbra-apache
Found zimbra-spell
Found zimbra-proxy

Select the packages to install

Install zimbra-ldap [Y] y
Install zimbra-logger [Y] y
Install zimbra-mta [Y] y
Install zimbra-snmp [Y] y
Install zimbra-store [Y] y
Install zimbra-apache [Y] y
Install zimbra-spell [Y] y
Install zimbra-proxy [N] n
Checking required space for zimbra-core
checking space for zimbra-store

Installing:
  zimbra-core
```

Imagen 144 – Instalación de paquetes de Zimbra

Cuando aparezca el mensaje de introducir el host o dominio, se deberá colocar el siguiente:

mail.esnualsa.edu.ec

Finalmente aparecerá un panel en el cual se deberá realizar unos cambios antes terminar la instalación, entre ellos asignar una contraseña al correo de administrador, y cambiar los puertos para salir por el navegador, debido a que se cuenta con solo una dirección IP estática, y solo esa fue propagada por el proveedor de dominio, se tuvo que cambiar los puertos, para http se asignó el puerto 81 y para el https se asignó el puerto 8443, es decir que para entrar a la interfaz del correo obligatoriamente deberá escribir la dirección de dominio del correo seguida de dos puntos (:) y el número de puerto en este caso 8443

```

select, or 'r' for previous menu [r] 10

Please enter the HTTP server port: [8080] 81

Store configuration

1) Status: Enabled
2) Create Admin User: yes
3) Admin user to create: admin@esnualsa.edu.ec
4) Admin Password: set
5) Anti-virus quarantine user: virus-quarantine.aamjmhmf@esnualsa.edu.ec
6) Enable automated spam training: yes
7) Spam training user: spam.3uag7jzb4c@esnualsa.edu.ec
8) Non-spam(Ham) training user: ham.ip337x9qze@esnualsa.edu.ec
9) SMTP host: mail.esnualsa.edu.ec
10) Web server HTTP port: 81
11) Web server HTTPS port: 8443
12) HTTP proxy port: 80
13) HTTPS proxy port: 443
14) Web server mode: https
15) IMAP server port: 7143
16) IMAP server SSL port: 7993
17) IMAP proxy port: 143
18) IMAP SSL proxy port: 993
19) POP server port: 7110
20) POP server SSL port: 7995
21) POP proxy port: 110
22) POP SSL proxy port: 995
23) Use spell check server: yes
24) Spell server URL: http://mail.esnualsa.edu.ec:7780/aspell.php
25) Configure for use with mail proxy: TRUE
26) Configure for use with web proxy: TRUE
27) Enable version update checks: TRUE
28) Enable version update notifications: TRUE
29) Version update notification email: admin@esnualsa.edu.ec
30) Version update source email: admin@esnualsa.edu.ec
31) Install mailstore (service webapp): yes
32) Install UI (zimbra,zimbraAdmin webapps): yes

select, or 'r' for previous menu [r] 

```

Imagen 145 – Configuración del Zimbra

38. Una vez terminada la instalación ingresar desde cualquier navegador la siguiente dirección para comprobar:

<https://mail.esnualsa.edu.ec:8443/>

Se ingresó desde los 3 navegadores conocidos, chrome, Firefox e internet explorer, para mostrar que aparece un mensaje, este indica que es una dirección https, pero no posee un certificado de seguridad, para obtener esto se debe cancelar un valor, pero en este proyecto simplemente se saltará esa opción.

Visto desde Google Chrome.

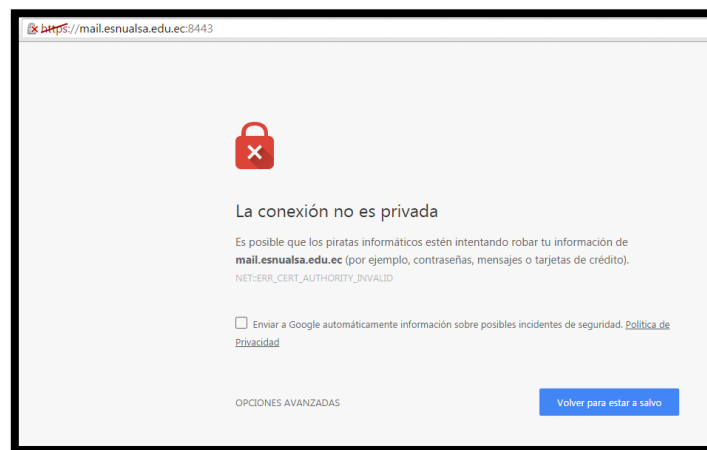


Imagen 146 – Correo desde google chrome

Visto desde Firefox.

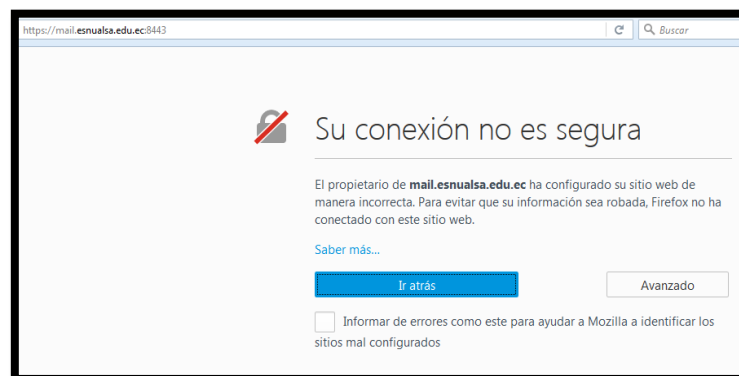


Imagen 147 – Correo desde firefox

Visto desde internet Explorer

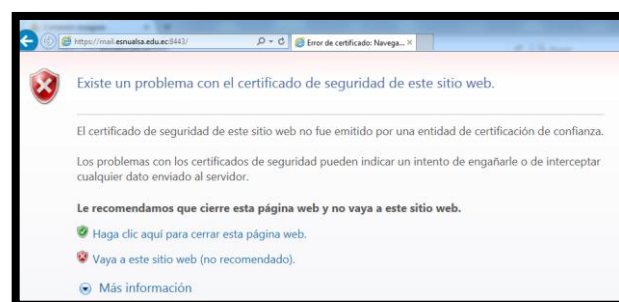


Imagen 148 – Correo desde internet explorer

39. Vista de la página de entrada de zimbra

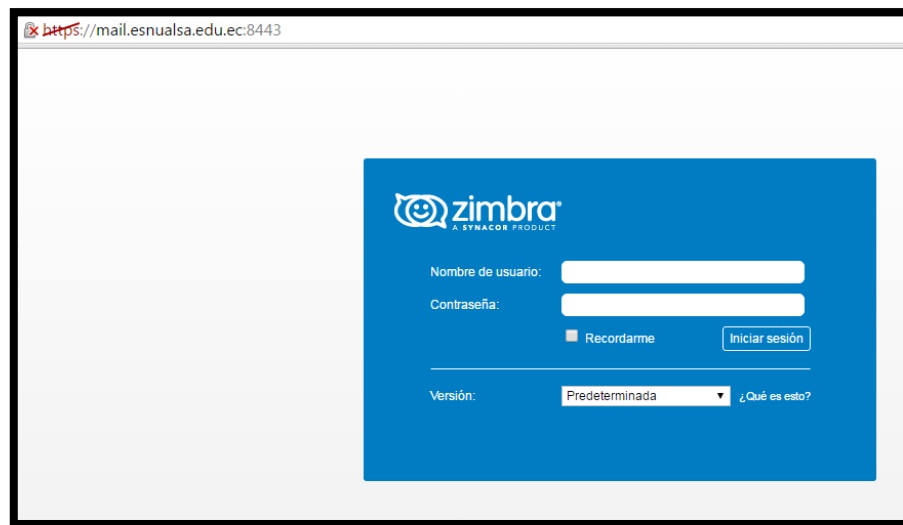


Imagen 149 – Ventana principal de Zimbra

40. Creación de Cuentas

Para entrar al Zimbra Administration, colocar la siguiente ruta desde el navegador:

<https://mail.esnualsa.edu.ec/7071>

A continuación loguearse con las credenciales de administrador y aparecerá el panel

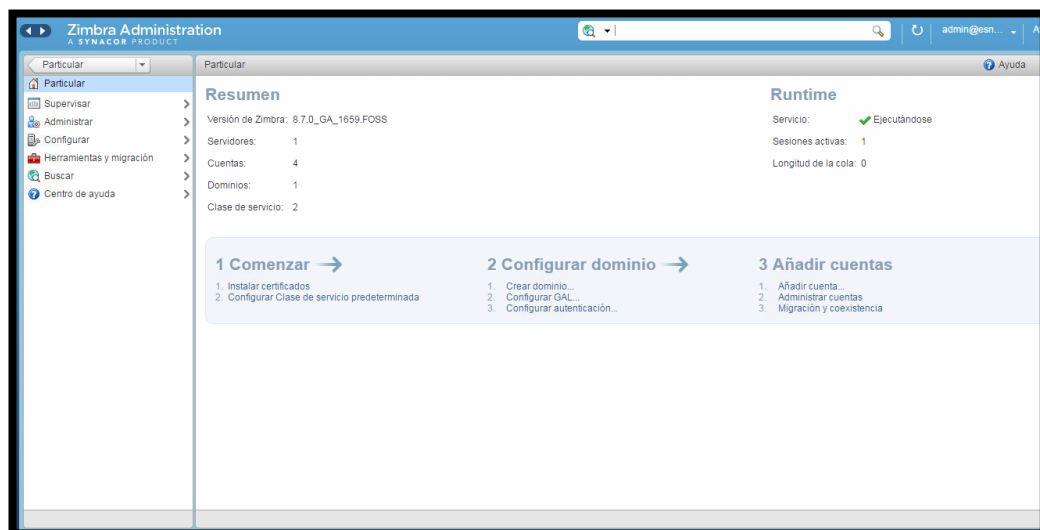


Imagen 150 – Ventana de Zimbra Administration

41. Seleccionar la opción **Administrar** que se encuentra en el panel de la izquierda, y a continuación presionar el botón que tiene forma de engrane

ubicado en la parte superior derecha, ahí se elegirá **Nuevo** para crear una nueva cuenta.

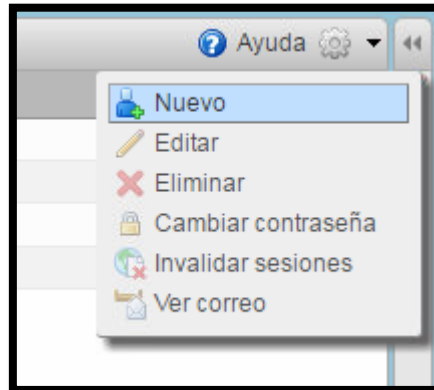


Imagen 151 – Creación nueva cuenta de correo

42. Se abrirá una nueva ventana en la cual se llenará los campos con asterisco (*) de forma obligatoria y los demás son opcionales.

7

Imagen 152 – Datos a llenar de la nueva cuenta

43. De esta manera se irán almacenando los correos que se vayan creando.

| | | | | |
|--|-----------------------------------|-------------------|--------|---------------------------|
| | johanna.hernandez@esnualsa.edu.ec | Johanna Hernández | Activo | 21 de Agosto 2016 2:21:21 |
| | sistemas@esnualsa.edu.ec | Andres Del Pozo | Activo | 21 de Agosto 2016 2:19:55 |

Imagen 153 – Cuentas creadas

Creación del Servidor Web

Antes de crear la virtual se deberá definir sus recursos físicos, estos se detallan a continuación:

- 1 HDD 30GB
- 2 GB RAM
- 1 Interfaz de red

Para crear la máquina virtual, se debe realizar el mismo procedimiento que con las dos máquinas anteriores escogiendo los recursos ya mencionados. El nombre de esta máquina virtual será srweb.

1. Instalación de la máquina virtual

Teniendo el conocimiento previo de la instalación de los servidores, se empezará este manual desde el particionamiento ya que los otros pasos son iguales.

Las particiones deberán ser las siguientes:

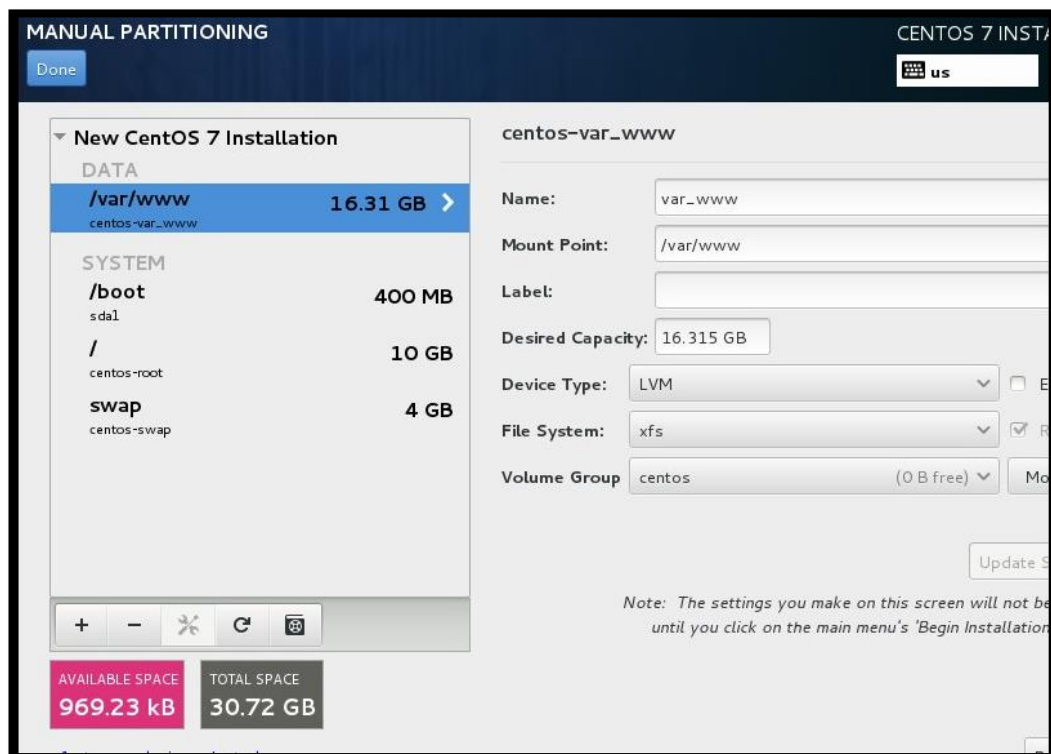


Imagen 154 – Particiones del servidor web

Se deberá crear el directorio /var/www en donde se alojará el sitio web.

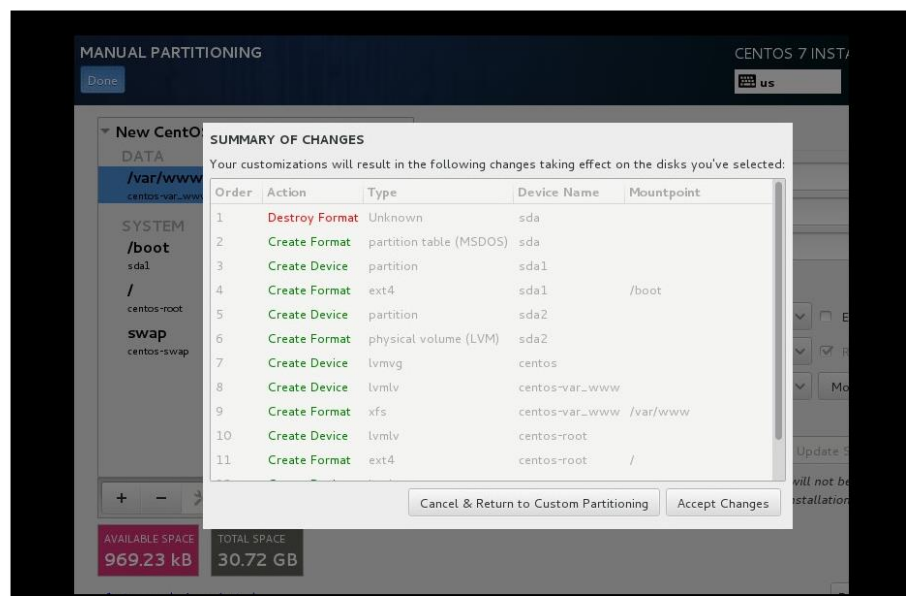


Imagen 155 – Resumen del particionamiento

2. No olvidar colocar una contraseña robusta para el root, y esperar a que se reinicie el servidor.
3. Una vez terminada la instalación configurar la interfaz de red

```
# cd /etc/sysconfig/network-script/
# vi eno16777984
```

- IPV6INIT= Colocar NO para que no se inicie
- ONBOOT= Escribir yes para que arranque cada que el servidor se reinicie
- IPADDR0= La IP que se haya asignado a este servidor
- PREFIX0= El prefijo de la máscara de Subred.
- GATEWAY0= La IP del Servidor firewall
- DNS1= La IP del Servidor de Correo

```
TYPE="Ethernet"
BOOTPROTO="none"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="no"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
NAME="eno16777984"
UUID="XXXXXXXXXXXXXXXXXXXX"
ONBOOT="yes"
HWADDR="08:00:27:00:12:34"
IPADDR0="192.168.1.100"
PREFIX0="24"
GATEWAY0="192.168.1.1"
DNS1="192.168.1.1"
IPV6_PEERDNS="yes"
IPV6_PEERROUTES="yes"
```

Imagen 156 – Contenido interfaz de red

4. Modificar el archivo /etc/sysconfig/network, y agregar lo siguiente:

- GATEWAY= La IP del servidor Firewall

```
# Created by anaconda
GATEWAY=
```

Imagen 157 – Contenido archivo network

5. Modificar el archivo /etc/selinux/config

- Modificar la línea selinux: SELINUX=disabled

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Imagen 158 – Contenido archivo selinux

6. Configurar el archivo /etc/resolv.conf

- search esnualsa.edu.ec
- nameserver Las IP del servidor de Correo

```
# Generated by NetworkManager
search esnualsa.edu.ec
nameserver
```

Imagen 159 – Contenido archivo resolv.conf

7. Al igual que en los servidores anteriores **dejar solo habilitados** los siguientes servicios:

- auditd
- crond
- getty
- irqbalance
- kdump
- lv2-monitor
- microcode
- rsyslog
- sshd

8. Reiniciar el servidor.

9. Probar si hay salida a internet para proceder a instalar paquetes.

```
PING www.google.com (74.125.21.104) 56(84) bytes of data.  
64 bytes from yv-in-f104.1e100.net (74.125.21.104): icmp_seq=1 ttl=44 time=69.0 ms  
64 bytes from yv-in-f104.1e100.net (74.125.21.104): icmp_seq=2 ttl=44 time=68.6 ms  
64 bytes from yv-in-f104.1e100.net (74.125.21.104): icmp_seq=3 ttl=44 time=68.5 ms  
64 bytes from yv-in-f104.1e100.net (74.125.21.104): icmp_seq=4 ttl=44 time=68.5 ms  
64 bytes from yv-in-f104.1e100.net (74.125.21.104): icmp_seq=5 ttl=44 time=68.5 ms  
64 bytes from yv-in-f104.1e100.net (74.125.21.104): icmp_seq=6 ttl=44 time=69.4 ms  
64 bytes from yv-in-f104.1e100.net (74.125.21.104): icmp_seq=7 ttl=44 time=68.5 ms  
^C  
--- www.google.com ping statistics ---
```

Imagen 160 – Ping a google

10. Actualizar el sistema, con la finalidad de corregir posibles bugs, este proceso tardará unos minutos, una vez finalizado reiniciar el servidor.

```
# yum update -y
```

11. **Instalación del paquete para el servidor web.**

Mediante el siguiente comando se debe instalar el paquete httpd.

```
# yum install httpd -y
```

12. Una vez instalado habilitarlo e iniciarlo

```
# systemctl start httpd  
# systemctl enable httpd
```

13. Verificar ingresando al dominio que aparezca la página de prueba del Apache

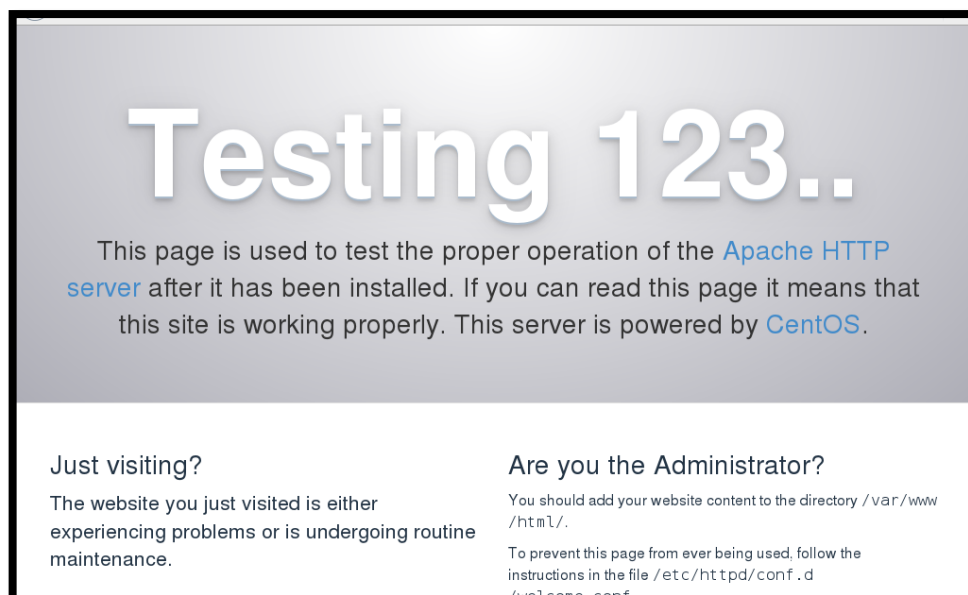


Imagen 161 – Página de prueba de Apache

14. Configurar el archivo httpd.conf

```
# cd /etc/httpd/conf/  
# vi httpd.conf
```

Dentro del archivo se deberá modificar las siguientes líneas, para numerar las líneas del archivo escribir **dos puntos set number (:set number)** y presionar enter.

- En la línea 41 el ejemplo dice **Listen 12.34.56.78:80**, en su lugar ubicar **Listen 80**
- En la línea 95 el ejemplo dice **ServerName www.example.com:80**, en su lugar irá **ServerName www.esnualsa.edu.ec:80**.
- En la línea 152 dice **AllowOverride None** reemplazar por **AllowOverride All**

15. Instalación de la Base de Datos

Normalmente se instala el paquete de Mysql, pero en esta versión ya de CentOS ya no existen repositorios para eso, en su reemplazo está MariaDB. Con el siguiente comando se instalará MariaDB.

```
# yum install mariadb-server mariadb -y
```

16. A continuación habilitar e iniciar el servicio.

```
# systemctl start mariadb  
# systemctl enable mariadb
```

17. Una vez corriendo el servicio se deberá crear la contraseña para el root de la base de datos con el siguiente comando

```
# mysql_secure_installation
```

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB  
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!  
  
In order to log into MariaDB to secure it, we'll need the current  
password for the root user. If you've just installed MariaDB, and  
you haven't set the root password yet, the password will be blank,  
so you should just press enter here.  
  
Enter current password for root (enter for none): █
```

Imagen 162 – Crear la contraseña para la Base de Datos

```

you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n]

```

Imagen 163 – Ingreso de contraseña para la Base de Datos

A continuación presionar “Y” a todas las opciones hasta que finalice la configuración.

```

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!

```

Imagen 164 – Configuración de MariaDB

18. Instalación de phpmyadmin

Se instalará este paquete para que si en algún futuro se necesita modificar algo en la base de datos, lo hagan mediante entorno gráfico si no se tiene conocimientos de comandos para hacerlo bajo consola.

Se empezará instalando PHP y varios de sus componentes con el siguiente comando.

```
# yum -y install php php-mysql php-gd php-ldap php-odbc php-pear
php-xml php-xmlrpc php-mbstring php-snmp php-soap curl
```

Ahora se procederá a instalar phpmyadmin con los siguientes comandos

```
# yum install epel-release -y  
# yum install phpmyadmin -y
```

Una vez realizado estas instalaciones reiniciar el servicio httpd, acceder desde un navegador a: ip_del_servidor/phpMyAdmin, y deberá aparecer la interfaz gráfica.



Imagen 165 – Ventana principal de phpMyAdmin

19. Instalación de WordPress

Descargar de la página oficial la última versión del paquete y ubicarla dentro de la carpeta /root, en este caso la última versión disponible es la 4.6, una vez dentro descomprimir el paquete.

```
[root@srvweb ~]# ll  
total 8908  
-rw-----, 1 root root    1314 Aug 20 08:23 anaconda-ks.cfg  
drwxr-xr-x, 5 root root    4096 Aug 17 08:20 wordpress  
-rw-r--r--, 1 root root 9111675 Aug 20 11:31 wordpress-4.6-es_3S.zip  
[root@srvweb ~]#
```

Imagen 166 – Descomprimir Wordpress


```
[root@srvweb ~]# cd wordpress
[root@srvweb wordpress]# ll
total 204
-rw-r--r--. 1 root root 418 Sep 24 2013 index.php
-rw-r--r--. 1 root root 17935 Aug 17 08:20 licencia.txt
-rw-r--r--. 1 root root 19935 Aug 17 08:19 license.txt
-rw-r--r--. 1 root root 7636 Aug 17 08:20 readme.html
-rw-r--r--. 1 root root 5456 May 24 16:02 wp-activate.php
drwxr-xr-x. 9 root root 4096 Aug 17 07:30 wp-admin
-rw-r--r--. 1 root root 364 Dec 19 2015 wp-blog-header.php
-rw-r--r--. 1 root root 1477 May 23 11:44 wp-comments-post.php
-rw-r--r--. 1 root root 3237 Aug 17 08:20 wp-config-sample.php
drwxr-xr-x. 5 root root 4096 Aug 17 08:20 wp-content
-rw-r--r--. 1 root root 3286 May 24 2015 wp-cron.php
drwxr-xr-x. 17 root root 12288 Aug 17 08:19 wp-includes
-rw-r--r--. 1 root root 2382 May 23 11:44 wp-links-opml.php
-rw-r--r--. 1 root root 3353 Apr 14 12:53 wp-load.php
-rw-r--r--. 1 root root 34057 Jun 14 16:51 wp-login.php
-rw-r--r--. 1 root root 7786 Jul 13 07:37 wp-mail.php
-rw-r--r--. 1 root root 13920 Aug 13 11:02 wp-settings.php
-rw-r--r--. 1 root root 29890 May 24 15:44 wp-signup.php
-rw-r--r--. 1 root root 4035 Nov 30 2014 wp-trackback.php
-rw-r--r--. 1 root root 3064 Jul 6 07:40 xmlrpc.php
[root@srvweb wordpress]#
```

Imagen 167 – Contenido de la carpeta Wordpress

20. Mover todo el contenido de la carpeta wordpress a la ruta donde se alojará el sitio web y se procederá con la instalación.

```
# mv * /var/www/html/
```

21. Para empezar la instalación de wordpress se debe dirigir a cualquier navegador y digitar el nombre de dominio, por experiencia se recomienda realizar la instalación desde una computadora remota que no tenga nada que ver con la red interna, se tuvo problemas cuando se lo instaló desde la LAN ya que cuando se abría el sitio web desde un lugar remoto, este no cargaba bien y las páginas no apuntaban hacia el dominio sino a la IP del servidor por lo que inmediatamente saltaba el proxy.
- La primera ventana que saldrá será la de bienvenida en donde explica lo necesario para la instalación.



Bienvenido a WordPress. Antes de empezar necesitamos alguna información de la base de datos. Necesitarás saber lo siguiente antes de continuar.

1. Nombre de la base de datos
2. Usuario de la base de datos
3. Contraseña de la base de datos
4. Servidor de la base de datos
5. Prefijo de la tabla (si quieres ejecutar más de un WordPress en una sola base de datos)

Vamos a usar esta información para crear un archivo `wp-config.php`. Si por alguna razón no funciona la creación automática de este archivo no te preocupes. Lo que hace es incluir en un archivo de configuración la información de la base de datos. También puedes simplemente abrir `wp-config-sample.php` en un editor de texto, rellenarlo con tu información y guardarlo como `wp-config.php`. ¿Necesitas más ayuda? [La tenemos](#).

Con toda seguridad, estos elementos te fueron suministrados por tu proveedor de hosting. Si no tienes esta información, necesitas contactar con ellos antes de continuar. Si estás listo...

Imagen 168 – Ventana principal de Wordpress

22. Llenar los campos que se solicita a continuación



A continuación deberás introducir los detalles de conexión a tu base de datos. Si no estás seguro de esta información contacta con tu proveedor de alojamiento web.

| | | |
|------------------------------|--|---|
| Nombre de la base de datos | <input type="text" value="wordpress"/> | El nombre de la base de datos que quieres usar con WordPress. |
| Nombre de usuario | <input type="text" value="nombre_de_usuario"/> | El nombre de usuario de tu base de datos. |
| Contraseña | <input type="text" value="contraseña"/> | La contraseña de tu base de datos. |
| Servidor de la base de datos | <input type="text" value="localhost"/> | Deberías recibir esta información de tu proveedor de alojamiento web, si localhost no funciona. |
| Prefijo de tabla | <input type="text" value="wp_"/> | Si quieres ejecutar varias instalaciones de WordPress en una sola base de datos cambia esto. |

Imagen 169 – Información de la Base de Datos

23. Bajo consola se deberá crear el archivo wp-config.php y se pegará el contenido que aparece en la siguiente ventana

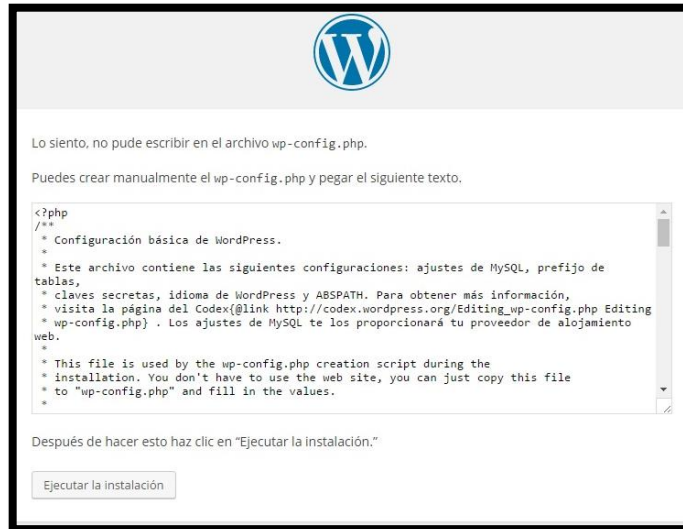


Imagen 170 – Ventana principal de Wordpress

24. Llenar la siguiente información y presionar instalar WordPress

This screenshot shows the "Información necesaria" (Necessary Information) section of the WordPress installation screen. At the top is the WordPress logo. Below it, a greeting "Hola" is followed by a welcome message: "¡Bienvenido al famoso proceso de instalación de WordPress en cinco minutos! Simplemente completa la información siguiente y estarás a punto de usar la más enriquecedora y potente plataforma de publicación personal del mundo." The section is titled "Información necesaria". Below the title, a message says "Por favor, debes facilitarnos los siguientes datos. No te preocupes, siempre podrás cambiar estos ajustes más tarde." There are four input fields: "Título del sitio", "Nombre de usuario", "Contraseña", and "Tu correo electrónico". The "Contraseña" field has a strength indicator showing "Fuerte" (Strong) and an "Ocultar" (Hide) button. Below the "Contraseña" field, a message says "Importante: Necesitas esta contraseña para acceder. Por favor, guárdala en un lugar seguro." Below the "Tu correo electrónico" field, a message says "Comprueba bien tu dirección de correo electrónico antes de continuar." There is a "Privacidad" section with a checked checkbox for "Permitir a los buscadores que indexen el sitio". At the bottom is a button labeled "Instalar WordPress".

Imagen 171 – Llenar información necesaria

25. Una vez culminada la instalación se accederá al panel de administración de WordPress



Imagen 172 – Mensaje final de la instalación



Imagen 173 – Ventana de Login

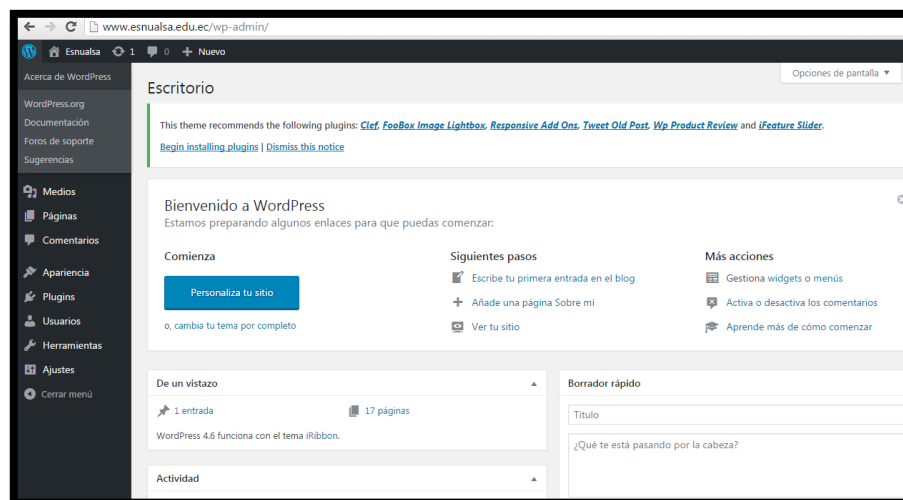


Imagen 174 – Ventana de administración de Wordpress

MANUAL TÉCNICO

SISTEMA CCTV

ESPECIFICACIONES TÉCNICAS

El sistema de CCTV está compuesto por varios elementos descritos a continuación:

- **DVR Samsung SDR-C5300**
 - ✓ 2TB de disco duro
 - ✓ 16 canales
 - ✓ Soporta hasta 1080p
 - ✓ Conectividad BNC



Imagen 175 – DVR

- **Control Remoto**
 - ✓ Permite manejar las opciones del DVR.



Imagen 176 – Control Remoto

- **11 Cámaras Color Bullet**
 - ✓ Cámaras que ya se encontraban instaladas en la Institución, no tienen infrarrojo para visualizar durante la noche.



Imagen 177 – Cámaras tipo tubo instaladas

- **1 Cámara tipo domo**
 - ✓ Esta cámara ya se encontraba instalada, es la primera en perder visibilidad cuando oscurece.



Imagen 178 – Cámara tipo domo instalada

- **2 Cámaras Hikvision tipo tubo para exteriores**

- ✓ Se adquirió 2 cámaras nuevas para ser ubicadas, una apuntando hacia la puerta principal y la otra hacia un pasillo que conduce al baño de varones.



Imagen 179 – Cámara nueva tipo tubo

- **1 Cámara Hikvision tipo domo para interior**

- ✓ Se adquirió una cámara tipo domo para el laboratorio de computación.



Imagen 180 – Cámara nueva tipo domo

- **Conectores balun**

- ✓ Se utilizaron 30 conectores de video, 15 conectores de poder macho y 15 conectores de poder hembra.



Imagen 181 – Conectores Balun

- **Cable UTP categoría 6 NEXXT**
 - ✓ Se utilizó este rollo de cable para conectar las cámaras con el DVR.



Imagen 182 – Rollo de cable UTP

INSTALACIÓN Y CONFIGURACIÓN DEL DVR

Antes de empezar, se debe hacer una revisión de los componentes que vinieron con el equipo, los cuales son:

- 1 mouse.
- 1 cargador.
- 1 cable hdmi.
- 1 cable de red.
- 1 control remoto y 2 pilas.
- 2 splitter



Imagen 183 – Componentes

Instalación de cámaras al DVR

Luego de haber realizado todo el cableado hacia los distintos puntos y de haber instalado las cámaras, realizar lo siguiente:

1. Ponchar los cables con los conectores balun con el siguiente estándar, para los conectores de video se utilizó 2 pares de cable naranja (+) y verde (-), mientras que para voltaje se usó los 2 pares restantes, azul (+) y café (-)

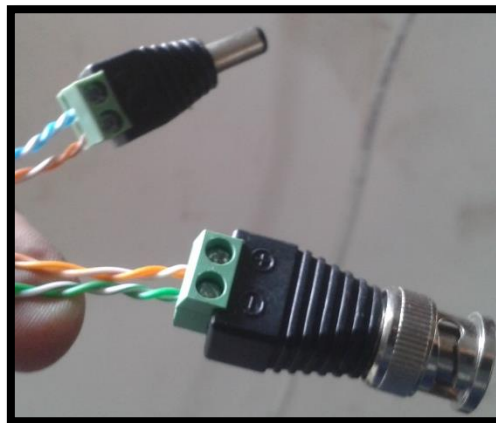


Imagen 184 – Conectores ponchados

2. Una vez ponchado de ambos extremos los cables, conectar los demás elementos como en el gráfico que está a continuación.

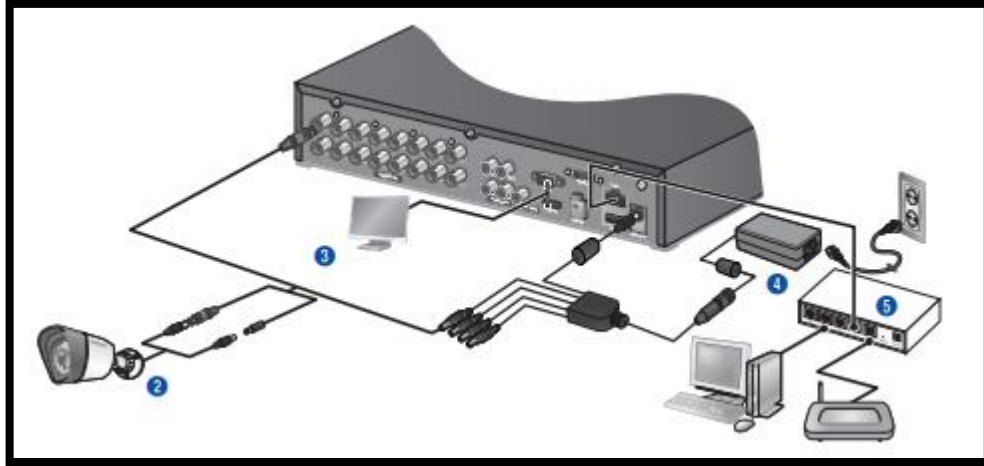


Imagen 185 – Conexión de dispositivos

- **Paso 1:** Conectar el mouse en la parte frontal. (en este caso se usará el control remoto).
 - **Paso 2:** Conectar un extremo de los cables ponchados a las cámaras mientras que el otro hacia el DVR.
 - **Paso 3:** Conectar un monitor en el puerto VGA del DVR.
 - **Paso 4:** Conectar los conectores de poder a los splitter y estos a su vez al DVR y al cargador.
 - **Paso 5:** conectar el DVR a la red
3. Una vez realizado los pasos anteriores, conectar el DVR a la corriente y esperar unos minutos a que se encienda.



Imagen 186 – DVR encendiendo

4. Cuando se haya encendido el DVR, se debe proceder a mover las cámaras para visualizar en una posición determinada

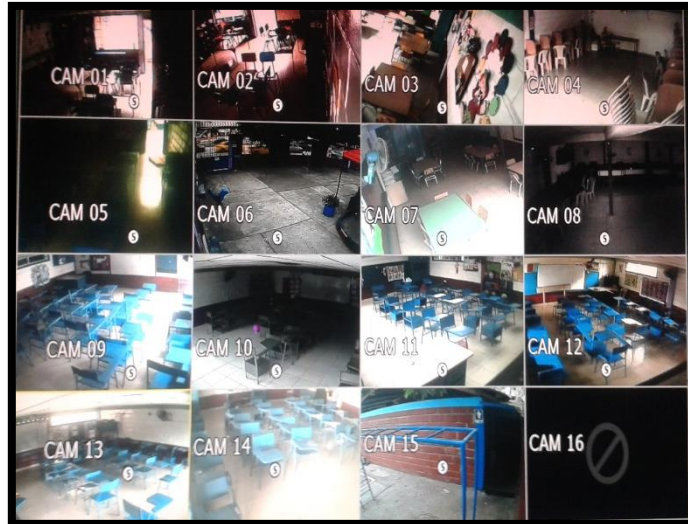


Imagen 187 – Visualización de cámaras de Esnualsa

Configuración del DVR

Se procederá a realizar ciertas configuraciones necesarias para un mejor uso del DVR.

1. **Contraseña de Administrador y creación de usuarios**

Se debe presionar el botón **menú** del control remoto y aparecerá una ventana de login, al ser el equipo nuevo simplemente seleccionar la opción aceptar ya que no tiene contraseña.

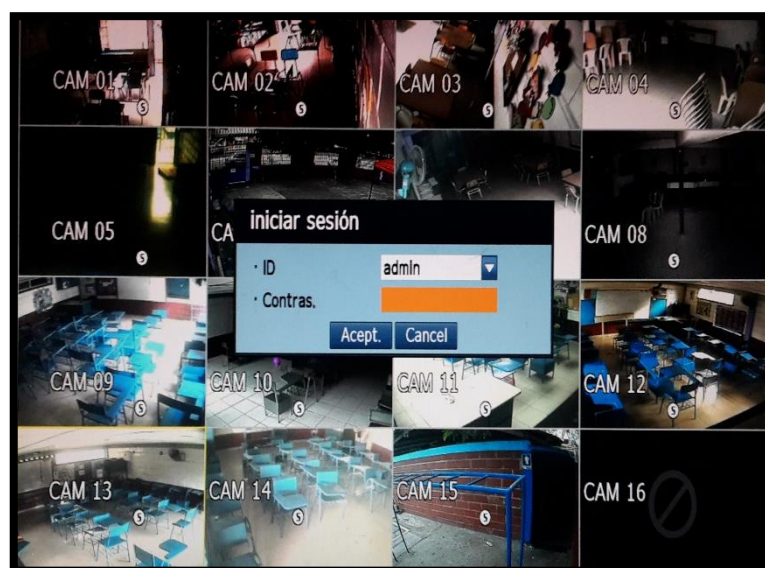


Imagen 188 – Inicio de sesión del DVR

2. Una vez dentro ir a la opción **Gestión de Permisos**, ahí se abrirá una nueva ventana en donde se podrá crear una nueva contraseña para el administrador y además de crear usuarios y grupos para visualización. Ya dentro de la opción mencionada, en la pestaña de **Admin** se escribirá la contraseña adecuada y presionar el botón aceptar.

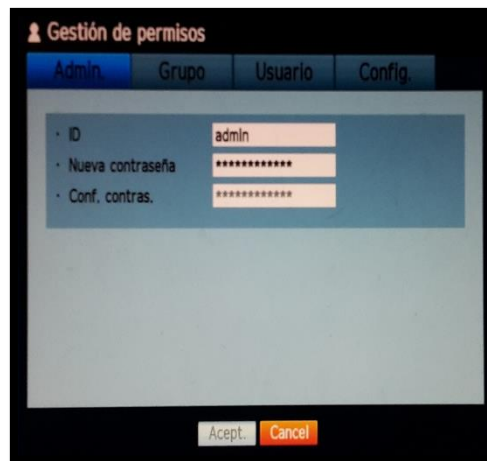


Imagen 189 – Contraseña de Administrador

3. Dentro de la misma ventana, se creará el grupo **Visualizar** en donde se ubicarán usuarios con permisos para visualizar y buscar videos, además de que se creará el usuario **Monitoreo**.

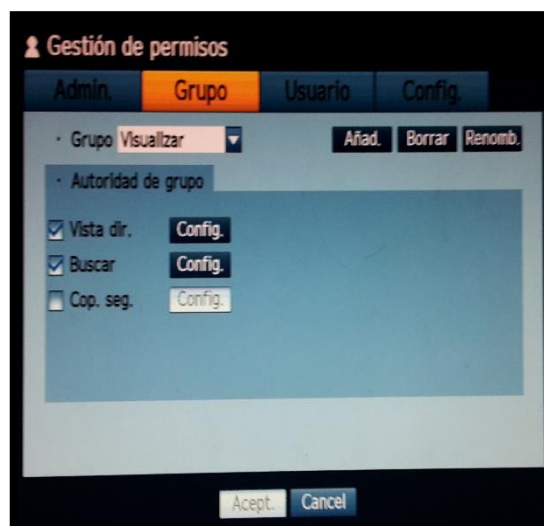


Imagen 190 – Creación del grupo

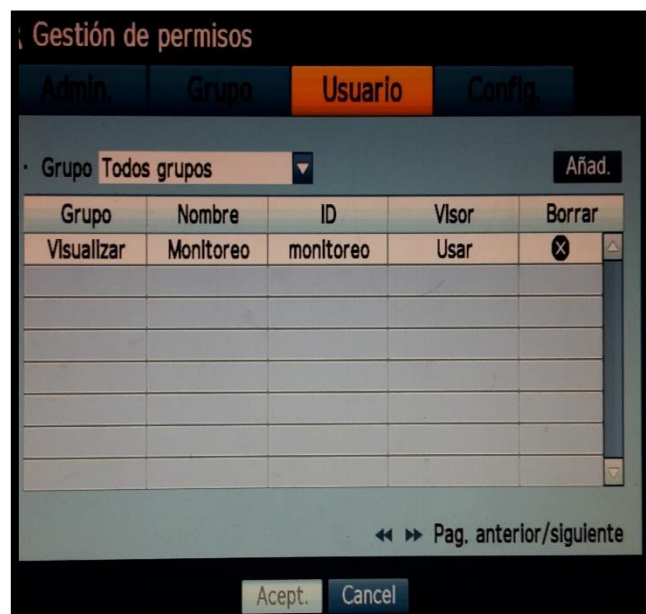


Imagen 191 – Creación del usuario

Para salir y guardar los cambios presionar el botón aceptar, aparecerá un mensaje que solicitará se reinicie el equipo.

4. Configuración de la fecha, hora e idioma

Ingresa al menú y entra en la primera opción de Fecha/Hora/Idioma, ahí aparecerá la siguiente ventana en la cual se deberá llenar la información que solicita.

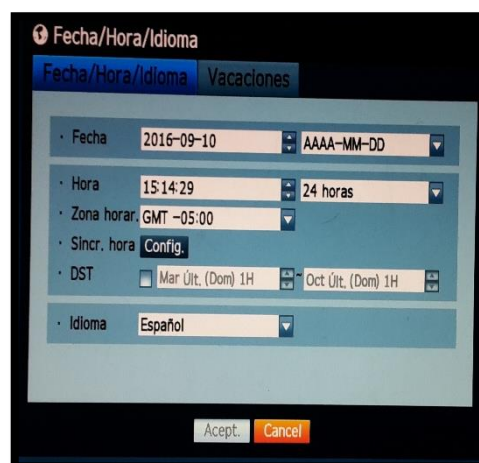


Imagen 192 – Configuración de fecha, hora e idioma

5. Configuración de la red

Dentro del menú principal ir hacia la opción **Red** y seleccionar la primera opción **Modo de conexión**, una vez dentro configurar la pestaña **Interfaz** con la dirección IP asignada para el DVR y la pestaña **Puerto**, con los siguientes:

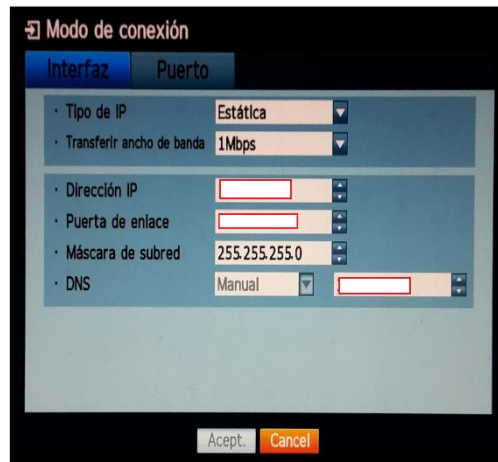


Imagen 193 – Configuración de Interfaz

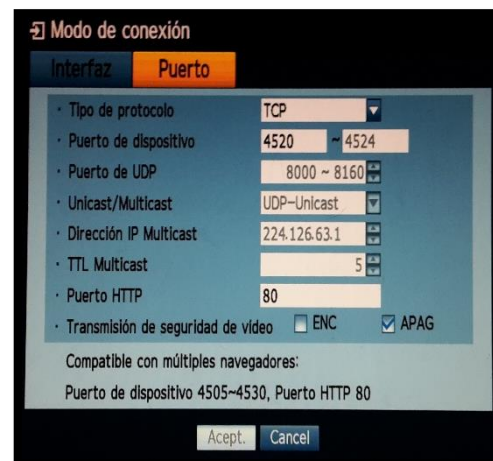


Imagen 194 – Configuración de Puerto

Una vez realizadas estas configuraciones, se podrá visualizar las cámaras desde cualquier computadora que esté conectada a la red mediante un software o simplemente desde internet explorer.

6. Políticas de grabación

Debido al tamaño del disco duro que posee este equipo, es necesario crear unas políticas de grabación para prolongar más el tiempo de respaldo ya que adicional se realizará una configuración para que una vez llegado al límite se proceda a sobrescribir la información, dejando así un determinado tiempo de respaldo, ya será responsabilidad del usuario encargado realizar los backups en discos externos en cuanto se produzca cualquier eventualidad.

En el menú principal ir hacia la opción **Grabación**, una vez dentro seleccionar **Programar grabación**, se abrirá una nueva ventana en donde aparecerá una cuadrícula, en la parte superior están las horas y en la parte izquierda están los días de la semana, en la parte inferior se encuentran unos cuadros de colores con la respectiva especificación para grabar, por defecto trae todos los cuadros de color naranja que significa que grabará continuamente.

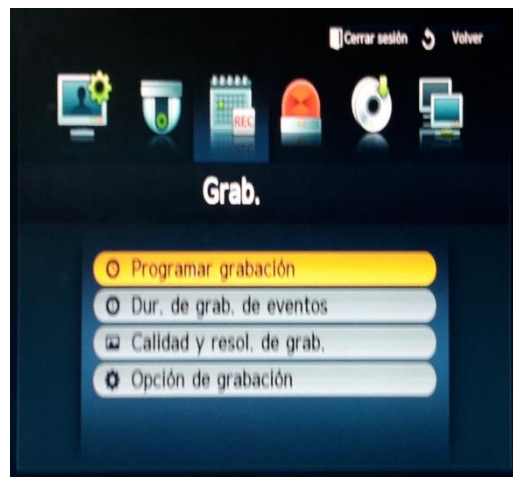


Imagen 195 – Programar grabación

7. Para las cámaras que ya se encontraba en la institución se configurará para que graben de forma continua todos los días a partir de las 6:00 hasta las 19:00, para esto se debe colocar los cuadros de color naranja.



Imagen 196 – Configuración de cámaras antiguas

8. Para las cámaras nuevas que si permiten visualizar durante la noche, se configurará para que grabe de forma continua y con eventos todos los días durante las 24 horas, es decir que toda la cuadrícula debe estar de color verde.

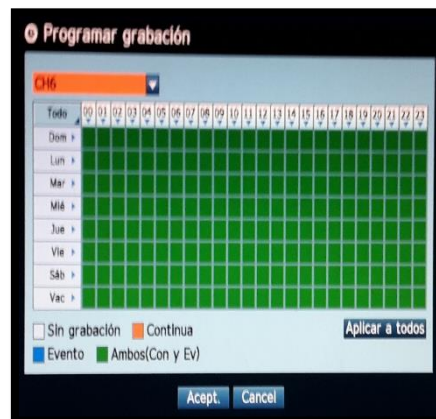


Imagen 197 – Configuración de cámaras nuevas

9. Dentro del menú Grabación ir hacia **Opción de grabación** y se deberá configurar para que el disco duro se sobrescriba cuando llegue al final.

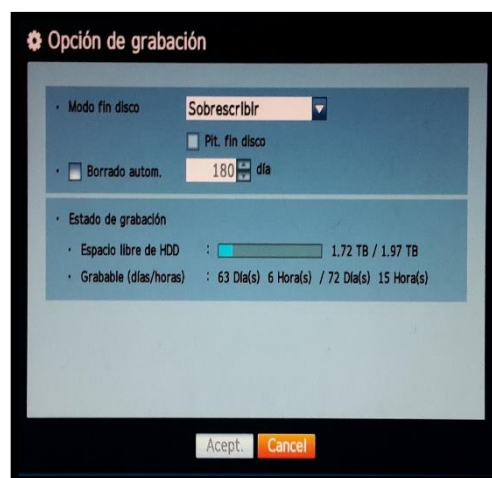


Imagen 198 – Configuración de almacenamiento