

Universidad Tecnológica de El Salvador

**FACULTAD DE INFORMÁTICA Y CIENCIAS APLICADAS
TÉCNICO EN INGENIERÍA DE REDES COMPUTACIONALES**



**TEMA: PROPUESTA DE CONFIGURACIONES DE SEGURIDAD A LA
INFRAESTRUCTURA DE RED INFORMÁTICA UTILIZADA POR LA
COMUNIDAD EDUCATIVA DEL CENTRO ESCOLAR SAN BARTOLOMÉ
PERULAPÍA.**

TRABAJO DE GRADUACIÓN PRESENTADO POR:

JULIO EDUARDO LÓPEZ LARREYNAGA

SAUL EDGARDO RODRIGUEZ ALVAREZ

KEVIN ENGELBERT MONTALVO QUINTANILLA

PARA OPTAR AL GRADO DE

**TÉCNICO EN INGENIERÍA DE REDES COMPUTACIONALES
SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA.**

SEPTIEMBRE, 2016

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA.

Página de Autoridades

ING. NELSON ZÁRATE SÁNCHEZ

RECTOR

LIC. JOSÉ MODESTO VENTURA

VICERRECTOR ACADÉMICO

ING. FRANCISCO ARMANDO ZEPEDA

DECANO

JURADO EXAMINADOR

ING. GUILLERMO ALAS.

PRESIDENTE.

ING. OSCAR RODRIGUEZ.

PRIMER VOCAL

ING. SALVADOR ALCIDES FRANCO.

SEGUNDO VOCAL

SEPTIEMBRE, 2016

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

ACTA DE EXAMEN PROFESIONAL

HABIÉNDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR:

Ing. Oscar Ernesto Rodríguez Alfaro, Ing. Salvador Alcides Franco Sánchez, Ing. José Guillermo Hernández Alas, a las 12:30m del día Lunes, 20 de Junio de dos mil dieciséis.

Y LUEGO DE HABER DELIBERADO SOBRE EL EXAMEN PROFESIONAL DE LOS ALUMNOS:

<u>1-Julio Eduardo López Larreynaga</u>	<u>Carnet 26-4829-2013</u>
<u>2-Kevin Engelbert Montalvo Quintanilla</u>	<u>Carnet 26-4821-2013</u>
<u>3-Saul Edgardo Rodriguez Alvarez</u>	<u>Carnet 26-2481-2011</u>

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:

"Propuesta de configuraciones de seguridad a la infraestructura de red informática, utilizada por la comunidad educativa del centro escolar san Bartolomé Perulapia"

PARA OPTAR AL GRADO DE:

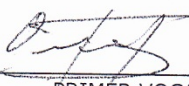
TÉCNICO EN INGENIERIA DE REDES COMPUTACIONALES

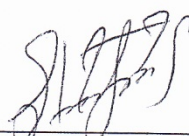
Y DEL CUAL TAMBIEN EVALUARON LOS CONOCIMIENTOS RELACIONADOS CON EL TEMA DEL MISMO. POR LO QUE ESTE JURADO RESUELVE DECLARAR EL EXAMEN COMO:

APROBADO

YA QUE CUMPLE CON LOS REQUISITOS ESTABLECIDOS EN EL REGLAMENTO DE GRADUACION DE LA UNIVERSIDAD.

San Salvador, 20 de Junio de dos mil dieciséis.

F. 
PRIMER VOCAL
Ing. Oscar Ernesto Rodríguez Alfaro

F. 
SEGUNDO VOCAL
Ing. Salvador Alcides Franco Sánchez

F. 
PRESIDENTE
Ing. José Guillermo Hernández Alas

Agradecimientos.

Le agradecemos a Dios por habernos acompañado y guiado a lo largo de estos años que cursamos nuestra carrera, por ser nuestra fortaleza en los momentos de debilidad y por brindarnos una vida llena de aprendizajes, experiencias y sobre todo felicidad.

Damos gracias a nuestros padres por apoyarnos en todo momento, por los valores que nos han inculcado, y por habernos dado la oportunidad de tener una excelente educación en el transcurso de nuestra vida. Sobre todo por ser un excelente ejemplo de vida a seguir.

Gracias a la gente importante para nosotros que ya no pudieron contemplar nuestros experiencias ya que no dudamos que están en el cielo y que observan nuestros pasos y celebran de igual forma nuestros triunfos y logros.

A nuestros familiares que son parte importante de nuestra vida y representan la unidad familiar.

Gracias a los Ingenieros, Técnicos y Docentes de la Universidad Tecnológica por el apoyo y la voluntad de darnos su instrucción. Gracias a la Universidad Tecnológica por darnos la oportunidad de crecer profesionalmente y aprender cosas nuevas.

El Grupo.

INDICE

Introducción.....	i
Capitulo I	
Planteamiento del problema.....	1
1. Antecedentes	1
2. Definición o Planteamiento	2
3. Objetivos.....	2
3.1. General	2
3.2. Específicos	2
4. Justificación.....	3
5. Alcances y Limitaciones del estudio.....	4
5.1. Alcances	4
5.2 Limitaciones.....	4
Marco Teórico	5
1. Antecedentes de la institución	5
2. Recursos de Software	5
2.1. ¿Qué es el Software Libre?.....	6
2.2 Zeroshell.	6
2.3 ClearOS.	8
2.4 Zentyal.	10
3. Seguridad Informática.....	11
4. Red Inalámbrica	12
4.1. Amenazas a la seguridad de las redes inalámbricas.....	13
5. Proxy	14
5.1. Funcionamiento	14
5.2 El filtrado.....	14
5.3 Autenticación.	14

5.4 Almacenamiento de 'logs'	15
5.5 Los proxys anónimos.	15
6. Seguridad Física de Las Instalaciones.....	15
7. Sistemas de Protección Eléctrica	19
Metodología	21
1. Participantes	21
2. Método	21
3. Instrumentos	22
3.1. Entrevista	22
3.2. Encuesta.....	23
3.3. Observación	23
4. Procedimientos	24
5. Estrategia de análisis de datos.....	25
Cuadro comparativo técnico	26
Análisis e interpretación de resultados.....	28
1. Encuesta dirigida a alumnos del Centro Escolar San Bartolomé Perulapía, para conocer la forma en que hacen uso de la red informática.	28
2. Hallazgos de los resultados.....	38
3. Propuesta de Solución.....	40
3.1 Diseño de infraestructura de red	40
3.2 Instalación y configuración de Clear Os 6.4.....	41
Red inalámbrica	73
Conclusiones	79
Referencias	81
Anexos	83

Introducción

El presente estudio tiene como finalidad determinar la problemática actual de la infraestructura de redes del Centro Escolar San Bartolomé Perulapía, a partir de ello poder identificar las posibles áreas de mejora con respecto a la seguridad física y lógica, se pretende definir y establecer el plan de acción para la mejora de los servicios locales y de Internet utilizados por los profesores, alumnos y personal administrativo, tomando en cuenta los alcances y limitaciones del estudio.

Para desarrollar la investigación y presentar las propuestas de mejora, es necesario contar con el marco de referencia que permita documentar las tecnologías existentes y que puedan ser utilizadas en el proyecto, por ello se ha incluido como parte de este documento temáticas relacionadas con la seguridad utilizando filtrado de contenido de código abierto, seguridad en la información, aspectos de seguridad en redes inalámbricas y seguridad física de las instalaciones de la red.

Siguiendo la metodología para la recolección de datos, fue necesario utilizar herramientas como la entrevista, la encuesta y la observación, en las cuales participaron profesores, alumnos y personal administrativo, recabando la información necesaria para luego tabularlas en una hoja de cálculo y así establecer la prioridad de incidencias.

Luego de la investigación se procede a presentar de manera ordenada los datos más relevantes de la investigación por medio de: tablas de Excel, graficas de pastel y generalidades de la infraestructura de red actual, diseño, desarrollo y requerimientos.

Capítulo I

Planteamiento del problema

1. Antecedentes

El Centro Escolar San Bartolomé Perulapía (CESABP), es una Institución de carácter oficial, que atiende a una población estudiantil cerca de los 400 alumnos, divididos entre los diferentes niveles, área básica, bachillerato y escuela para adultos, cuenta con la planta docente para atender a los aspectos académicos y personal administrativo para el control de la documentación, asignación del recurso didácticos a cada profesor y la asignación de prácticas en centro de cómputo.

Dentro del centro escolar se consideran tres tipos de usuarios: administrativos, profesores y alumnos, cada uno hacen uso de la red de informática que posee el centro escolar, que está constituida por un centro de prácticas de forma cableada y servicios de red inalámbricos, con cobertura en algunas zonas de la institución. El problema principal de la infraestructura de red del centro escolar, es que no se cuenta con un dispositivo de red, software adecuado y aplicativos para controlar los accesos a Internet, generando que la comunidad educativa tenga libre acceso y sin ninguna restricción al momento de navegar en diferentes sitios de Internet, al no poseer los controles adecuados los equipos del centro de cómputo se ven expuestos a contaminarse mucho más rápido de virus. La falta de estos filtros también pone en riesgo la información de los alumnos, profesores, personal administrativo y el centro escolar, ya que pueden estar expuestos al robo de información. Otro aspecto importante es el hecho de que los profesores cuando necesitan

acceso a información por parte del administrador del centro de cómputo lo hacen a través del uso de USB, ya que no se cuenta con un recurso compartido centralizado, también hay poco uso de la red inalámbrica por parte de los alumnos, debido a que no se cuenta con las configuraciones adecuadas en los equipos inalámbricos para una conexión segura. El último aspecto a considerar es que la infraestructura de red también carece de la seguridad física con respecto al cableado estructurado, hay algunos cables de red que están expuestos y sin ninguna protección.

2. Definición o Planteamiento

¿Qué hardware y software deben aplicarse para aumentar la seguridad en la infraestructura de la red informática utilizada en el Centro Escolar San Bartolomé Perulapía?

3. Objetivos

3.1. General

Elaborar una propuesta de configuraciones que ayuden a mejorar la seguridad física y lógica de la infraestructura de red del Centro Escolar San Bartolomé Perulapía.

3.2. Específicos

- Identificar los elementos claves que afectan la seguridad en la infraestructura de red del centro escolar y que sirva como base para el diseño de una propuesta de mejora a la seguridad.
- Documentar las tecnologías de seguridad física y lógica que puedan ser utilizadas en la propuesta de solución.

- Seleccionar las tecnologías adecuadas para resolver la problemática actual de la infraestructura de red del centro escolar.
- Implementar configuraciones que aumenten la seguridad en el acceso a Internet por parte de la comunidad educativa.
- Realizar la propuesta de mejora a la seguridad de la red inalámbrica y las recomendaciones de seguridad física del cableado estructurado.

4. Justificación

El presente estudio nace a raíz de la necesidad que posee el Centro Escolar San Bartolomé Perulapía con respecto al manejo de los recursos informáticos locales y de Internet. El desarrollo de la investigación pretende beneficiar a la comunidad educativa y al centro escolar como tal.

- Alumno: Se mejorará el acceso a los recursos de Internet en centro de prácticas y la red inalámbrica, ya que con la implementación del filtrado de contenido se bloqueará el acceso a Sitios no autorizados, aumentando así la disponibilidad de los servicios que sí están permitidos.
- Profesor: El acceso a la información se centralizará de tal forma que pueda estar disponible en el momento que se requiera.
- Personal administrativo: Se aumentará la seguridad en el acceso a sitios Web potencialmente peligrosos y que sean potenciales puertas para el robo de información.
- Centro Escolar: Se contará con una infraestructura de red informática con mejores niveles de seguridad física y lógica.

5. Alcances y Limitaciones del estudio

5.1. Alcances

La presente investigación tiene por finalidad realizar el siguiente:

- Realizar una propuesta de diseño para mejorar los problemas de seguridad en la infraestructura de red
- Realizar una propuesta de configuración de hardware y software adecuado a las necesidades de acceso a Internet en el centro de prácticas y las áreas administrativas
- Realizar una propuesta de mejora a las configuraciones en la red inalámbrica que esté acorde a las necesidades de la comunidad educativa.
- Realizar una guía de recomendaciones para proteger el cableado estructurado de la red, mejorando así la seguridad física.

5.2 Limitaciones

La presente investigación tiene como limitaciones los siguientes aspectos:

- Temporales: El estudio de la problemática está contemplado a realizarse entre el 8 de febrero hasta el 5 de junio, tiempo que dura el proceso de graduación.
- Geográficas: Se estudia la infraestructura de red del Centro Escolar San Bartolomé Perulapía, ubicado en Avenida Felipe de Paz, Barrio el Centro del municipio de San Bartolomé Perulapía, Departamento de Cuscatlán.
- Tecnológicas: Sólo se utilizarán los equipos de red y servicios de Internet con los que cuenta la institución.
- Financieras: La adquisición de nuevas tecnologías dependerá del presupuesto con que cuente el grupo de trabajo.

Capítulo II

Marco Teórico

1. Antecedentes de la institución

El Centro Escolar San Bartolomé Perulapía (CESABP), es una Institución pública, esta se encuentra ubicada en una zona semi-rural del municipio de San Bartolomé Perulapía en el Departamento de Cuscatlán, esta atiende los niveles de tercer ciclo (7° a 9° grado), bachillerato general y escuela para jóvenes y adultos. Cuenta con un total de quince maestros y tres empleados administrativos. Sus instalaciones cuentan con seis aulas disponibles para clases, un Centro Computo y una biblioteca. Desde el año 2015 se cuenta con una con una conexión a internet de 5 Mbps (Megabytes por segundo). En el proceso educativo se hace uso de diferentes herramientas entre las que sobresale el uso de las computadoras, las cuales son utilizadas por alumnos, profesores y personal administrativo. Según consta en el Plan Anual Escolar (PEA) (CESABP, 2015).

En este proceso la red informática de la institución constituye un soporte vital, ya que con este administrativos realizan el trabajo referente a actividades del Ministerio de Educación vía Internet, maestros la utilizan para llevar a sus estudiantes a buscar información, así como también para realizar prácticas.

2. Recursos de Software

En base a los objetivos planteados, se investigaron recursos de Software, que pueden dar una solución a los problemas que la red informática requiere. Un factor muy importante es el económico, por ello se sugieren Sistemas basados en Administración de Redes Informáticas que pertenecen a la categoría del Software Libre.

2.1. ¿Qué es el Software Libre?

El software libre significa que los usuarios tienen la libertad para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software.

El software libre es una cuestión de libertad, no de precio. Para entender el concepto, debe pensarse en «libre» como en «libertad de expresión», no como en "cerveza gratis".

De manera más precisa, el software libre significa que los usuarios de un programa tienen las cuatro libertades esenciales:

- La libertad de ejecutar el programa como desee, en cualquier propósito (libertad 0).
- La libertad de estudiar cómo funciona el programa, y adaptarlo a tus necesidades (libertad 1).El acceso al código fuente es una condición previa para esto.
- La libertad de distribuir copias, con lo que puedes ayudar a tu vecino (libertad 2).
- La libertad de mejorar el programa y publicar sus mejoras al público, de modo que toda la comunidad se beneficie (libertad 3).El acceso al código fuente es una condición previa para esto. (Free Software Foundation, Inc., 2016).

Es por ello que a continuación se describen algunos Sistemas Operativos de licencia libre que proporcionan funciones de Administración de redes informáticas.

2.2 Zeroshell.

(FulvioRicciardi, Zeroshell, 2015) Describe que Zeroshell es una distribución Linux para servidores y dispositivos integrados destinados a proporcionar los servicios de red principal de una LAN requiere. Está disponible en forma de Live CD o de imagen de Compact Flash y se puede configurar y administrar utilizando el navegador web.

Características de esta distribución de Linux para aplicaciones de red que se ajustan a lo requerido son:

- Portal Cautivo para apoyar el inicio de sesión web, en redes cableadas e inalámbricas. Zeroshell actúa como puerta de enlace de las redes en la que el portal cautivo está activo y en la que las direcciones IP (Protocolo de Internet) (por lo general pertenecientes a las subredes privadas) son asignados dinámicamente por el servidor DHCP. Un cliente que tiene acceso a esta red privada debe autenticarse a través de un navegador web utilizando Kerberos 5 nombre de usuario y contraseña antes de que el firewall del Zeroshell permite al público acceder a la LAN. El Captive Portal se utilizan a menudo para proporcionar acceso autenticado a Internet en los hotspots en alternativa al protocolo de autenticación 802.1X demasiado complicado de configurar para los usuarios. Zeroshell implementa la funcionalidad de Portal Cautivo en forma nativa, sin necesidad de utilizar otro software específico NoCat o Chillispot;
- Servidor proxy de HTTP (Hypertext Transfer Protocol) que es capaz de bloquear las páginas web que contienen virus. Esta característica se implementa con la solución antivirus ClamAV y el servidor proxy HAVP. El servidor proxy trabaja en proxy transparente el modo en el que, no es necesario configurar los navegadores de los usuarios a usarlo, pero las peticiones http será redirigido automáticamente;

- Firewall Packet Filter y Stateful Packet Inspection (SPI) con filtros aplicables en las dos rutas y bridges en todo tipo de interfaces, incluyendo VPN (Virtual Private Network) y VLAN;
- QoS (Quality of Service) y de gestión de tráfico para controlar el tráfico en una red congestionada. Usted será capaz de garantizar el ancho de banda mínimo, limitar el ancho de banda máximo y asignar una prioridad a una clase de tráfico.

2.3 ClearOS.

ClearOS es una distribución GNU/Linux para servidores enfocada a PYMES (Pequeñas y Medianas Empresas), que incluye la funcionalidad de cortafuegos entre varias otras. Es configurable mediante acceso por interfaz web. Puede instalarse en un servidor hardware, en una máquina virtual o en la nube.

Funcionalidad:

- **DMZ Firewall - Cortafuegos DMZ**

Establecer una zona desmilitarizada (DMZ) en la red de la empresa puede aumentar considerablemente la seguridad de la misma. Una DMZ está aislada de la red local (LAN) de la empresa, de forma que el tráfico desde el exterior pasa por esta zona y desde ésta a la LAN. Así, al establecer un filtrado en la DMZ, llegar a la LAN únicamente el tráfico exterior que supere dicho filtrado.

- **Egress Firewall - Cortafuegos de salida**

Así como se establecen reglas de filtrado en la entrada, también pueden especificarse para el tráfico de salida desde la LAN de la empresa. De esta manera,

pueden bloquearse varios tipos de tráfico que tengan como origen la LAN y como destino una red externa.

- **QoS**

La QoS (calidad de servicio) aplicación se utiliza para dar forma o priorizar el tráfico de red.

- **Definición manual de reglas**

Pueden modificarse manualmente las reglas de los cortafuegos mediante consola, editando el fichero /etc/firewall con el editor vim, incluido en clearOS. Esta opción sólo es recomendable para usuarios expertos, por su dificultad y porque mediante la edición manual pueden producirse fallos inesperados y difíciles de detectar.

- **Otras funcionalidades de clearOS**

- | | |
|-------------------------------------|--------------------------------------|
| - Protección antivirus. | - Protección antiphishing. |
| - Sistema de detección de intrusos. | - Sistema de prevención de intrusos. |
| - Servidor Proxy. | - Servidor MySQL. |
| - Servidor FTP. | - QoS (Calidad de Servicio) |
| - Servidor DNS. | |
| - Servidor DHCP. | |

(Centro de Apoyo Tecnológico a Emprendedores, 2011).

ClearOS se conoce comúnmente como la próxima generación de Small Business Server (PYMES), incluyendo al mismo tiempo funcionalidades indispensables como Gateway y Networking. Proporciona una solución de TI (Tecnologías de Información y Comunicación) de gran alcance con una interfaz de usuario elegante que está completamente basado en la web. (ClearCenter, Corp., 2016).

2.4 Zentyal.

Zentyal es un servidor linux desarrollado expresamente para la administración de redes a través del navegador web firefox.

Funcionalidad:

Zentyal puede actuar:

- Gestionando la infraestructura de red, al permitir la instalación/configuración de servidores DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), WEB y FTP (File Transfer Protocol) entre otros.
- Como puerta de enlace o gateway a Internet.
- Gestionando las amenazas de seguridad.
- Como servidor de oficina, al compartir recursos como ficheros e impresoras.
- Como servidor de comunicaciones unificadas o una combinación de estas, tales como correo electrónico, VoIP, mensajería instantánea, y groupware (compartición de calendarios, agendas, webmail, wiki).
- Además, Zentyal incluye un marco de desarrollo para facilitar el desarrollo de nuevos servicios basados en Unix. (Sánchez, Guadalupe Bermejo, 2012)

3. Seguridad Informática

Si nos atenemos a la definición de la Real Academia de la Lengua RAE, seguridad es la "cualidad de seguro". Buscamos ahora seguro y obtenemos "libre y exento de todo peligro, daño o riesgo".

A partir de estas definiciones no podríamos aceptar que la seguridad informática es la cualidad de un sistema informático exento de peligro", por lo que habrá que buscar una definición más apropiada.

Algo básico la seguridad no es un producto, si no un proceso. Por lo tanto, podríamos aceptar que una primera definición más o menos aceptable de seguridad informática seria:

"Un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas. Concienciarlas de su importancia en el cual será algo crítico".

Recuerde que la seguridad informática no es medible, en cambio si podríamos desarrollar diversas herramientas para cuantificar de alguna forma nuestra inseguridad informática. Todo lo anterior en base a lo descrito en Libro Electrónico de Seguridad Informática y Criptografía (Jorge Ramío, 2006).

Ahora podemos resumir que de La seguridad de la red es el proceso por el cual se protegen los recursos de información digital. Los objetivos de la seguridad son mantener la integridad, proteger la confidencialidad y asegurar la disponibilidad. El crecimiento de la computación ha generado enormes avances en la forma en que las

personas viven y trabajan. Por lo tanto, todas las redes deben estar protegidas para alcanzar su máximo potencial. Esto como específica. (MicroCisco, 2009).

Un propósito principal de la seguridad es mantener afuera a los intrusos. En la mayoría de los casos, esto significa construir paredes fuertes y establecer puertas pequeñas bien protegidas para proporcionar acceso seguro a un grupo selecto de personas. Esta estrategia funciona mejor para las LANs cableadas que para las WLANs. El crecimiento del comercio móvil y de las redes inalámbricas hace que los modelos viejos sean inadecuados. Las soluciones de seguridad deben estar integradas sin fisuras y ser muy transparentes, flexibles y administrables. Cuando la mayoría de la gente habla sobre seguridad, hacen referencia a asegurar que los usuarios puedan realizar sólo las tareas que tienen autorizado hacer y que puedan obtener sólo la información que tienen autorizado tener. La seguridad también significa asegurar que los usuarios no puedan causar daño a los datos, a las aplicaciones o al entorno operativo de un sistema. La palabra seguridad comprende la protección contra ataques maliciosos, también comprende el control de los efectos de los errores y de las fallas del equipo. Todo lo que pueda proteger contra un ataque inalámbrico probablemente evitará también otros tipos de problemas. (MicroCisco, 2009)

4. Red Inalámbrica

Una red inalámbrica (Wireless Network) es la conexión de nodos que se da por medio de ondas electromagnéticas, sin necesidad de una red cableada o alámbrica, la transmisión y la recepción se realizan a través de puertos. Una de sus principales ventajas es la reducción de los costos, ya que se elimina el cableado Ethernet y

conexiones físicas entre nodos, pero también tiene una desventaja considerable ya que para este tipo de red se debe tener una seguridad mucho más exigente y robusta para evitar a los intrusos. (Madrid Molina, 2006).

4.1. Amenazas a la seguridad de las redes inalámbricas

La mayoría de los incidentes de seguridad inalámbrica ocurren porque los administradores de sistemas no implementan contramedidas. Por lo tanto, la cuestión no es sólo confirmar que existe una vulnerabilidad técnica y encontrar una contramedida que funcione. También es crítico verificar que la contramedida está en su lugar y que funciona correctamente. (Ríos, 2011).

Existen cuatro clases principales de amenazas a la seguridad inalámbrica:

1. **Amenazas no estructuradas:** Las amenazas no estructuradas consisten principalmente en personas sin experiencia que usan herramientas de piratería informática.
2. **Amenazas estructuradas:** Estas personas conocen las vulnerabilidades del sistema y utilizan técnicas de piratería informática sofisticadas para introducirse en las empresas confiadas.
3. **Amenazas externas:** Las amenazas externas pueden provenir de personas u organizaciones que trabajan fuera de una empresa y que no tienen acceso autorizado a los sistemas informáticos ni a la red.
4. **Amenazas internas:** Las amenazas internas son las provocadas por una persona que tiene acceso autorizado a la red, ya sea mediante una cuenta o acceso físico. (Ríos, 2011)

5. Proxy

Un servidor proxy es un ordenador que sirve de intermediario entre un navegador web e Internet. El proxy contribuye a la seguridad de la red. Es un equipo que actúa de intermediario entre un explorador web e Internet. Los servidores proxy ayudan a mejorar el rendimiento en Internet ya que almacenan una copia de las páginas web más utilizadas. También ayudan a mejorar la seguridad, ya que filtran algunos contenidos web y software malintencionado. (Dyllan, 2009).

5.1. Funcionamiento

Los servidores proxy permiten proteger y mejorar el acceso a las páginas web, al conservarlas en la caché. De este modo, cuando un navegador envía una petición para acceder a una página web, que previamente ha sido almacenada en la caché, la respuesta y el tiempo de visualización es más rápido. (Dyllan, 2009)

5.2 El filtrado.

El filtrado se aplica en función de la política de seguridad implementada en la red. Este permite bloquear sitios considerados maliciosos o sitios considerados inútiles en relación a la actividad de la empresa. (Dyllan, 2009)

5.3 Autenticación.

A fin de limitar el acceso a la red exterior, y aumentar de este modo la seguridad de la red local, se puede implementar un sistema de autenticación para acceder a recursos externos. Esto es bastante disuasivo para los usuarios que desean visitar sitios que estén en contra de las reglas de uso de Internet en la empresa. (Dyllan, 2009).

5.4 Almacenamiento de 'logs'.

El almacenamiento de logs de los sitios visitados y páginas vistas, permite al administrador de la red redefinir la política de seguridad de la red y/o detectar a un usuario que visita frecuentemente sitios maliciosos o sin relación con la actividad de la empresa. (Dyllan, 2009)

5.5 Los proxys anónimos.

Además de ocultar la dirección IP, un proxy anónimo puede eliminar cookies, pop-ups, banners, scripts e información confidencial en los campos de texto (nombre de usuario y contraseña). (Dyllan, 2009).

6. Seguridad Física de Las Instalaciones

Los locales donde se ubiquen los ordenadores que contienen o puedan acceder a los ficheros y datos más sensibles de la organización deber ser objetos de una especial protección, de modo que se pueda garantizar la confidencialidad, integridad y disponibilidad de los datos y aplicaciones más críticas. Estos locales deberán contar con los medios mínimos de seguridad que eviten riesgos de indisponibilidad que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas.

Generalmente, una organización de tamaño mediano o grande dispondrá de una sala especialmente acondicionada para ubicar los servidores centrales con todos los ficheros y aplicaciones informáticas, Se debería implantar un sistema, de control de acceso físico a esta sala, permitiendo la entrada al personal debidamente autorizado relacionando con el sistema de información.

Las medidas relacionadas con la seguridad física deberán contemplar, en primer lugar, las características de construcción de los edificios o instalaciones donde se vayan a ubicar los recursos informáticos y del sistema de información, analizando aspectos como los siguientes:

- Protección frente a daños por fuego, inundación, explosiones, accesos no autorizados, etcétera.
- Selección de los elementos constructivos internos más adecuados: puertas, paredes, suelos y falsos techos, canalizaciones eléctricas, canalizaciones de comunicaciones... Estos elementos deberán cumplir con el máximo nivel de protección exigido por la normativa de construcción. Para evitar el polvo y la electricidad estática se debería aplicar un revestimiento especial en las paredes, el techo y el suelo de las salas donde se vayan a ubicar los servidores y equipos con los datos y aplicaciones más importantes. Asimismo, por este mismo motivo, no se deberían utilizar alfombras o mosquetas para cubrir el suelo en estas salas.
- Definición de distintas áreas o zonas de seguridad dentro del edificio:
 - Áreas públicas:** pueden acceder sin restricciones personas ajenas a la organización.
 - Áreas Internas:** reservadas a los empleados.
 - Áreas de acceso restringido:** áreas críticas a las que solo pueden acceder un grupo reducido de empleados con el nivel de autorización requeridos
- Disponibilidad de zonas destinadas a la carga, descarga y almacenamiento de suministros.

- Implantación de sistema de vigilancia basados en cámaras en circuito cerrado de televisión y en alarmas y detectores de movimiento. En este último caso se podrían utilizar barreras de infrarrojos, barreras de microondas, detectores de ultrasonidos, detectores de apertura de puertas, detectores de rotura de vidrios, detectores de vibraciones en superficies, etcétera.
- Control de las condiciones ambientales en las instalaciones, mediante un sistema independiente de ventilación, calefacción, aire acondicionado y humidificación /deshumidificación (HVAC: “Heating, Ventilating and Air-conditioning System”) que hacer posible, debería funcionar de forma ininterrumpida, 24 horas al día durante 365 días del año. El objetivo perseguido es tratar de mantener estables la temperatura y la humedad de la sala o salas donde se ubiquen los servidores y los equipos informáticos más importantes para la organización, dentro de los límites recomendados por los fabricantes: la temperatura entre los 18 y 24 grados centígrados, con una humedad relativa del ambiente de la sala de entre 30% y el 50%.

En relación con las medidas contra incendios y contra inundaciones, conviene destacar la importancia de que el local donde se vayan ubicar los equipos informáticos debería estar construido con materiales ignífugos, empelando muebles incombustibles y tratando de evitar en la medida delo posible los materiales plásticos e inflamables. Esta medida constructiva se debería complementar con la instalación de sistema de detección y de extinción de incendios: detectores de humos y sistemas de extinción por aerosol, que reemplazan a los antiguos sistemas de extinción mediante gas halón.

Por otra parte, en lo que se refiere al control de acceso físico a las instalaciones, la política de seguridad debería definir cómo se va a llevar la identificación del personal propio (identificador con nombre, cargo y fotografía) y del personal ajeno (utilización de un identificador provisional), estableciendo asimismo los procedimientos de acceso a las Áreas Críticas (Áreas de acceso Restringido).

La organización debería elaborar y mantener actualizada una lista de personal con autorización de acceso permanente a estas Áreas Críticas, así como a una segunda lista de personal con autorización de acceso temporal, contemplando también los posibles accesos de empleados fuera de su horario de laboral habitual. Una autorización de acceso temporal debería reflejar el nombre de quien lo autoriza, la identidad del visitante autorizado, el motivo, el intervalo de fechas en que se tiene validez la autorización.

En estas áreas críticas se podrían ubicar arcos con electroimanes en los puntos de acceso, con el objetivo de provocar el borrado inmediato de discos duros y otros soportes que pudieran ser sustraídos sin la correspondiente autorización de la organización.

Asimismo, la política de seguridad debería contemplar la existencia de un registro de entradas y salidas del personal, sobre todo en las áreas de acceso restringido, a fin de poder monitorizar las actividades y horarios del personal.

En lo que se refiere al control de acceso y protección física de los equipos informáticos más sensibles, como los servidores y algunas estaciones de trabajo, estos deberían estar ubicados en salas especialmente acondicionadas, con puertas dotadas de

cerraduras de seguridad, habilitando un control de acceso mediante llaves, tarjetas electrónicas, dispositivos biométricos u otros elementos similares, aplicando medidas de seguridad adicionales en días y en horarios sin actividad laboral.

La seguridad física de los sistemas informáticas se podría reforzar con medidas como la utilización de anclajes de los quipos a mesas de trabajo; el bloqueo de disqueteras, lectores de CD/DVD y puertos USB; los protectores de teclado: etcétera.

Si las instalaciones de la organización no pudiesen garantizar un adecuado nivel de protección de los activos en los que se refiere a la seguridad física del edificio, control de accesos, cableado, alarmas, etcétera, la solución podría pasar por la ubicación de estos recursos en el “data center” de un operador de servicios de telecomunicación, bajo la modalidad de “housing” o de “hosting”, firmando un contrato con unas determinadas garantías de nivel de servicio (SLA).

7. Sistemas de Protección Eléctrica

Las directrices de seguridad relacionadas con la protección eléctrica de los equipos informáticos deberían definir aspectos como los que se indican a continuación:

- Adecuada conexión de los equipos a la toma de tierra.
- Revisión de la instalación eléctrica específica para el sistema informático, siendo recomendable disponer de tomas protegidas y estabilizadas, aisladas del resto de la instalación eléctrica de la organización.
- Eliminación de la electricidad estática en las salas donde se ubiquen los equipos más importantes, como los servidores para ellos, sería recomendable emplear un revestimiento especial en las paredes, el techo y el suelo del

local para evitar el polvo y la electricidad estática, así como evitar el uso de alfombras o moquetas para cubrir el suelo.

- Filtrado de ruidos e interferencias electromagnéticas, que pueden afectar el normal funcionamiento de los equipos.
- Utilización de Sistemas de Alimentación Ininterrumpida (SAI).

En relación con este último apartado, los Sistemas de Alimentación Ininterrumpida permiten proteger a los equipos informáticos frente a picos a caídas de tensión, así como de los cambios en la frecuencia del fluido eléctrico.

De este modo, se consigue una mayor estabilización del suministro y se dispone de una alimentación auxiliar para afrontar posibles cortes en este suministro (aunque sólo por tiempo limitado, debido a que se utilizan acumuladores). También se podría contemplar la posibilidad de utilizar generadores diésel en lugar de acumuladores para prolongar la duración de la alimentación auxiliar del sistema.

Por lo tanto, para proteger la seguridad de los servidores más importantes frente a fallos en el suministro eléctrico o sobretensiones, la empresa podría disponer de un SAI conectado a cada una de estas máquinas, configurado de tal modo que, a través de una conexión vía puerto serie o USB, se pueda facilitar el cierre ordenado de las bases de datos y el apagado automático de servidor en caso de un corte prolongado del suministro eléctrico. (Veites, 2011)

Capítulo III

Metodología

La investigación se llevó a cabo en el Municipio de San Bartolomé Perulapía, ubicado en el departamento de Cuscatlán, específicamente en el Centro Escolar San Bartolomé Perulapía con el fin de recabar información necesaria para conocer las vulnerabilidades informáticas que se tienen mediante la entrevista y encuesta a la población estudiantil para mejorar el uso de la misma.

Para realizarla se tomaron en cuenta los siguientes puntos:

1. Participantes

Era necesario saber la situación actual de la infraestructura de red en la institución por lo que se entrevistó al Coordinador de Informática para que este explicara directamente los detalles de cómo está distribuida. También era importante saber la forma en la que los maestros hacen uso de la red y las herramientas tecnológicas asociadas. Por último fue necesario encuestar a los alumnos para saber de qué forma utilizan la red inalámbrica e internet en sus clases.

2. Método

Se realizó una encuesta a un número de ochenta alumnos, entre ellos sesenta fueron alumnos de bachillerato y veinte de nivel básico, se tomó como muestra la mayor parte de alumnos de bachillerato debido a que por su edad, conocimientos y la carga académica a la que están sujetos, les convierte en sujetos propicios para poner a prueba las debilidades de la conexión a internet.

Los maestros entrevistados imparten las materias de Matemáticas, Ciencias, Estudios Sociales, Seminarios y Orientación para la vida. Se decidió elegir estas materias ya que son las que más hacen uso del aula informática y por lo tanto de la red.

No fue necesario entrevistar al personal administrativo ya que el coordinador informático pertenece a esta categoría y utiliza diariamente la red, dando fe de lo anterior

3. Instrumentos

Se utilizaron tres métodos para la recolección de datos: la entrevista, la encuesta y la observación. Existen muchos detalles de la red que solo el encargado de esta conoce por lo que era importante saber sus impresiones, por lo que la mejor forma de hacerlo era mediante una entrevista. De igual forma se realizó entrevista únicamente a tres maestros que hacen uso cotidiano de internet.

Para ello se tomó este criterio debido a que estos imparten materias en el que por su contenido hacen uso constante de la red alrededor de cuarenta horas semanales repartidas entre todas las materias.(CESABP)

También se visitaron las instalaciones del centro escolar y se observó la forma en que tanto maestros, alumnos y personal administrativo realizan sus actividades y la manera como la red informática se utiliza como apoyo a las actividades diarias.

3.1. Entrevista

La entrevista, es la comunicación interpersonal establecida entre el investigador y el sujeto de estudio a fin de obtener respuestas verbales a los interrogantes planteados sobre el problema propuesto. Se considera que este método es más eficaz que el

cuestionario, ya que permite obtener una información más completa. A través de ella el investigador puede explicar el propósito del estudio y especificar claramente la información que necesite; si hay interpretación errónea de las preguntas permite aclararla, asegurando una mejor respuesta.

Se podrá definir que la entrevista consiste en obtención de información oral de parte de una persona (entrevistado) lograda por el entrevistador directamente, en una situación de cara a cara, a veces la información no se transmite en un solo sentido, sino en ambos, por lo tanto una entrevista es una conversación entre el investigador y una persona que responde a preguntas orientadas a obtener información exigida por los objetivos específicos de un estudio.(Amador, 2009)

3.2. Encuesta

La encuesta es un método de investigación que consiste en obtener información de las personas encuestadas mediante el uso de cuestionarios diseñados en forma previa, con una serie de preguntas pre-elaboradas en un orden pre-establecido e indicaciones claras para guiar la obtención de respuestas.(Thompson, 2005)

3.3. Observación

La observación es la adquisición activa de información a partir del sentido de la vista. Se trata de una actividad que detecta y asimila los rasgos de un elemento utilizando los sentidos como instrumentos principales. El término también puede referirse a cualquier dato recogido durante esta actividad. (Galindo, 1998)

4. Procedimientos

La primera tarea consistió en redactar una entrevista que recolectara la información necesaria para saber el estado actual de la red informática y la forma en que los tres tipos de usuarios: administrativos, profesores y alumnos hacen uso de ella.

La segunda tarea consistió en pasar una encuesta a cada alumno utilizando la metodología antes mencionada para poder recabar la información necesaria para mejoras en la infraestructura de red.

La tercera tarea se observó la infraestructura de la red, su funcionamiento, equipos utilizados y verificación de la conexión a Internet. El encargado manifestó que existe una red inalámbrica, con dos ID de Red: CESABP e INFO.

El primero corresponde al que se conectan los administrativos y los maestros, posee un filtro de seguridad por dirección MAC. El segundo está disponible para alumnos y no posee restricciones.

Se observó que la porción de red que va del aula informática hacia la dirección no está distribuida bajo ninguna norma de cableado estructurado.

La red del aula informática fue instalada hace dieciséis años, tiempo en el cual se ha dañado cuatro puntos de red dentro ella. (Acta de entrega del ministerio de educación, 2003).

La cuarta tarea consistió en tabular el resultado de las encuestas y entrevistas para una interpretación de los datos la cual revelaría la prioridad y la incidencia de los problemas que posee la infraestructura de red.

5. Estrategia de análisis de datos

Es un proceso que se llevará a cabo desde el análisis hasta tabular el resultado de las encuestas y entrevistas en una hoja de cálculo en Excel y luego se hará una interpretación de los datos obtenidos para representarlos mediante gráficos con el fin de profundizar acerca de la problemática en este caso la infraestructura de la red informática y tener las ideas más importantes para mejorar el uso de la misma de acuerdo a las necesidades de los alumnos y maestros.

Hoja de cálculo

Una hoja de cálculo es una estructura tabular de renglones y columnas que permiten una infinidad de aplicaciones. Una vez que se introducen los datos en la hoja de cálculo se pueden analizar y trabajar fácilmente con ellos. Su función es realizar operaciones matemáticas. Permite procesar números y ayuda a realizar cálculos desde los más simples hasta los más complejos que implican manipular muchos números y realizar muchas operaciones numéricas. (Pérez, 2009)

Gráfico

Un gráfico es la representación de datos, generalmente numéricos, mediante líneas, superficies o símbolos, para ver la relación que esos datos guardan entre sí y facilitar su interpretación. También puede ser un conjunto de puntos, que se plasman en coordenadas cartesianas, y sirven para analizar el comportamiento de un proceso, o un conjunto de elementos. La utilización de gráficos hace más sencilla e inmediata la interpretación de los datos. A menudo un gráfico nos dice mucho más que una serie de datos clasificados por filas y columnas. (Ávila, 2005)

Cuadro comparativo técnico

En los siguientes puntos se detallan las necesidades de la red en el centro escolar:

- No cuenta con un software adecuado y aplicativo para controlar los accesos a Internet.
- Ninguna restricción al momento de navegar en diferentes sitios de Internet.
- Expuestos al robo de información.
- No se cuenta con un recurso compartido centralizado.
- No se cuenta con las configuraciones adecuadas en los equipos inalámbricos para una conexión segura.

Partiendo de las necesidades que presenta la institución en su infraestructura de red, se investigó los distintos tipos de software red de licencia libre que cumplan con los requisitos necesarios para implementar mejoras en la seguridad de la red.

Software libre

- Zeroshell
- Zentyal
- ClearOS

Para poder elegir un programa que se adapte a las necesidades, se hizo un cuadro comparativo de las distintas funcionalidades de cada software mencionado.

Ver a continuación el siguiente cuadro comparativo del software de red de licencia libre.

CUADRO COMPARATIVO						
Funcionalidades del software	Software Libre - Sistemas Operativos de Red que cumplen con las necesidades del C.E.					
	ClearOs Cumple		ZeroShell Cumple		Zentyal Cumple	
	Si	No	Si	No	Si	No
Proxy Web con filtro de contenido y antivirus (Squid y DansGuardian).	x		x		x	
Sistema de prevención y detección de intrusos (Snort).	x			x		x
Compartir impresoras y archivos por medio de su controlador de Dominio. (Samba y CUPS).	x		x		x	
Redes Privadas Virtuales (PPTP, OpenVPN).	x		x		x	
Filtrado de protocolo por ejemplo p2p.	x		x		x	
Protección Antispam.	x		x		x	
Bloqueo de Host Externos.	x			x	x	
Administración en la velocidad de Carga y Descarga.	x		x		x	
Protección a usuarios de phishing, mensajes fraudulentos que roban información privilegiada.	x			x		x
Administración de firewall	x		x		x	
Total	10 pts.		7 pts.		8 pts.	

Según los objetivos planteados al principio de esta investigación y tomando como base los resultados del cuadro comparativo se llegó a la conclusión de elegir ClearOS como el Software de red a implementar en la propuesta de solución ya que cumple con todo lo requerido para gestionar los servicios que la infraestructura de red de la institución requiere.

Capítulo IV

Análisis e interpretación de resultados

En este capítulo se presentan de manera ordenada los datos más relevantes de la investigación por medio de: tablas de Excel, graficas de pastel y generalidades de la infraestructura de red actual, diseño, desarrollo y requerimientos propuestos, de acuerdo a las encuestas, entrevistas hechas a los alumnos y maestros del Centro Escolar, así como también las pruebas necesarias para asegurar su correcto funcionamiento.

1. Encuesta dirigida a alumnos del Centro Escolar San Bartolomé Perulapía, para conocer la forma en que hacen uso de la red informática.

Pregunta # 1. ¿Tiene acceso a internet en su escuela?

Objetivo: Determinar qué porcentaje de los usuarios de la Institución tiene conocimiento de que la escuela posee conexión a internet.

Tabla 4.1

Alternativas	Frecuencia	Porcentaje
Si	40	100%
No	0	0%
No se	0	0%
Total	40	100%

C.E San Bartolomé Perulapía 2016.

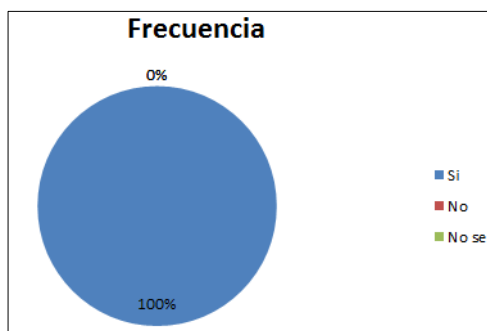


Figura 4.1. Grafica de resultados 1

Análisis e interpretación de la pregunta 1.

El 100% de los alumnos encuestados tienen conocimiento que la escuela posee conexión a internet, por lo que hacer uso de esta herramienta depende simplemente de la necesidad o del conocimiento necesario para su utilización.

Pregunta # 2 ¿Cuántas horas a la semana hace uso del recurso de internet?

Objetivo: Determinar la importancia que tiene el uso de internet en las actividades diarias.

Tabla 4.2

Tabla muestra la frecuencia y porcentaje en horas que un usuario hace uso del recurso de internet.

Alternativas	Frecuencia	Porcentaje
2 horas	28	70%
4 horas	6	15%
6 o mas	6	15%
Total	40	100%

C.E San Bartolomé Perulapía 2016.

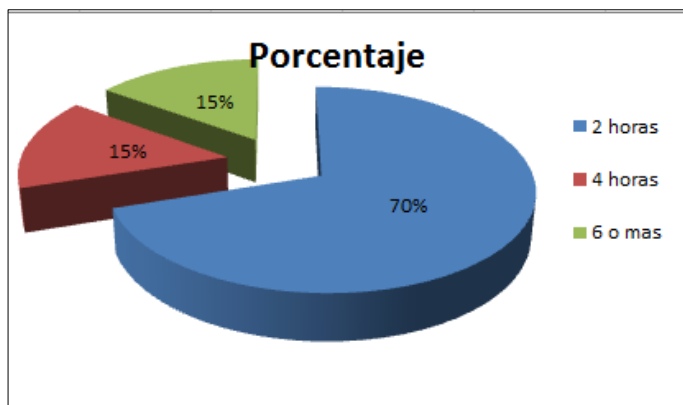


Figura 4.2. Grafica de resultados de la encuesta pregunta 2

Análisis e interpretación de la pregunta 2.

La encuesta reveló que un 70% de los usuarios hacen uso lo que podría saturarlo si la cantidad total de usuarios lo se conectan al mismo tiempo.

Pregunta # 3

¿Qué tipo de contenido web suele visitar cuando tiene acceso a internet?

Objetivo: Determinar si la conexión a internet es la adecuada para el tipo de información que solicitan los usuarios.

Tabla 4.3 Tabla de resultados acerca del tipo de contenido que visitan los usuarios.

Alternativas	Frecuencia	Porcentaje
Información en forma de texto	21	32.30%
YouTube	24	36.92%
Facebook	7	10.76%
Aula Virtual	5	7.69%
Documentos PDF	6	9.23%
Todas las anteriores	2	3.07%
Todas	65	100%

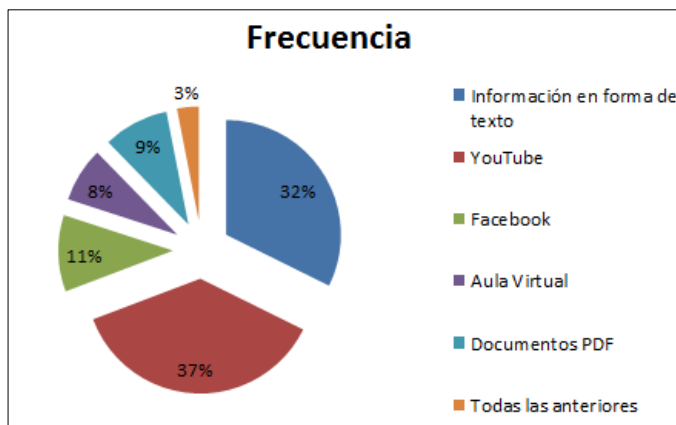


Figura 4.3. Grafica que muestra el tipo de contenido que visitan los usuarios

Análisis e interpretación de la pregunta 3

Se pudo comprobar que la mayor incidencia en la solicitud de información no se requiere de una conexión a internet de mayor ancho de banda y que las computadoras son capaces de interpretar y reproducir la información que es solicitada. Esto debido a que la información que los usuarios solicitan constantemente proviene de aplicaciones para el uso de internet (navegador web y sus complementos) que requieren de pocas exigencias en hardware.

Pregunta # 4

¿En sus clases puede compartir archivos mediante la red?

Objetivo: Determinar si hay un sistema operativo servidor que permita compartir archivos y carpetas a profesores, administrativos y alumnos.

Tabla 4.4. Tabla de resultados pregunta 4

Alternativas	Frecuencia	Porcentaje
Si	4	10%
No	36	90%
Total	40	100%

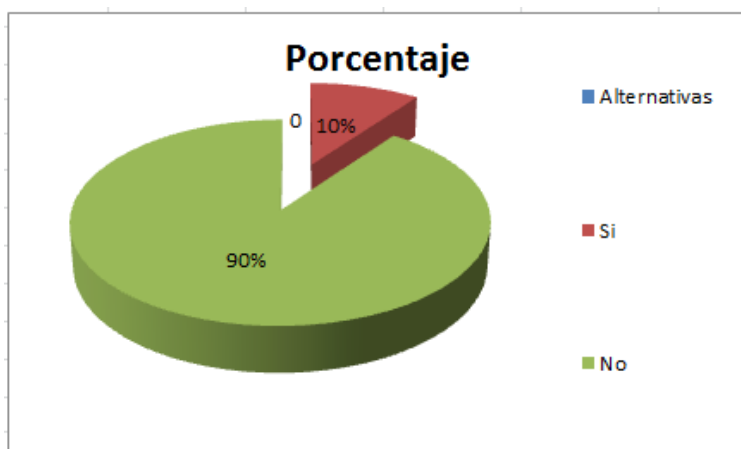


Figura 4.4. Grafico que denota que no hay servicio de compartir archivos

Análisis e interpretación de la pregunta 4.

Según lo que revelan los datos de la encuesta se pudo comprobar que no existe la opción de compartir archivos mediante la red o no hay una sistema de red que proporcione este servicio.

Pregunta # 5

¿Qué cree que debe mejorar el aula informática para trabajar adecuadamente?

Objetivo: Determinar la prioridad de los problemas de la infraestructura de red informática.

Tabla 4.5. Tabla de resultados sobre qué aspectos mejorar en la red.

Alternativas	Frecuencia	Porcentaje
Computadoras más rápidas	23	57.5%
Internet con mayor ancho de banda	8	20%
La conexión a internet	28	70%
Total	40	100%

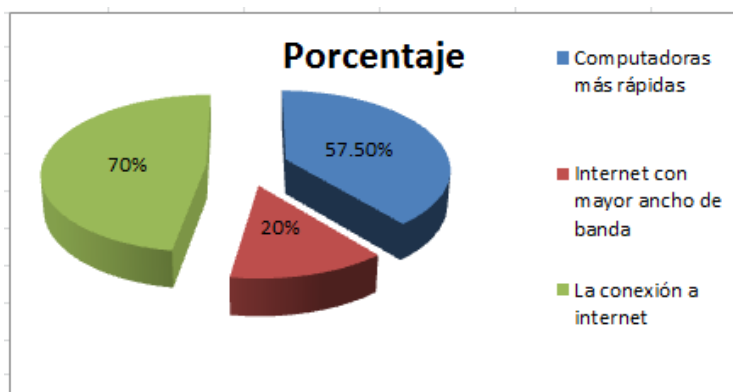


Figura 4.5 Gráfico que muestra la inestabilidad en la red como prioridad alta.

Análisis e interpretación de la pregunta 5.

Debido a que la pregunta era de alternativa múltiple los resultados reflejan que muchos usuarios opinaron que hay más de un problema relacionado a la infraestructura de la red informática.

Se logra comprobar que la mayor prioridad recae sobre la forma como se conectan las computadoras a la red, debido a que la conexión a internet suele fallar mucho.

Pregunta # 6 ¿Posee la escuela servicio de internet inalámbrico?

Objetivo: Determinar si la red inalámbrica es utilizada o no debido al desconocimiento de que este servicio de red se está servicio prestando.

Tabla 4.6 Tabla de resultados

Alternativas	Frecuencia	Porcentaje
Si	37	92.5%
No	0	0%
No se	3	7.5%
Total	40	100%

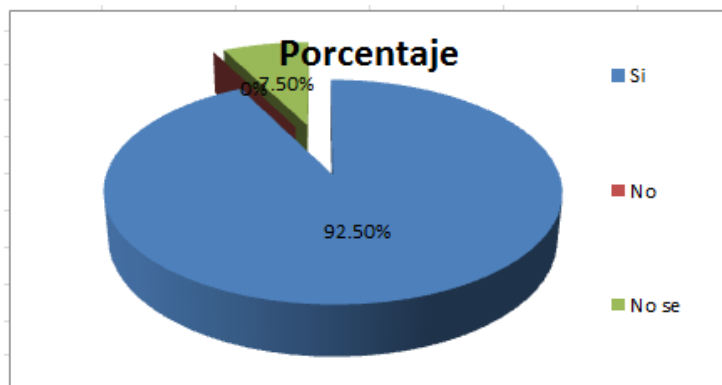


Figura 4.6. Grafico que muestra que si hay conocimiento de la red inalámbrica.

Análisis e interpretación de la pregunta 6.

Se logró demostrar que si se tiene conocimiento de la existencia del servicio de internet inalámbrico, lo que significa que su uso depende únicamente de la necesidad de los usuarios.

Pregunta # 7 ¿Usted tiene acceso a la red inalámbrica?

Objetivo: Determinar si el acceso a la red inalámbrica tiene un uso frecuente y así saber la prioridad que pudiera tener con respecto a los problemas relacionados a la infraestructura de red informática.

Tabla 4.7 Tabla de resultados sobre el acceso de usuarios a la red inalámbrica.

Alternativas	Frecuencia	Porcentaje
Si	25	62.5%
No	15	37.5%
No se	0	0%
Total	40	100%

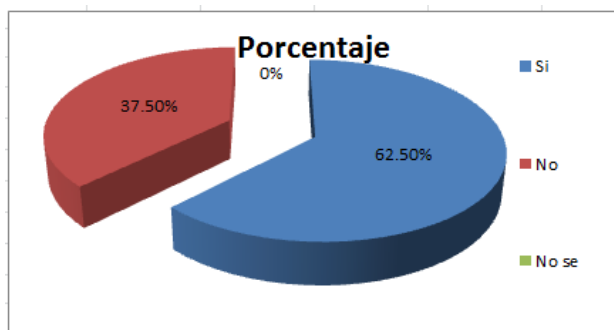


Figura 4.7. Grafico que muestra el porcentaje de usuario que tiene acceso a la red inalámbrica.

Análisis e interpretación de la pregunta 7.

Datos revelan que aunque hay un uso frecuente de la red inalámbrica, existe un gran porcentaje de usuarios que aunque saben que la red inalámbrica está funcionando, no hacen uso de ella por diferentes razones.

Pregunta # 8 ¿Con que frecuencia se conecta a la red inalámbrica?

Objetivo: Determinar cuál es valor que tiene la red inalámbrica en las actividades diarias de los usuarios del centro escolar.

Tabla 4.8. Tabla de resultados sobre la frecuencia con que usuarios usan la red inalámbrica

Alternativas	Frecuencia	Porcentaje
A veces	27	67.5%
Siempre	3	7.5%
Casi siempre	1	2.5%
Nunca	11	27.5%
Total	40	100%

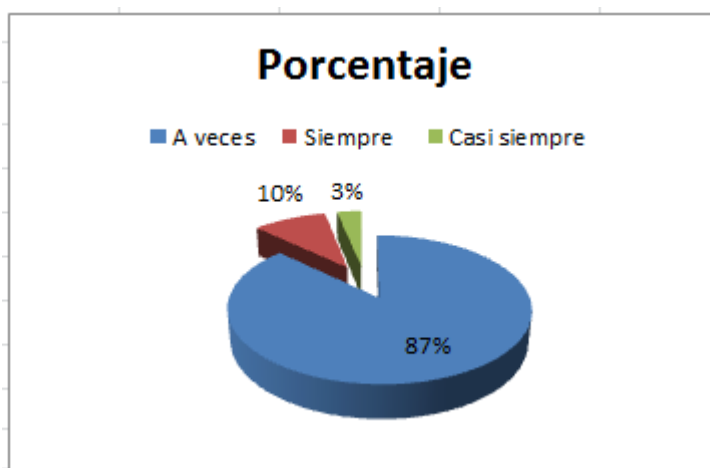


Figura 4.8. Grafico que muestra la frecuencia con que usuarios usan la red inalámbrica

Análisis e interpretación de la pregunta 8.

Se encontró que tomando en cuenta el porcentaje de los que la usan la red inalámbrica con frecuencia se llega a la conclusión de que un fallo en esta afectaría considerablemente.

Pregunta # 9

¿Qué tipo de dispositivo utiliza para conectarse a la red inalámbrica?

Objetivo: Determinar si hay equipos informáticos necesarios para el uso de este servicio.

Tabla 4.9. Tabla de resultados acerca del tipo de dispositivo informático con que usuarios se conectan a la red.

Alternativas	Frecuencia	Porcentaje
Computadora	19	47.5%
Laptop	5	12.5%
Celular Inteligente	15	37.5%
Total	40	100%

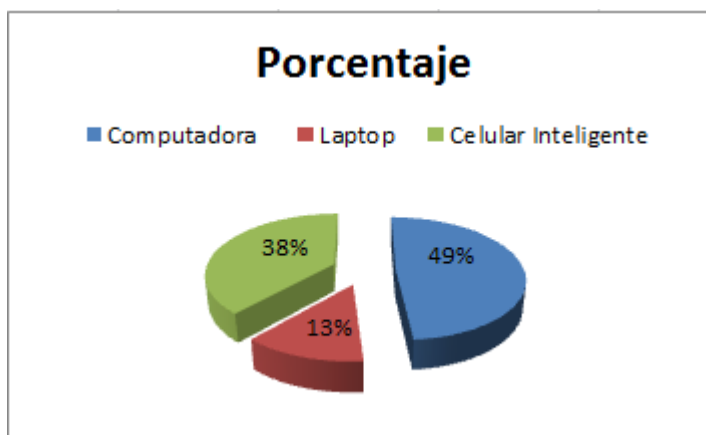


Figura 4.9. Grafico que muestra el resultado sobre qué equipo informático es más utilizado para conectarse a la red.

Análisis e interpretación de la pregunta 9.

Se determinó que la mayor parte de los equipos informáticos que hacen uso de la red inalámbrica lo conforman las laptop y los celulares inteligentes, por lo que se tiene la certeza de que múltiples usuarios hacen uso de la red constantemente.

Pregunta # 10 ¿Para qué fin utiliza la red inalámbrica?

Objetivo: Determinar el tipo de contenido al que tienen acceso los usuarios cuando hacen uso del internet que se comparte por conexión inalámbrica.

Tabla 4.10 Tabla de resultados acerca del uso que se le da a la red inalámbrica.

Alternativas	Frecuencia	Porcentaje
Investigar tareas	37	69.81%
Jugar o ver videos	7	13.20%
Utilizar las redes sociales	9	16.985%
Total	53	100%

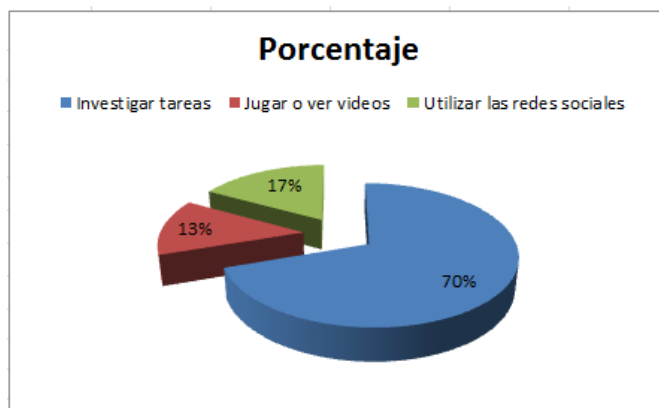


Figura 4.10. Gráfico que muestra la finalidad con que usuarios utilizan el recurso de red.

Análisis e interpretación de la pregunta 10.

Los resultados demuestran que una gran mayoría de los usuarios utilizan la red inalámbrica para los fines que el Centro Escolar estableció. Pero también hay bastante

demanda de usuarios que visitan las redes sociales y poco ocio. Es decir el uso de la red inalámbrica es justificable según los resultados de arrojo la encuesta.

2. Hallazgos de los resultados.

- 1- Mediante la encuesta se pudo verificar que uno de los problemas de mayor prioridad es inestabilidad de la conexión inalámbrica y el ancho de banda limitado, lo cual no permite a los usuarios realizar sus actividades de forma adecuada dando como resultado un uso ineficiente del recurso. El problema anterior se comprobó que no se debe al estado de los equipos, ya que estos se encuentran en buen estado, más bien se debe a sus configuraciones que no son las correctas. Para solucionar dicho problema se deben implementar las configuraciones adecuadas para hacer un reparto correcto del ancho de banda igual para cada dispositivo.
- 2- Se comprobó también mediante la encuesta que la mayoría de los usuarios que hacen uso del recurso de internet en la comunidad educativa lo utilizan para observar videos en YouTube, lo cual podría llegar a saturar el ancho de banda si se planean actividades simultáneas con alumnos. Otro factor que se determinó mediante la encuesta es la necesidad de implementación del filtrado de contenido web, para tener un mayor control sobre lo que los usuarios están viendo o haciendo, más que todo en sus horas clases, después queda a disposición del administrador de la red el dejar libre el acceso a internet.
- 3- A través de la entrevista realizada al encargado del Aula Informática, se pudo determinar que a pesar de que hay planes para para implementar medidas de seguridad a la infraestructura de red, esta no se puede efectuar debido a la falta de

recursos. Esta manifiesta que las autoridades de la institución tienen poca visión para invertir en este rubro.

4- Otro hallazgo significativo que se logró determinar mediante esta entrevista es que actualmente la infraestructura de red no posee un filtro de datos, por lo que no hay un control del contenido al que tienen acceso los usuarios.

5- Se pudo determinar por medio de la observación que la zona interna del aula informática está construida de acuerdo a las normas:

- ANSI/TIA/EIA-568-B,
- ANSI/TIA/EIA-569,
- ANSI/TIA/EIA-606

. Sin embargo las extensiones de red que van hacia los otros salones no poseen ninguna norma del cableado estructurado por lo que son considerados como puntos débiles de la red.

6- La infraestructura de red inalámbrica actual no tiene el alcance necesario para repartir la señal hacia todos los puntos necesarios de la institución.

3. Propuesta de Solución

Para intentar solventar los problemas de la red informática actual se ha dividido la propuesta de solución en tres aspectos.

- Creación de un diseño de infraestructura de red que resuelva los problemas actuales.
- Instalar un servidor que cuente con filtrado de contenido web
- Configurar dos dispositivo router WLAN.
- Establecer bases para la seguridad física.

3.1 Diseño de infraestructura de red

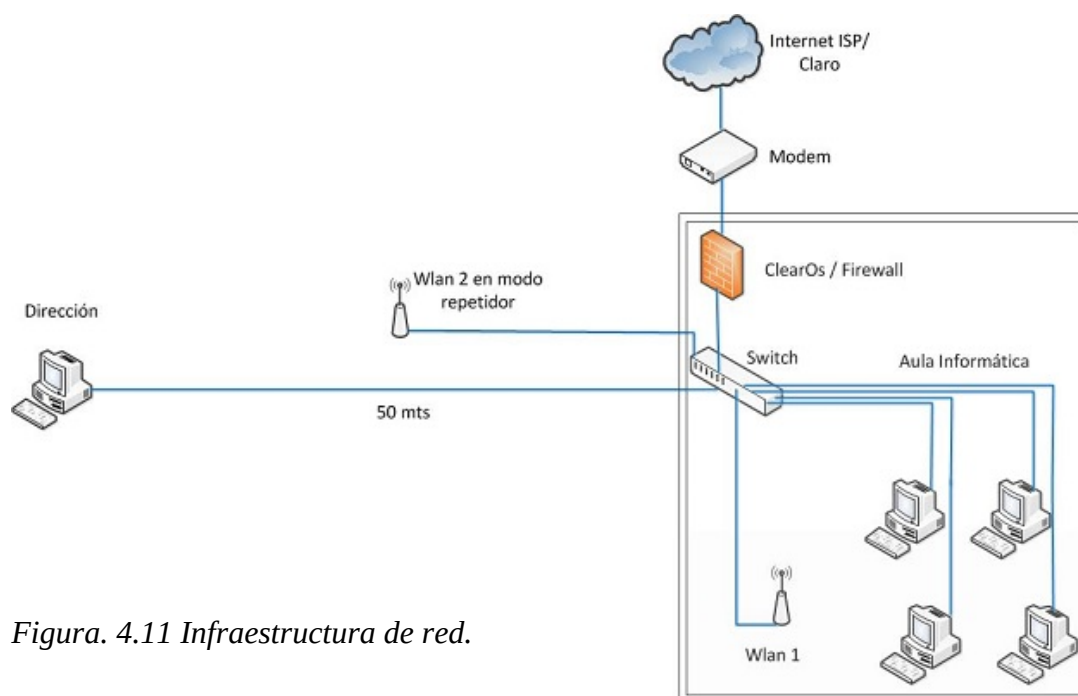


Figura. 4.11 Infraestructura de red.

Descripción de Hardware requerido

Computadora	x86 o 64 bit
Memoria / RAM	4 GB Recomendado
Disco Duro	500 GB Recomendado
Tarjeta de red	Ethernet integrada
Tarjeta de red	Ethernet adicional

3.2 Instalación y configuración de Clear Os 6.4

1. Requisitos de hardware.

Los requisitos de hardware mínimos para la instalación, recomendados son las siguientes:

Sistema Base	
Procesador / CPU	32 o 64 bit
Memoria / RAM	1 GB Recomendado
Disco Duro	10 GB Recomendado
Red	Ethernet, Cable, DSL

Los siguientes son requerimientos para estimar el hardware adecuado para el sistema. Teniendo en cuenta como se utilice el sistema.

RAM y CPU	5 Usuarios	5-25	25-50	50-250	250 +
		Usuarios	Usuarios	Usuarios	Usuarios
Procesador / CPU	Baja Capacidad	Básico	Dual-Core	Quad-Core	Multi-Core
Memoria / RAM	1 -2 GB	2 – 4 GB	4 – 8 GB	8 – 16 GB	16 – 32 GB
Disco Duro					
Disco Duro	10 GB como mínimo.				
RAID	No para este caso				

Los módulos que requieren más recursos son:

- Intrusion Detection and Prevention (Detección de Intrusos y Prevención)
- Content Filtering (Filtrado de Contenido)
- Antispam
- Antivirus

2. Instalación de sistema.

Una vez insertado el CD, nos mostrara el asistente de instalación de Clear OS, el cual nos guiara en todo el proceso.

- 2.1. Como primer paso nos mostrara la siguiente ventana en la cual daremos **Enter** y continuara con el proceso.



- 2.2. La instalación de este sistema se realiza en entorno gráfico y muy amigable.

En esta pantalla inicia el proceso de configuración para la instalación. Y seleccionares **Next**.

- 2.3. Seleccionaremos el Idioma para el proceso de Instalación. En el cual buscaremos **Spanish (Español)** y daremos clic **Next**.

- 2.4. Seleccionamos el tipo de teclado a utilizar. **Siguiente**

2.5. Definiremos el nombre de equipo, “**svrvarios**”. **Siguiente.**



2.6. En esta etapa indicaremos que tipo de dispositivo de almacenamiento tenemos. En el cual podemos seleccionar dispositivos de almacenamientos comunes o especializados. **Siguiente**

2.7. Seleccionaremos la zona horaria. **Siguiente.**

2.8. Digitaremos la contraseña para root (usuario administrador)
colocamos “**Pa55w0rd**”. **Siguiente.**

2.9. Mostrará cómo queremos configurar nuestro Disco Duro con respecto a Particiones.

Siguiente

¿Qué tipo de instalación desea?

☒ **Usar todo el espacio**
Elimina todas las particiones en los dispositivos seleccionados. Esto incluye las particiones creadas por otros sistemas operativos.
Consejo: Esta opción eliminará los datos de los dispositivos seleccionados. Asegúrese de hacer copias de seguridad.

☐ **Remplazar sistema(s) Linux existente(s)**
Elimina sólo las particiones Linux (creadas desde una instalación previa de Linux). Esto no elimina otras particiones que tenga en sus dispositivos de almacenamiento (tales como VFAT o FAT32).
Consejo: Esta opción eliminará los datos de los dispositivos seleccionados. Asegúrese de hacer copias de seguridad.

☐ **Achicar el sistema Actual**
Achica las particiones existentes para dar campo al diseño predeterminado.

☐ **Usar el espacio libre**
Mantiene sus datos actuales y particiones, y usa solamente el espacio no particionado en los dispositivos seleccionados, asumiendo que hay espacio libre suficiente.

☐ **Crear un diseño personalizado.**
Crear manualmente su propio diseño en los dispositivos seleccionados usando nuestra herramienta de particionamiento.

☐ Sistema de Encriptado
☒ Revisar y modificar el diseño de particiones

[← Atrás](#) [→ Siguiente](#)

Utilizar todo el espacio: Seleccionamos esta opción ya que no existirá ningún arreglo RAID. Esta opción también asume que ClearOS no está compartiendo el disco duro con otros sistemas operativos.

2.10. Una vez seleccionado lo anterior, nos mostrara un resumen de la tabla de particiones. **Siguiente.**

Por favor seleccione un dispositivo

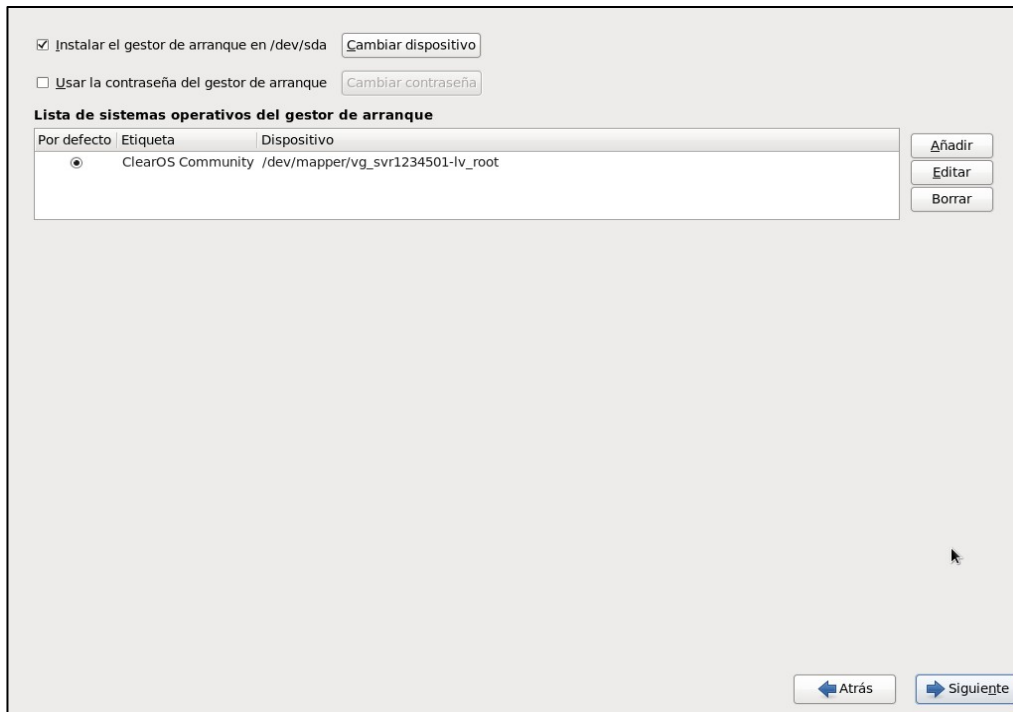
Dispositivo	Tamaño (MB)	Punto de Montaje/ RAID/Volumen	Tipo	Formato
Grupos de volumen LVM				
vg_svr1234501	19976			
lv_root	15912	/	ext4	✓
lv_swap	4064		swap	✓
Discos duros				
sda (/dev/sda)				
sda1	500	/boot	ext4	✓
sda2	19979	vg_svr1234501	physical volume (LVM)	✓

Una vez que demos **Siguiente**, nos mostrara una advertencia sobre los cambios hechos a las particiones del disco duro, si estamos seguros de los cambios. Seleccionaremos **Escribir cambios al disco**.

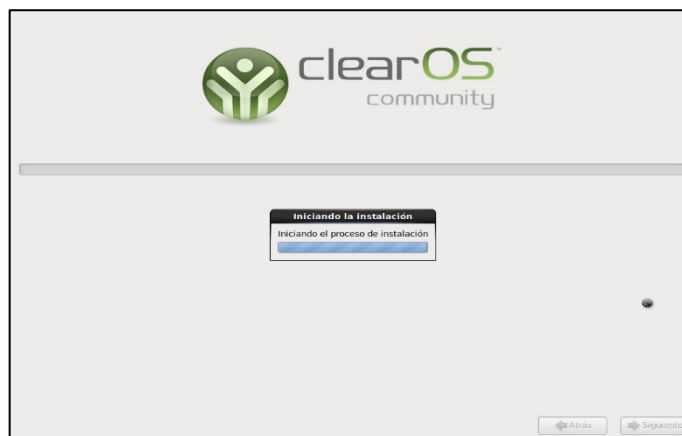
Escribiendo la configuración de almacenamiento en el

 Las opciones de particionamiento que ha seleccionado, se escribirán ahora en el disco. Cualquier dato en particiones borradas o reformateadas se perderán.

2.11. En esta pantalla nos muestra en donde se instalara el gestor de arranque, en el cual haremos clic en **Siguiente**.



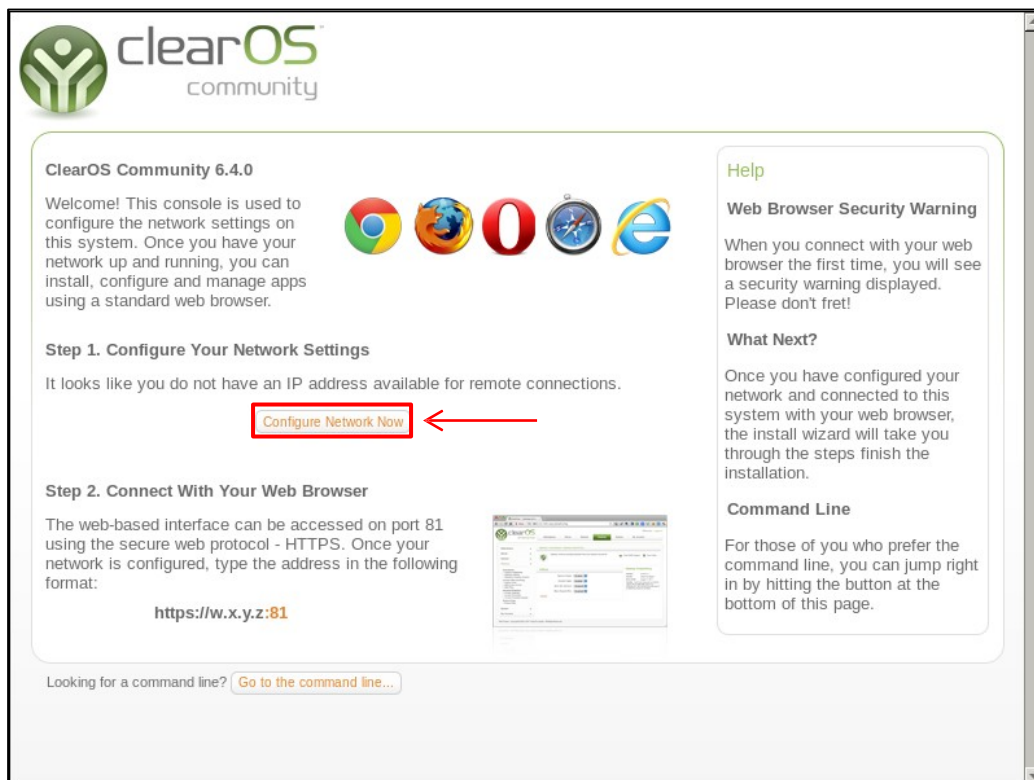
2.12. Con esto termina la configuración, por lo que inicia el proceso de instalación.



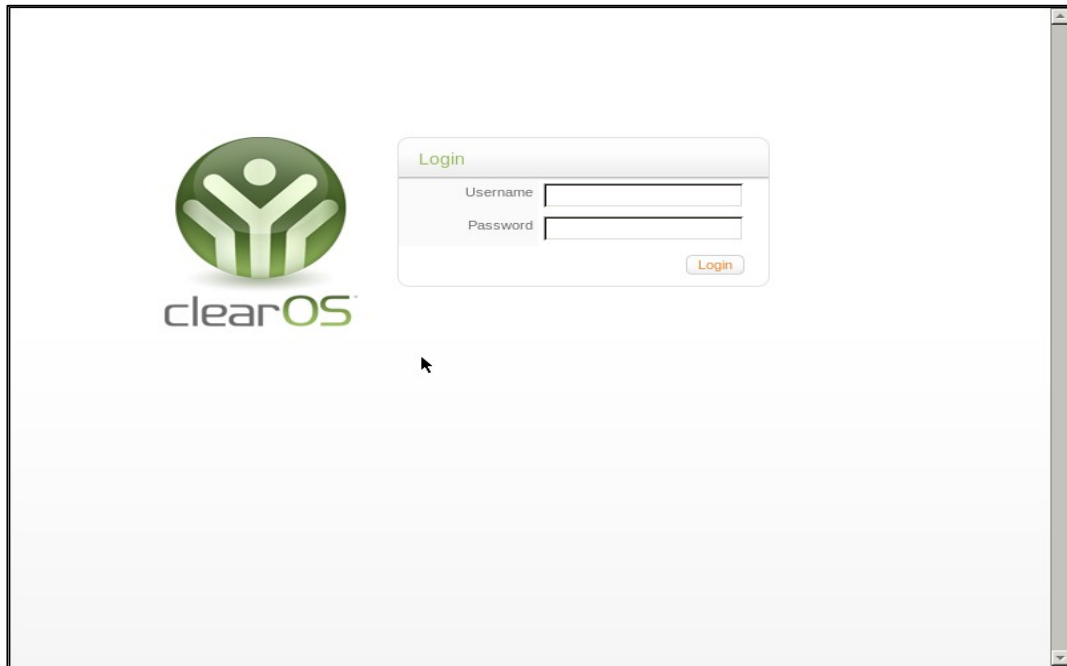
Una vez terminada la instalación nos mostrara la ventana de instalación completa, y el equipo se reiniciara.

2.13 Cuando el equipo vuelva a iniciar nos mostrara la siguiente ventana. Y
Seleccionaremos

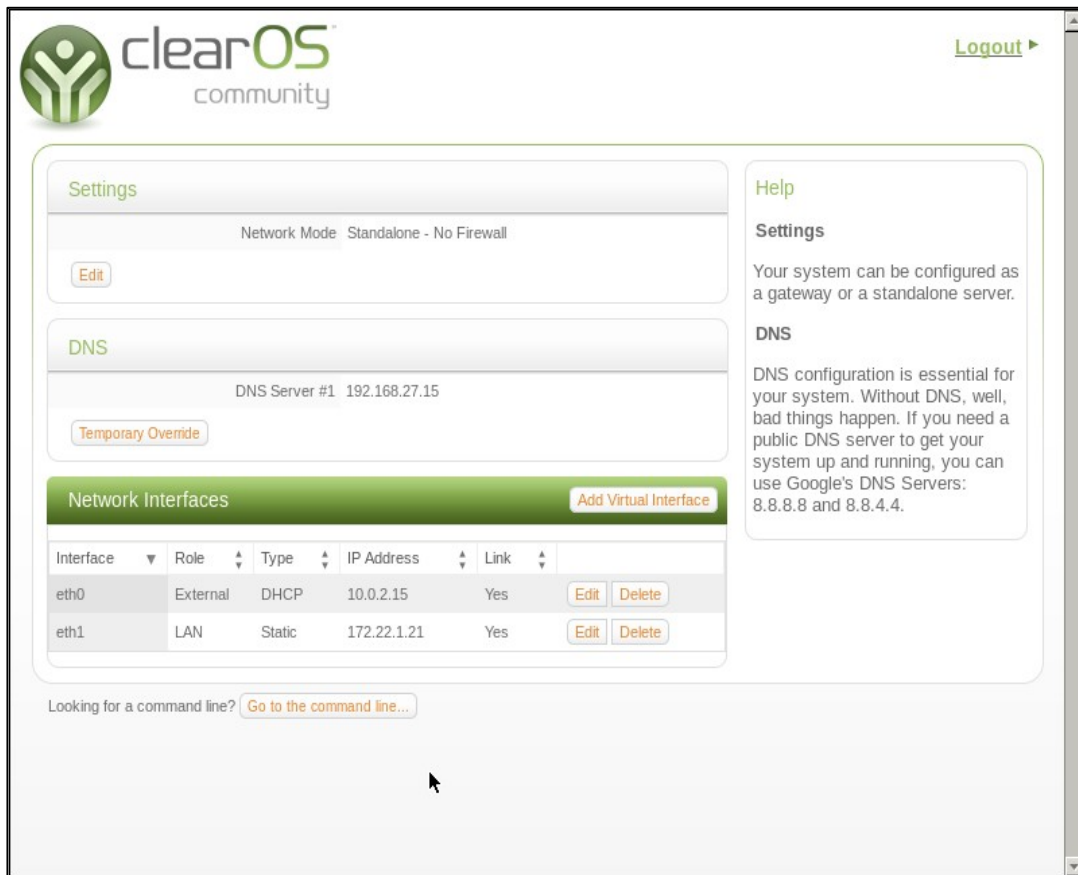
Configure Network Console



2.14 Una vez que demos clic nos solicitara un usuario y contraseña, para este sistema el usuario administrador es **root** y la contraseña que se coloca es **Pa55w0rd**.



2.15 Una vez iniciada la sesión, nos mostrara la única pantalla que podemos ver en el equipo que se ha instalado, en el cual configuraremos las conexiones de red (LAN, Internet).



En la imagen la tarjeta eth0 es la que nos proporcionara el acceso a internet, por lo que se configura el rol como External y el tipo, para este caso DHCP.

Y la tarjeta eth1 será la que se configurara en la red LAN con el tipo de rol LAN y por medio de

Estático. Y la IP que se configura es: IP 172.22.1.21 con MASCARA DE RED: 255.255.255.0

Y se define que la tarjeta de red integrada del equipo se configurara como red LAN y la tarjeta de red PCI se configurara para que brinde el acceso a Internet.

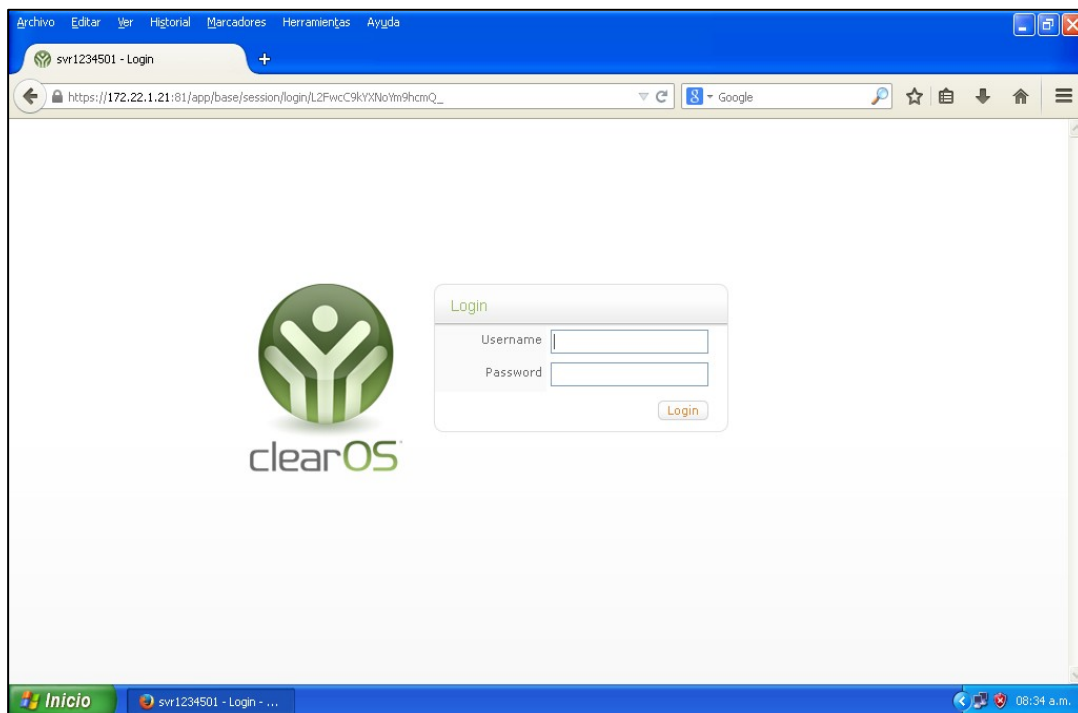
Proceso de instalación de servicios desde un equipo cliente.

Para esto necesitamos verificar que nuestro equipo tenga una IP del mismo rango que nuestro servidor.

Instalación de servicios

El proceso de instalación se realizara a través del navegador web, una vez que iniciamos cualquiera de los navegadores (En el ejemplo se desarrolló con Firefox) digitamos la dirección URL:

<https://172.22.1.21:81>



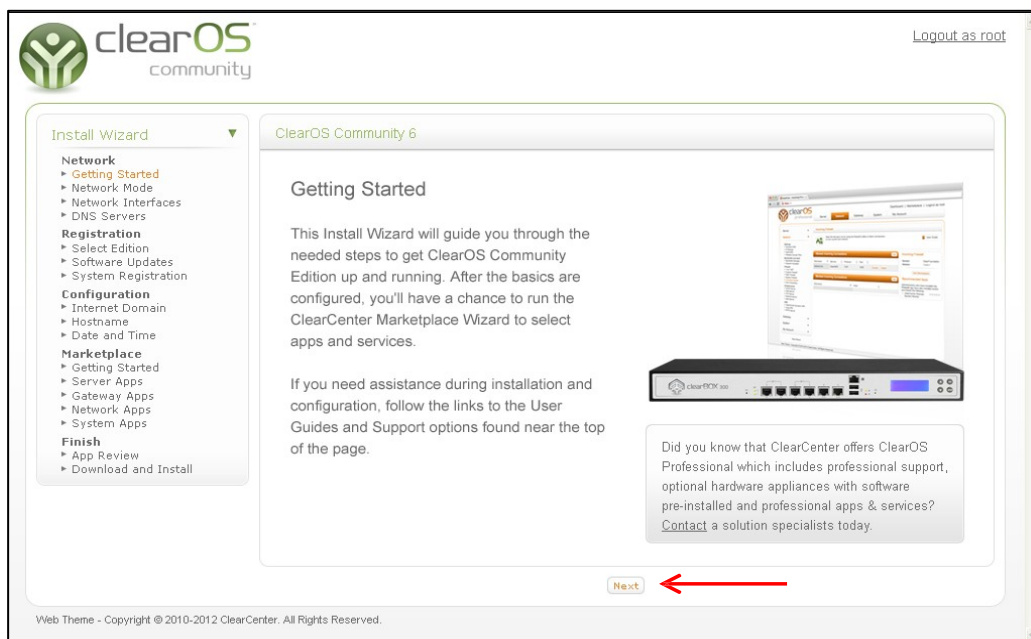
El resultado de digitar la URL será la pantalla de inicio de sesión de Clear OS en el cual las credenciales son:

Username: **root**

Password: **Pa55w0rd**

3.1 Cuando iniciemos sesión la instalación continuara, y nos mostrara el asistente.

Next



3.2 El Sistema Operativo, muestra 3 Opciones:

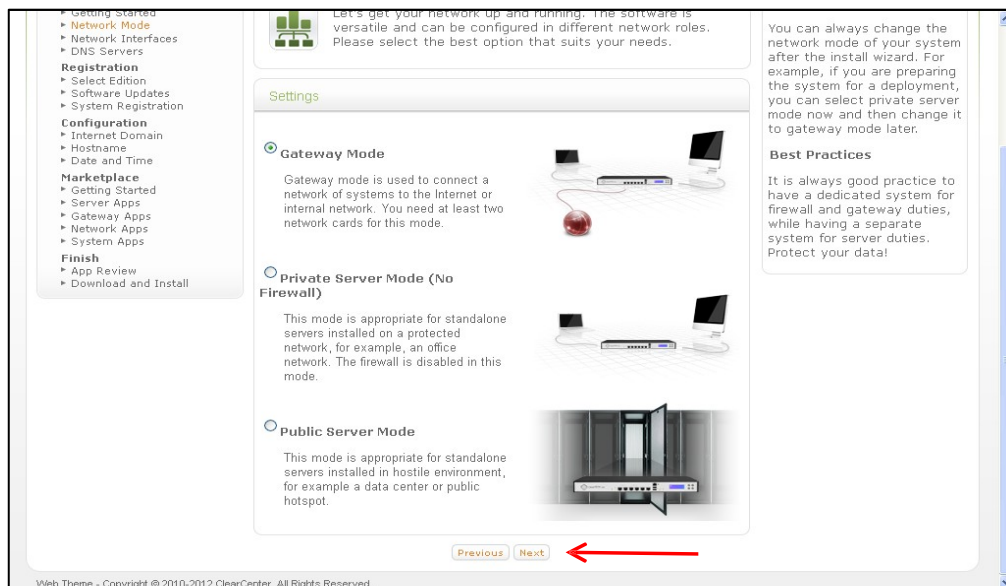
Gateway Mode: Este modo es utilizado para unir tu Red Local con Internet. Para esto el equipo necesita 2 tarjetas de Red.

Private Server Mode (No Firewall): Este modo es apropiado para el servidor independiente instalado en una red protegida, por ejemplo, una red de oficina. El

firewall está desactivado en este modo

Public Server Name: Este modo es adecuado para servidor independiente instalado en ambiente hostil, por ejemplo, un centro de datos o punto de acceso público

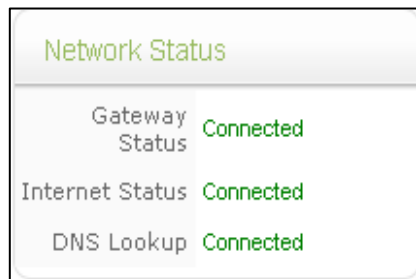
Para este caso seleccionaremos Gateway Mode. **Next**



3.3 En esta pantalla nos mostrara las configuraciones que hemos realizada

a las tarjetas de red, en el cual en la parte de la parte de la derecha hace un test con respecto al enlace de Internet, en el cual no tiene que dar ningún error para poder continuar.

Si el test que realiza muestra que esta todo correcto daremos clic en **Next**.



3.4 Y ahora realizara la comprobación del DNS, por lo que también se podrán realizar cambios y Clear realizar la comprobación. Y así como en el paso anterior no tiene que dar ningún error para poder seguir. Si no hubo errores **Next**

Performing DNS Test

DNS lookup succeeded!

[Previous](#) [Next](#)

Network Status

Gateway Status	Connected
Internet Status	Connected
DNS Lookup	Connected

3.5 Ya configurada nuestras tarjetas de Red, nos mostrara las versiones de Clear OS que podemos instalar en el cual se encuentra.

clearOS[™]
community

Logout as root

Install Wizard

Network

Getting Started

Network Mode

Network Interfaces

DNS Servers

Registration

Select Edition

Software Updates

System Registration

Configuration

Internet Domain

Hostname

Date and Time

Marketplace

Getting Started

Server Apps

Gateway Apps

Network Apps

System Apps

Finish

App Review

Download and Install

Select Edition

Thank You for Choosing ClearOS

ClearOS Community Edition is supported by a community of volunteers donating their time and knowledge via the ClearFoundation. This support model may not be the best solution for your business or organisation. Please consider all factors (technical skill, number of users, data sensitivity, resources etc.) when considering using ClearOS Community Edition in a commercial, professional, educational or large-scale deployment.

ClearCenter offers a commercially supported version of ClearOS called ClearOS Professional Edition. If you would like to upgrade to a 30-day evaluation of ClearOS Professional Edition, please select this option.

clearOS[™]
community

Install ClearOS Community

clearOS[™]
professional

Install and Evaluate ClearOS Professional

Previous

Next

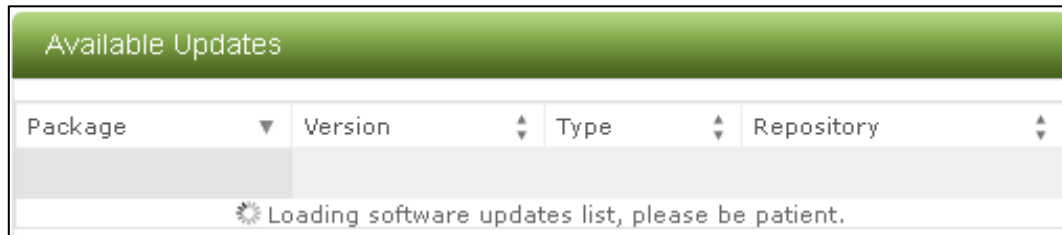
Web Theme - Copyright © 2010-2012 ClearCenter. All Rights Reserved.

Seleccionaremos la versión Community, ya que esta es una versión gratuita. **Next**

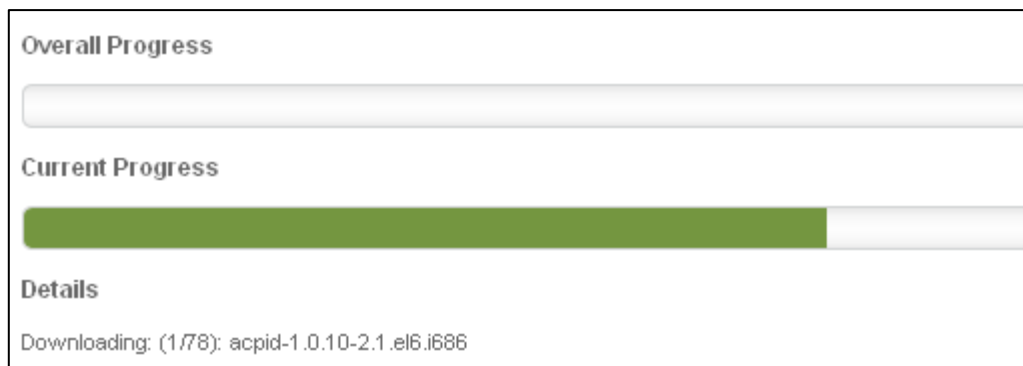
3.6 El siguiente paso es la actualización del sistema, en donde realiza la búsqueda

54

y nos mostrara el listado de las actualizaciones disponibles. Una vez que la búsqueda termina **Next**.



3.7 La instalación de las actualizaciones iniciara, y este tiempo tardar según el enlace de Internet que se posea. Mostrará una barra de estado de la descarga así como de la instalación.



Cuando la descarga e instalación finalice nos mostrara la siguiente pantalla. **Next**

Overall Progress

Current Progress

Details

Installation complete.

Previous Next

3.8 Cuando Clear OS termine la actualización de Sistema, nos solicitara registrarlo, y nos solicitara un usuario de la cuenta y su respectiva contraseña.

Siendo así el usuario o Account (ClearCenter): **utec2016**

Contraseña: **Pa55w0rd**

System Registration

Account (ClearCenter) utec2016

Password

Type New Install

System Name svrvarios

Environment Education

Terms of Service By clicking **Register System**, you agree to the [Terms of Service](#).

Register System Refresh Form Create Account

Una vez que se llenaron todos los campos requeridos, daremos clic en “**Register**

System” e iniciara el proceso de registro, al finalizar nos mostrara el resumen de dicho registro.

System Registration	
Status	Registered
Account	utec2016
System Name	svrvarios
External Hostname/IP	svr100z66z805.poweredbyclear.com
Hostkey	9eef8720a6aa2a6717eef15c82dffa32
Software End-of-Life	August 31, 2017

3.9 El siguiente paso es configurar el dominio, el cual tiene el nombre de **mined.edu.sv**. **Next**

Settings	
Domain	mined.edu.sv

3.10 Nos solicitara un nombre de equipo, al que solo se le agregara **“.local”**. **Next**

Settings	
Hostname	svrvarios.local
Internet Hostname	svrvarios.local

3.11 Si la hora y fecha no están correctas en este paso se puede sincronizar. **Next**

Settings

Date

Sep 17 2014

Time

09:01:45 CST

Time Zone

America/El Salvador

Automatic Synchronize

Enabled

Synchronize Now

3.12 En esta etapa seleccionaremos los servicios que se descargarán e instalarán en nuestro equipo. Estos pasos los haremos a través de **MarketPlace** la cual es una herramienta de Clear OS.

Nos mostrará como queremos filtrar los servicios disponibles, para una mejor visualización de dichos servicios seleccionaremos que los filtre por categoría.

Install Apps by Function

If you are new to ClearOS or prefer to configure the system by specific tasks (eg. prevent users from accessing certain websites, share files between users etc.), select this option.

Quick Select File

ClearCenter and the ClearFoundation community have a wide selection of pre-configured templates that will quickly get you up and running.

Install Apps by Category

Displays groups of apps based on a category classification system used in the main menu. If you are familiar with basic networking/server terms and familiar with the ClearOS Marketplace, select this option.

Skip App Install Wizard

Skip the Marketplace wizard. You can install apps at any time by navigating to the Marketplace.

Haremos clic en **Next**.

3.13 Nos mostrará un filtro por categoría de los cuales seleccionaremos:

App Selection

Select All

Cloud

Gateway

Server

Network

System

Reports

Cloud



Gateway

Server



Network



System



Reports



3.14 Una vez seleccionados los paquetes a instalar nos mostrara el listado completo, en el cual si estamos de acuerdo daremos clic a “**Download and Install**” e iniciar el proceso.

App Install List

Delete All

Download and Install

100

Q

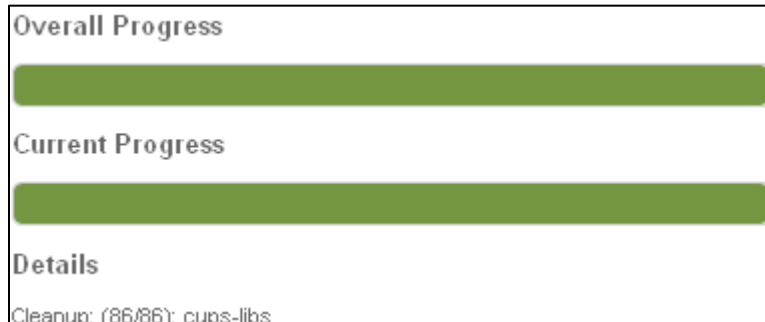
Description	Price	Unit	Discount	Extended	EULA	
Administrators	Free		---	\$ 0.00	None	Delete
Content Filter	Free		---	\$ 0.00	None	Delete
Directory Server	Free		---	\$ 0.00	None	Delete
Dynamic DNS	Free	yr	---	\$ 0.00	None	Delete
Filter and Proxy Report	Free		---	\$ 0.00	None	Delete
Flexshares	Free		---	\$ 0.00	None	Delete
Network Map	Free		---	\$ 0.00	None	Delete
Password Policies	Free		---	\$ 0.00	None	Delete
Print Server	Free		---	\$ 0.00	None	Delete
Web Access Control	Free		---	\$ 0.00	None	Delete
Web Proxy	Free		---	\$ 0.00	None	Delete
Windows Networking	Free		---	\$ 0.00	None	Delete

Overall Progress

Current Progress

Details

Updating repositories and preparing package dependencies... this may take a few minutes.

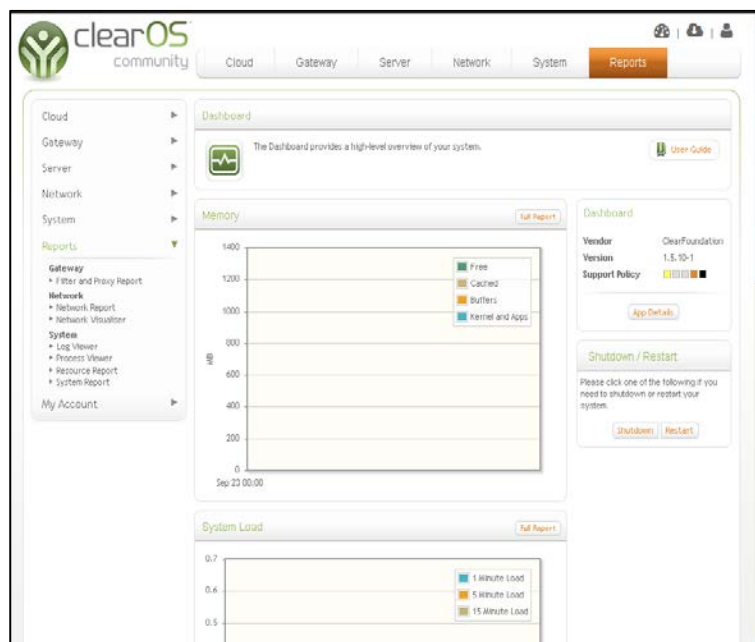


Una vez terminado el proceso daremos clic en **“Finish Install Wizard”**.

Con este paso el proceso de Instalación ha terminado.

Configuración de Servicios

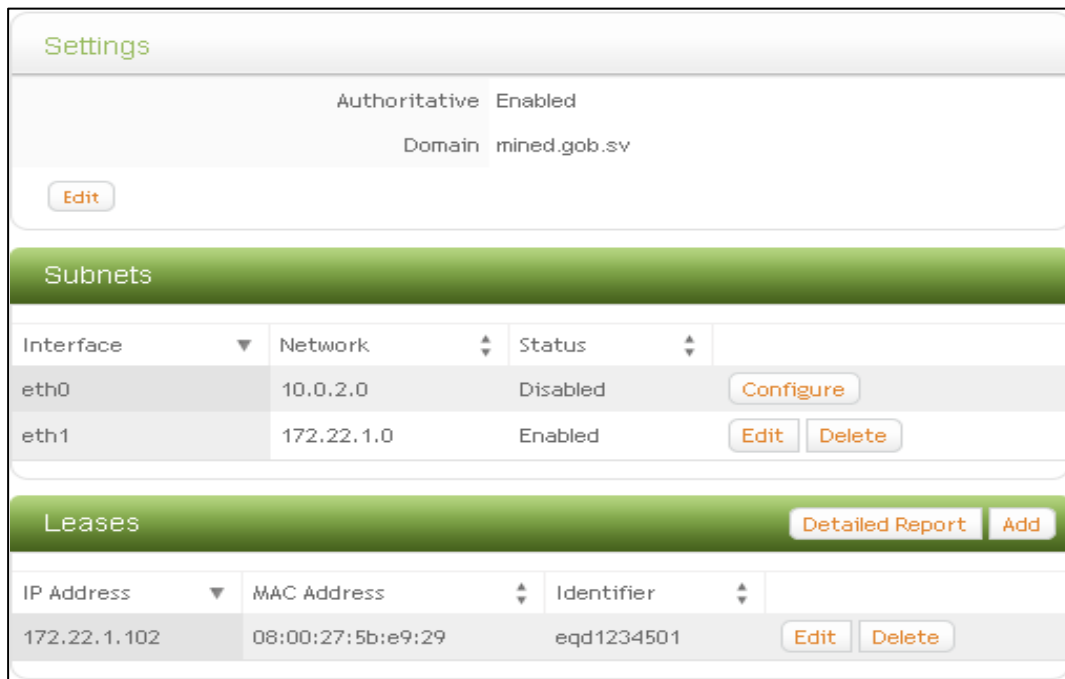
En esta etapa configuraremos los servicios que descargamos. Y nos mostrara el menú completo de Clear OS en el cual encontraremos gráficos del flujo de datos, así como también características de nuestro equipo.



En esta pantalla además encontraremos los botones de apagar o reiniciar el equipo.

4.1 Comenzaremos con configurar con el servicio DHCP, y para eso nos ubicaremos en el menú

Network | DHCP Server.



Settings			
Authoritative	Enabled		
Domain	mined.gob.sv		
Edit			

Subnets			
Interface	Network	Status	
eth0	10.0.2.0	Disabled	Configure
eth1	172.22.1.0	Enabled	Edit Delete

Leases			Detailed Report	Add
IP Address	MAC Address	Identifier		
172.22.1.102	08:00:27:5b:e9:29	eqd1234501	Edit	Delete

Para que este servicio funcione correctamente, es necesario que el único que este Habilitado sea el de nuestra tarjeta de red configurada para LAN, así como aparece en el ejemplo.

4.2 El siguiente servicio a configurar es el Dominio, esta configuración se encuentra en

Server | Directory Server.

En el cual le pondremos **mined.edu.sv** e **Initialize**.

Settings

Mode	Standalone
Base Domain	mined.edu.sv
Publish Policy	Not Published ▼

Initialize

Cuando el proceso termine, nos mostrara el resumen de dicha configuración.

Settings

Mode	Standalone
Base Domain	mined.edu.sv
Publish Policy	Not Published

Edit

Directory Information

Capabilities

Mode	Standalone
------	------------

Connection Information

Base DN	dc=mined,dc=edu,dc=sv
Bind DN	cn=manager,ou=Internal,dc=mined,dc=edu,dc=sv
Bind Password	Ad/b87dpZ73E1ave

Containers

Users	ou=Users,ou=Accounts,dc=mined,dc=edu,dc=sv
Groups	ou=Groups,ou=Accounts,dc=mined,dc=edu,dc=sv
Computers	ou=Computers,ou=Accounts,dc=mined,dc=edu,dc=sv

4.3 Configuraremos el dominio para Windows para esto vamos a **Server |**

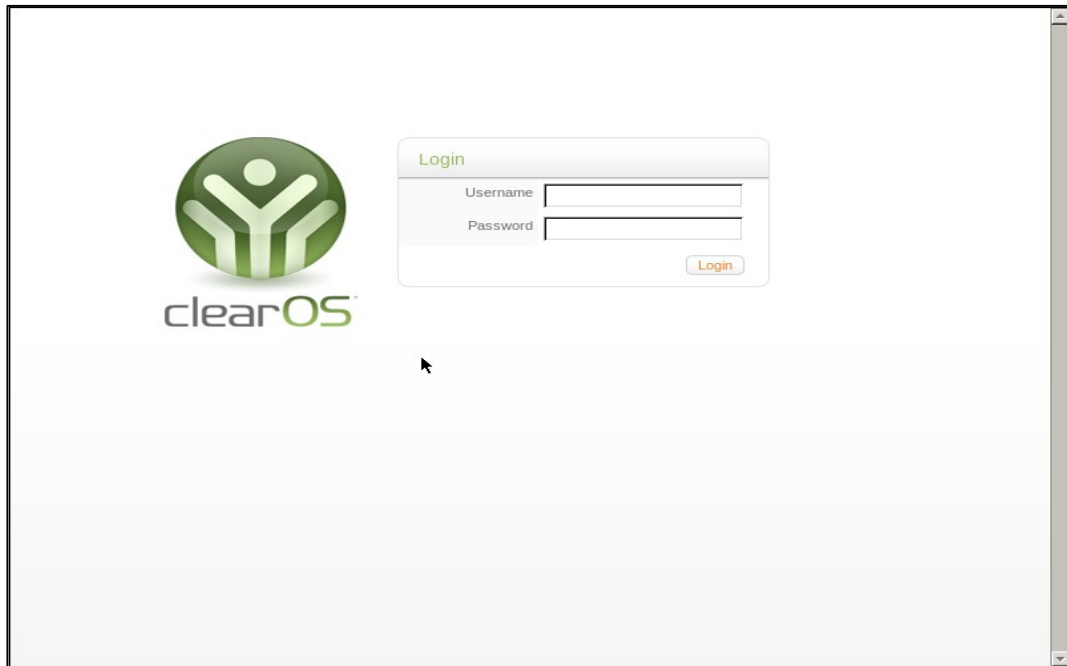
Windows Networking

Y nos solicitara:

Server Name: **svrvarios**.

Windows Domain: **ce11830**

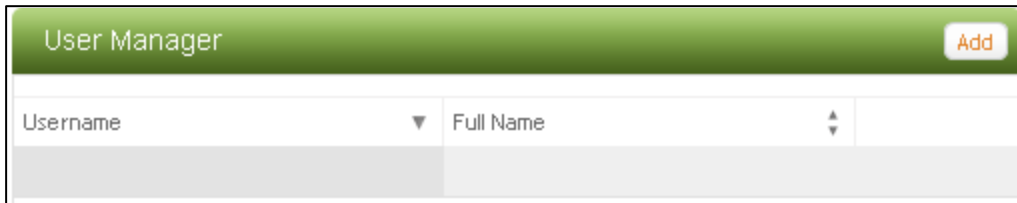
Contraseña para usuario Winadmin: **Pa55w0rd**



Ya lleno el formulario daremos clic **Initialize**. Y nos mostrara el resumen de la configuración.

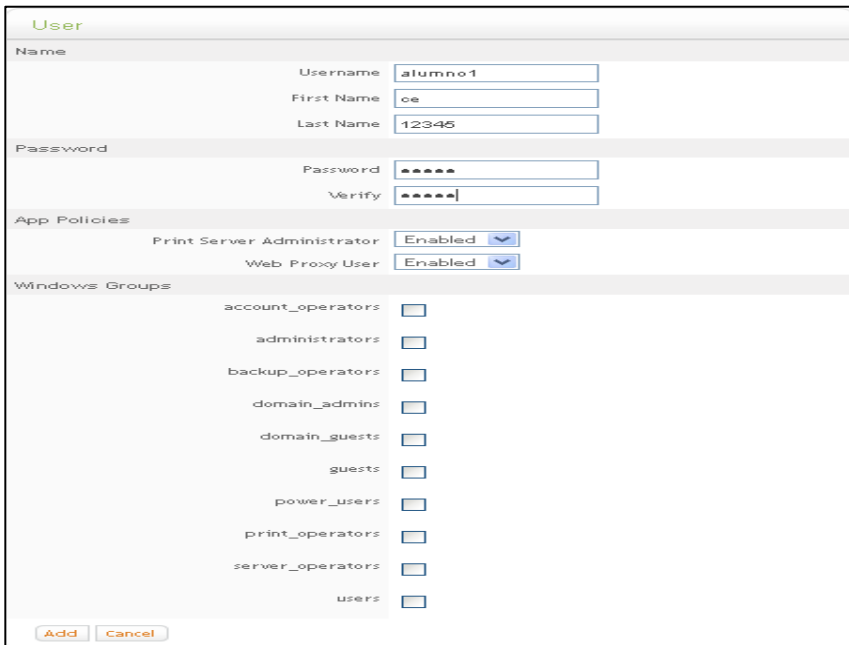
4.4 Ahora crearemos los usuarios, para esto nos dirigimos a **System | Users**

Y daremos clic en **Add** para agregar el usuario.



The image shows a 'User Manager' interface. At the top, there is a green header bar with the text 'User Manager' and an 'Add' button. Below the header is a table with two columns: 'Username' and 'Full Name'. The table is currently empty, and there is a grey bar at the bottom.

Nos mostrara un formulario, en donde nos solicita el nombre del usuario, contraseña y los servicios que tendrá acceso



The image shows a 'User' creation form. It has several sections: 'Name' with fields for Username (alumno1), First Name (oe), and Last Name (12345); 'Password' with fields for Password (masked with dots) and Verify (masked with dots); 'App Policies' with checkboxes for 'Print Server Administrator' and 'Web Proxy User', both set to 'Enabled'; and 'Windows Groups' with a list of groups (account_operators, administrators, backup_operators, domain_admins, domain_guests, guests, power_users, print_operators, server_operators, users) and checkboxes for each. At the bottom, there are 'Add' and 'Cancel' buttons.

Las configuraciones hechas en el ejemplo son los estándares de Ministerio de Educación.

User Manager		Add
Username ▼	Full Name ▲▼	
alumno1	ce 12345	Edit Delete

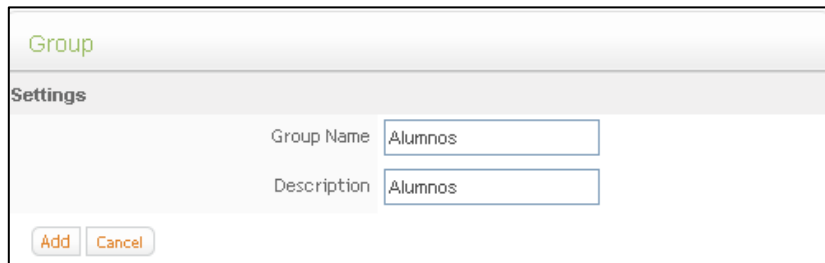
4.5 Ahora crearemos el grupo para los usuarios creados. Y para esto nos ubicamos

System | Groups

Daremos clic en el botón **Add** para crear nuestro grupo. En esta pantalla nos muestra los grupos que están creados por defecto del Sistema.

User Defined Groups		Add
Group ▼		
Windows Groups		
Group ▼		
account_operators	Edit Members Edit	
administrators	Edit Members Edit	
backup_operators	Edit Members Edit	
domain_admins	Edit Members Edit	
domain_guests	Edit Members Edit	
guests	Edit Members Edit	
power_users	Edit Members Edit	
print_operators	Edit Members Edit	
server_operators	Edit Members Edit	
users	Edit Members Edit	
Built-in Groups		
Group ▼		
allusers	View Members View	

Nos solicitara un nombre para el grupo así como una descripción.



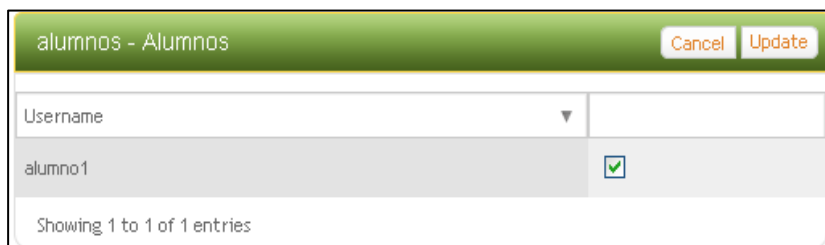
Group

Settings

Group Name

Description

Cuando llenemos los campos y damos clic en **Add**, nos preguntara que usuarios formaran parte de este grupo, para lo que seleccionaremos el usuario **alumno1**.



alumnos - Alumnos

Username	
alumno1	☒

Showing 1 to 1 of 1 entries

4.6 Configuración de Web Proxy, para esto vamos a **Gateway | Web Proxy**

Este servicio se encuentra detenido, por lo que el primer paso será iniciarlo para ello nos ubicamos en la parte derecha de la configuración. En donde nos aparece un recuadro, ya ubicado damos clic en el botón **Start**

Web Proxy

Vendor	ClearFoundation
Version	1.5.11-1
Support Policy	☐ ☐ ☐ ☒ ☐
Status	Stopped
Action	Start

Ahora configuraremos el modo en que trabajara nuestro proxy, en la pantalla principal en la parte

Settings daremos clic en **Edit**

Settings

Transparent Mode	Enabled
User Authentication	Disabled
Performance Level	Home Network

Edit

Cache

Maximum Cache Size	10 GB
Maximum Object Size	500 MB
Maximum File Download Size	Unlimited

Edit

Reset Cache

Web Proxy Bypass

Add

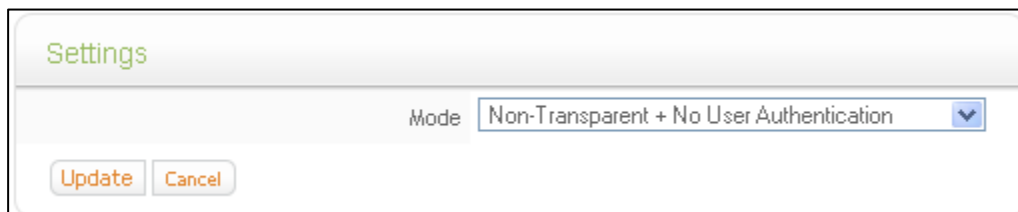
Nickname	Network Address
----------	-----------------

App Policies

Policy Name	Group
Web Proxy User	web_proxy_plugin

Edit Members

En esta parte solo configuraremos el modo, en el cual seleccionaremos: **Non-Transparent + Not User Authentication**, y daremos clic en **Update**.

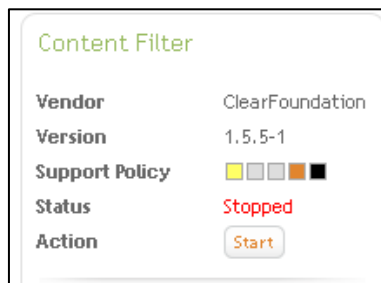


4.7 Ahora configuraremos el **Filtrado de Contenido o Content Filter** el cual está ubicado

Gateway | Content Filter.

Al igual que Web Proxy este servicio está detenido, por eso iniciaremos el servicio, dando clic en

Start



Ya iniciado el servicio podemos configurar el Filtrado de Contenido. Para eso nos ubicamos en la parte inferior en el módulo **App Policies**

App Policies			Add
Policy Name	Group		
Default	-		Configure Policy

Y daremos clic en **Configure Policy** en donde encontraremos lo que podemos filtrar en base a configuraciones generales, por frase, por MIME, Extensión de Archivos, Sitios Bloqueados.

Policy - Default		Return to Summary
General Settings		Edit
Blacklists		Edit
Phrase Lists		Edit
MIME Types		Edit
File Extensions		Edit
Banned Sites		Edit
Gray Sites		Edit
Exception Sites		Edit

En donde para bloquear una página específica como por ejemplo

“www.facebook.com”

Seleccionaremos la opción **“Banned Sites”**

Site

Y nos mostrara un listado de los sitios que podemos que podemos agregar para el bloqueo. Seleccionamos **Add**

Site: facebook.com

Add Cancel

Ya en esta parte nos solicitara colocar el sitio, basta en colocar **“Facebook.com”** para que bloquee las páginas que contengan ese nombre en la URL. Y seleccionamos **Add**.

Site
facebook.com

Delete

Ya agregada la página Web que vamos a bloquear, los cambios los hace casi inmediatos y en una pc cliente lo que se va a observar en el navegador será una advertencia Clear OS.



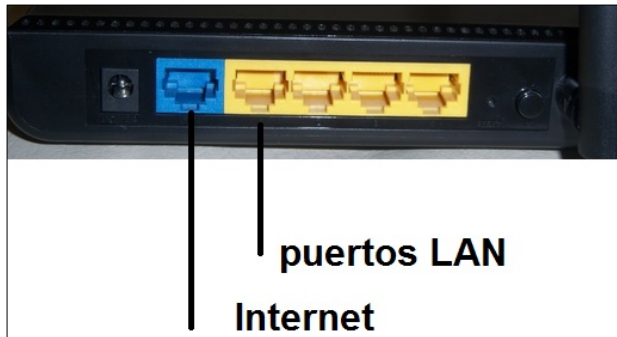
Red inalámbrica

Para este caso se sugiere colocar 2 dispositivos inalámbricos, uno que funcione como router y el otro que haga la función de puente. Ambos equipos son de la marca NEXXT, esto debido a que es el hardware con que la institución cuenta.

A continuación se muestran las configuraciones posibles para una correcta gestión de la red inalámbrica.

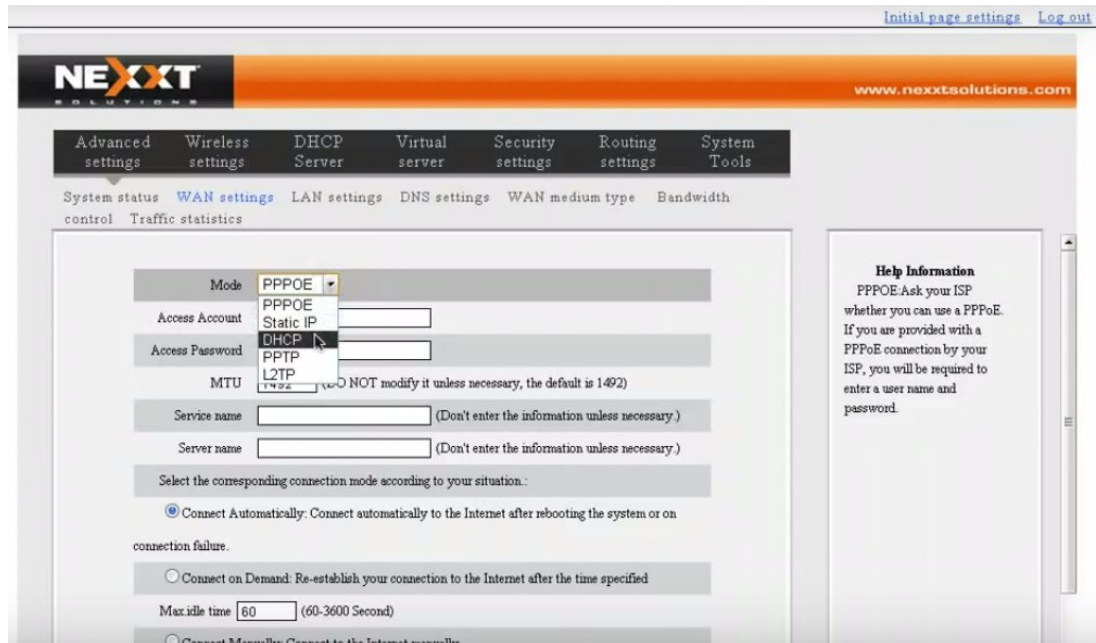
Configuración para Router Principal

Lo primero que debemos hacer es conectar el router a nuestra computadora en cualquiera de los puertos LAN.



Ahora en nuestra computadora abrimos el navegador de Internet y escribimos en la barra de direcciones la dirección de IP del router "192.168.0.1" por defecto y escribimos "admin" (son así por defecto en los router de la marca NEXXT) como Usuario y contraseña. Debemos asegurarnos que nuestro router está configurado en modo Router para posteriormente configurar un segundo router en modo repetidor.

En la opción WAN setting seleccionamos la forma como obtenemos la señal de nuestro proveedor de internet, para este caso la dejamos en modo DHCP.



En “**LAN settings**”, cambiamos la direccion IP del router para evitar que este dentro de la misma tabla dinámica de dirección IP del modem de la empresa Claro y que este pueda tomar por defecto. Para este caso usaremos **192.168.1.1**

En la opción “**WLAN settings - Basic Settings**”, hacemos los ajustes básicos para la conexión Wireless tales como la SSID (para este caso será **CESABP**), canales y canales de extensión. Damos clic en Presione “**Apply**” para salvar los cambios.

[Initial page settings](#) [Log out](#)



www.nexxtsolutions.com

Advanced settings
Wireless settings
DHCP Server
Virtual server
Security settings
Routing settings
System Tools

Wireless Basic Settings
Wireless Security
Access Control
Connection Status

☒ Enable wireless function

Wireless Working Mode ☒ Wireless Access Point (AP) ☐ Network Bridge (WDS)

Network Mode 11b/g/n mixed mode

primary SSID CESABP

secondary SSID

Broadcast(SSID) ☒ Enable ☐ Disable

AP Isolation ☐ Enable ☒ Disable

Channel 2437MHz (Channel 6)

WMM Capable ☒ Enable ☐ Disable

APSD Capable ☐ Enable ☒ Disable

Channel Bandwidth ☐ 20 ☒ 20/40

Extension Channel 2417MHz (Channel 2)

Help information

You only need to set the basic wireless information on this page. It is suggested that you only change the SSID and channel, and keep the other items at their default settings.

SSID is the network name shared by all the devices in the wireless network.

When the wireless clients search for the wireless networks to connect to in the area, they detect the SSID broadcast via the router. If selected, the router will broadcast its SSID to all wireless hosts.

You can select Auto-select mode, or any of the 11 available channels. Try to select the channels with less

Ahora en "**WLAN settings – Wireless Security**", Seleccionamos como modo de seguridad la opción WPA2-PSK. Y como contraseña xaby5087. Luego de eso damos clic en OK

[Initial page settings](#) [Log](#)



www.nexxtsolutions.com

Advanced settings
Wireless settings
DHCP Server
Virtual server
Security settings
Routing settings
System Tools

Wireless Basic Settings
Wireless Security
Access Control
Connection Status

Security Mode WPA2 - PSK

WPA Algorithms ☐ AES ☒ TKIP ☐ TKIP&AES

Key xaby5087

Key Renewal Interval 3600 Second

WPS Settings ☒ Disable ☐ Enable

Reset OOB

Note: Wireless Security Settings

802.11n standard only defines Open-None (Disable), WPA personal-AES, and WPA2 personal-AES

sure that your wireless client supports this encryption method. If you are not familiar with security modes, it is suggested that you use WPA-personal. Otherwise, you can select any security mode as long as your wireless client also supports it.

Configuración del Router como Repetidor

En "WLAN Settings - WDS settings", debemos seleccionar el modo WDS a trabajar. Para este caso tenemos las opciones "Repeater" o "Bridge". El modo "Bridge" solo brindara acceso LAN mas no Wireless. Por eso seleccionamos el modo el modo "Repeater" para expandir el rango de la señal de la red Wireless y brindar acceso por conexion LAN).

Colocamos la misma contraseña para WDS que usamos en el router principal. Luego, agregamos en la tabla de direcciones MAC la direccion MAC de nuestro router principal. Presionamos "Apply" para salvar la configuración.

Ahora en la opción "DHCP Server y DHCP Server", desactivamos el servidor DHCP. Y hacemos clic en OK para guardar los cambios. Reiniciamos el router en "System Tools" en la opción de "Reboot router".

Seguridad Física

Debido a que la zona interna del aula informática cumple con las normas ANSI/TIA/EIA-568-B, las recomendaciones se basan únicamente en las zonas exteriores a esta

- Se recomienda que el cableado que va desde el Switch del aula informática y que recorre 50 mts hasta la dirección, debe ser protegido por medio de un tecno-ducto ya que está expuesto.
- Se recomienda colocar canaleta de 32x12.5 milímetros en la zona interna del aula Dirección para proteger el cableado.



- Se recomienda colocar una roseta doble a una altura de 15 cm (esta altura protegerá la roseta de posibles golpes o rasos).



- En la roseta que conectara desde el Switch del aula informática a la dirección debe estar sujeta bajo la norma ANSI/TIA/EIA-568-B del cableado estructurado.

Capítulo V

Conclusiones

La presente tesis tuvo como objetivo identificar los elementos claves que afectan la seguridad en la infraestructura de red del Centro Escolar en cuestión y con ello establecer bases para el diseño de una propuesta de mejoras.

Para demostrar esto, primero se realizó un análisis del uso actual que se le da a la red inalámbrica en el centro escolar mediante encuestas y entrevistas a docentes y alumnos. Pudiendo observar que la población que la utiliza está en aumento y a su vez demanda mejor estabilidad en el servicio y mayor seguridad inalámbrica para evitar que personas ajenas al centro escolar se conecten a la red.

En base a las debilidades encontradas en cuanto al control del contenido al que se tiene acceso vía internet se hizo una investigación acerca del software necesario para resolver esta problemática y se creó un cuadro comparativo de los diferentes sistemas operativos de red y saber cuál es la mejor opción y así generar una propuesta de mejora al diseño de la seguridad informática. El resultado determinó que el software adecuado y que cumple con la resolución de las necesidades es ClearOS, por ello se hizo la implementación de él para brindar un mejor servicio y a su vez incrementar la seguridad en la red.

El desarrollo e implementación de las mejoras no fue nada fácil ya que se presentaron muchas limitantes, una de las más difíciles fue que debido a nuestro presupuesto solo contamos con los recursos de red, equipos informáticos y servicio de

internet que tiene la institución en la actualidad, por ello se tuvo que adaptar las mejoras y las configuraciones a los equipos disponibles para mejorar el rendimiento, eficacia y seguridad de la red, sin aumentar los gastos de la institución.

Referencias

Centro de Apoyo Tecnológico a Emprendedores. (2011). *Análisis de aplicación:*

Cortafuegos de la distribución clearOS. Castilla, La Mancha. España

Centro Escolar San Bartolomé Perulapía. (2015). *Plan Escolar Anual*. San Bartolomé Perulapía. El Salvador.

ClearCenter. (2016). *ClearOs*. Recuperado de <https://www.clearos.com/>

Dyllan. (2009). *es.ccm.net*. Recuperado de <http://es.ccm.net/faq/2755-que-es-un-proxy>.

Free Software Foundation, Inc. (2016). *El Sistema Operativo GNU*. Recuperado de <https://gnu.org/>

Fulvio Ricciardi. (2015). *Zeroshell*. Recuperado de <http://www.zeroshell.org/>

Ramió, J. (2006). *Libro Electrónico de Seguridad Informática y Criptografía*. Mérida. España.

Madrid Molina, J. M. (2006). *Seguridad en redes inalámbricas 802.11. Sistemas y Telemática*. Recuperado de http://bibliotecadigital.icesi.edu.co/biblioteca_digital/handle/10906/400.

MicroCisco. (2009). *Fundamentos de WLAN Redes Inalámbricas*. Estados Unidos de Norteamérica.

Ríos, I. M. (2011). *Administración de Redes*. Recuperado de <http://redyseguridad.fi-p.unam.mx/pp/maru/labpracticass/Seguridad.pdf>.

Sánchez, G.B. (2012). *Máster Universitario en Software Libre*.
Recuperado de: <http://www.uoc.edu/masters/softwarelibre/esp/pdf/impresion.pdf>

Veites, Á. C. (2011). *Enciclopedia de la seguridad informática*. Alfa Omega Ra-Ma. España.

Anexos

Entrevista a encargado de informática del Centro escolar San Bartolomé Perulapía.

Nombre: Julio Eduardo López Larreynaga

Cargo: Encargado del centro de informática

1. ¿Existe algún plan para implementar medidas de seguridad a la infraestructura de red?

2. ¿Por qué es tan importante un firewall para la seguridad en la infraestructura de red?

3. ¿Cómo está diseñada la infraestructura de red informática en el centro escolar?

4. ¿Posee el centro escolar los recursos necesarios para implementar seguridad en la infraestructura de red?

5. ¿Considera que es importante filtrar el uso de contenido web para los alumnos?

6. ¿Qué tipo de hardware o software posee actualmente para el filtrado de contenido web?

7. ¿Poseen los alumnos acceso a internet mediante red inalámbrica?

8. ¿Qué tipo de seguridad posee actualmente la red inalámbrica del centro escolar?

9. ¿Cuenta el centro de informática con la seguridad física en sus instalaciones?

10. ¿Ha implementado alguna política de seguridad a los usuarios que tienen acceso a la red del centro escolar?

Encuesta dirigida a alumnos del
Centro Escolar San Bartolomé Perulapía
acerca del acceso a internet.

Marca con una sola X en los círculos sobre las respuestas y con más de una X en las preguntas cuya respuesta poseen casillas.

1. ¿Tiene acceso a internet en su escuela?

Sí ☐ No ☐ No Se ☐

2. ¿Cuántas horas a la semana hace uso del recurso de internet?

2 horas ☐ 4 horas ☐ 6 horas o más ☐

3. ¿Qué tipo de contenido web suele visitar cuando tiene acceso a internet?

Información en forma de texto ☐

YouTube ☐

Facebook ☐

Aula Virtual ☐

Documentos PDF ☐

Todas las anteriores ☐

4. ¿En sus clases puede compartir archivos mediante la red?

Sí ☐ No ☐ No Se ☐

5. ¿Qué cree que debe mejorar el aula informática para trabajar adecuadamente?

- Computadoras más rápidas ☐
- Internet con mayor ancho de banda ☐
- La conexión a internet ☐

6. ¿Posee la escuela servicio de internet inalámbrico?

Sí ☐ No ☐ No Se ☐

7. ¿Usted tiene acceso a la red inalámbrica?

Sí ☐ No ☐ No Se ☐

8. ¿Con que frecuencia se conecta a la red inalámbrica?

A veces ☐

Siempre ☐

Casi siempre ☐

Nunca ☐

9. ¿Qué tipo de dispositivo utiliza para conectarse a la red inalámbrica?

Computadora ☐

Laptop ☐

Celular Inteligente ☐

10. ¿Para qué fin utiliza la red inalámbrica?

Investigar tareas ☐

Jugar o ver videos ☐

Utilizar las redes sociales ☐

Presupuesto de la propuesta de mejora a la infraestructura de red

Cantidad	Descripción	Precio Unitario	Sub-total
50 mts	Tecno ducto	\$ 0.45	\$22.50
10 mts	Cable UTP	\$0.50	\$5.00
8 mts	Pliego de canaleta 32x12.5 milímetros	\$2.00	\$16.00
1	Tarjeta de red PCI	\$10.00	\$10.00
4	Roseta de red RJ45	\$2.5	\$10.00
1	Mano de obra de implementación	\$300.00	\$300.00
Total			\$363.50