UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

TEMA:

IMPLEMENTACIÓN DE UNA DISTRIBUCIÓN GNU/LINUX LSBS PARA LA AUTENTICACIÓN DE LOS USUARIOS Y LA SEGURIDAD DE LOS RECURSOS DE RED DE LA COOPERATIVA DE AHORRO Y CRÉDITO ESCENCIA INDÍGENA LTDA.

Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos

SUBLINEA DE INVESTIGACIÓN: Sistemas Administradores de Recursos

AUTOR: Luis Alberto Mungabusi Sisa

TUTOR: Ing. David Omar Guevara Aulestia, Mg.

Ambato - Ecuador

Enero, 2016

APROBACIÓN DEL TUTOR

En mi calidad de tutor del Trabajo de Investigación sobre el tema: **IMPLEMENTACIÓN DE UNA DISTRIBUCIÓN GNU/LINUX LSBS PARA LA AUTENTICACIÓN DE LOS USUARIOS Y LA SEGURIDAD DE LOS RECURSOS DE RED DE LA COOPERATIVA DE AHORRO Y CRÉDITO ESCENCIA INDÍGENA LTDA**, del señor Luis Alberto Mungabusi Sisa, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el numeral 7.2 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ambato enero, 2016

EL TUTOR

Ing. David Guevara Aulestia, Mg.

AUTORÍA

El presente Proyecto de Investigación titulado: **IMPLEMENTACIÓN DE UNA DISTRIBUCIÓN GNU/LINUX LSBS PARA LA AUTENTICACIÓN DE LOS USUARIOS Y LA SEGURIDAD DE LOS RECURSOS DE RED DE LA COOPERATIVA DE AHORRO Y CRÉDITO ESCENCIA INDÍGENA LTDA**, es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato enero, 2016

Luis Alberto Mungabusi Sisa

CC: 1804783411

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad .

Ambato enero, 2016

Juan Gabriel Acosta Calderón

CC: 1803735289

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Juan Carlos Ruiz y Marcos Benitez, revisó y aprobó el Informe Final del Proyecto de Investigación titulado **IMPLEMENTACIÓN DE UNA DISTRIBUCIÓN GNU/LINUX LSBS PARA LA AUTENTICACIÓN DE LOS USUARIOS Y LA SEGURIDAD DE LOS RECURSOS DE RED DE LA COOPERATIVA DE AHORRO Y CRÉDITO ESCENCIA INDÍGENA LTDA**, presentado por el señor Luis Alberto Mungabusi Sisa de acuerdo al numeral 9.1 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ing. José Vicente Morales Lozada, Mg.

PRESIDENTE DEL TRIBUNAL

Ing. Juan Carlos Ruiz, Mg.
DOCENTE CALIFICADOR

Ing. Marcos Benitez A., Mg.
DOCENTE CALIFICADOR

DEDICATORIA

A Dios porque siempre guía nuestro camino para que hagamos el bien y contribuyamos en la sociedad, de manera muy especial a mis padres y hermano por el apoyo incondicional que me brindaron para la culminación de mi educación superior, ellos me enseñaron el valor de luchar por mis sueños y que nada es imposible si se lo desea con el corazón.

A esa persona especial que siempre permaneció a mi lado en todo momento a pesar de las adversidades de la vida.

Para todas aquellas personas que de una u otra manera me brindaron su apoyo moral y espiritual para la feliz culminación del presente proyecto de investigación.

Luis Alberto Mungabusi Sisa

AGRADECIMIENTO

A Dios quien siempre guía mi camino hacia el éxito, de la misma manera a mis padres quienes me apoyaron incondicionalmente hasta la culminación de mis estudios para llegar a la meta anhelada.
A mis profesores de la prestigiosa facultad de Ingeniería en Sistemas, Electrónica e Industrial quienes me brindaron su apoyo compartiendo sus experiencias profesionales.
A mi persona favorita quien siempre me brindó su apoyo incondicional a pesar de todas las circunstancias para que pueda alcanzar esta meta.
A las personas que conforman la institución financiera Escencia Indígena que me abrieron las puertas para la realización de mi proyecto de investigación.

Luis Alberto Mungabusi Sisa

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

La seguridad de los recursos de internos de la red se ha vuelto uno de los pilares fundamentales para que las entidades financieras que se mantienen el constante crecimiento, ya que si no existiese una seguridad de la información, cualquier ente externo podría acceder a la información importante para la misma; por esta razón las entidades financieras deben estar a la par de la tecnología a lo que a seguridad de la información se refiere, no solo para ser competitivas con otras similares sino por alcanzar los objetivos propuestos de la entidades mismas.

En tal virtud dada la importancia de la seguridad de la información que manejan diariamente la Cooperativa es fundamental la implementación de un mecanismo de seguridad informática que proteja toda la información interna de la red, para que así no se puedan generar pérdidas considerables para la Cooperativa.

La implementación de este proyecto permitirá que la información que se encuentra internamente en la red sea más segura, compartiendo los recursos solo a usuarios validos que se encuentran registrados como empleados de la COAC Escencia Indígena Ltda, así también la instalación de Servidor Proxy HTTP y Firewall que no permitirá el ingreso a páginas innecesarias para el trabajo diario.

ABSTRACT

The security of internal resources of the network has become one of the fundamental pillars for financial institutions remain steady growth, as if there were no security of information, any external body could access important information for the same; For this reason, financial institutions must keep pace with technology far as information security is concerned, not only to be competitive with other similar but to achieve the objectives of the same entities.

As such, it is given the importance of information security to manage the cooperative daily is essential to implement a security mechanism that protects all internal information network, so that not may generate substantial losses for the cooperative.

The implementation of this project will allow the information found internally in the network more secure, sharing resources only valid users who are registered as employees of the COAC. Escencia Indígena Ltda, so Server installation HTTP Proxy and Firewall will not allow entry to unnecessary pages for daily work.

INTRODUCCIÓN

Actualmente la seguridad de la información se ha vuelto uno de los pilares fundamentales para que las entidades financieras puedan permanecer en constante crecimiento en el mercado crediticio, por lo tanto, la seguridad y la tecnología deben ir de la mano para que las empresas puedan crecer de manera libre sin el temor a que su información sea sustraída por entes externos o internos a la institución, esta información solo pueden ser accedidas por las personas autorizadas de la institución. El presente artículo está enfocado a la seguridad de los recursos internos de la red que maneja la entidad financiera, por lo cual, se pretenderá realizar un análisis de soluciones GNU/Linux Small Business Server para posteriormente implementarlo, realizando un análisis de las diferentes distribuciones existentes en el mercado, dando como resultado una distribución que más se ajusta a los requerimientos de la entidad que posteriormente administrará de manera correcta los recursos internos de la red

Este proyecto de investigación está organizada en capítulos, las mismas que se detallan a continuación:

Capítulo 1, se expone el tema del proyecto de investigación, se realiza el planteamiento del problema, así como también la delimitación de la misma, conjuntamente con la justificación y los objetivos.

Capítulo 2, se presenta el marco teórico, donde se exponen los antecedentes investigativos, los diferentes conceptos relacionados al proyecto de investigación, que servirán como soporte para el desarrollo del mismo, definiendo de esta manera la propuesta de solución al problema planteado.

Capítulo 3, se describe la modalidad de la investigación, recolección y procesamiento de la información, así también, se describen los pasos a seguir para llegar a la solución del problema planteado.

Capítulo 4, se presenta detalladamente todos los pasos descritos en el capítulo anterior para lograr los objetivos propuestos en el presente proyecto de investigación.

Capítulo 5, se presentan las conclusiones y recomendaciones de este proyecto. Así mismo, las referencias bibliográficas utilizadas durante el desarrollo del proyecto y los anexos facilitados por la institución.

CAPÍTULO 1

El problema

1.1. Tema

Implementación de una distribución GNU/Linux LSBS para la autenticación de los usuarios y la seguridad de los recursos de red de la Cooperativa de Ahorro y Crédito Escencia Indígena Ltda.

1.2. Planteamiento del problema

A medida que el tiempo pasa se incrementa la importancia de la seguridad de la información corporativa por parte de las organizaciones e instituciones, ya que pueden llegar a tener éxito o fracaso por la información que manejan internamente, por lo tanto, se considera un activo valioso para la misma. La información confidencial lo manejan solamente los directivos y personal autorizado.

En la actualidad, la tecnología se ha convertido en uno de los factores más importantes en cuanto al uso institucional se refiere, produciendo cambios significativos en todas las instituciones financieras ya que tienen que sujetarse al cambio de la tecnología, para dar mayor protección a la información que manejan internamente.

La mayoría de las organizaciones están conectadas a una red informática, la cual les permite prestar sus servicios de una manera adecuada. El sistema interno maneja mucha información confidencial que solo le sirve a la organización, por lo tanto, está expuesta a un fraude de informático tanto por agentes externos o internos, por lo que la misma se ven en la necesidad de adquirir un sistema informático para proteger la información corporativa ante estas amenazas informáticas[1].

De la misma manera, que se vienen dando los avances tecnológicos como Internet, móviles, banda ancha, satélites, microondas y comunicaciones, se dan ataques a redes tanto públicas como privadas, no existen redes seguras sino redes fiables, aquellas que se supone responderá tal como el administrador lo espera, es decir que debe cumplir ciertas políticas de seguridad o directivas de grupo que no sean fácilmente vulneradas por entes externos a la institución[2].

El robo de información y actos que atentan a la institución, suelen darse de manera interna, por los mismos empleados o también por los ex empleados que fueron despedidos intempestivamente, dando así como resultado fraudes financieros que perjudica gravemente a la misma.

En la Cooperativa existe un alto porcentaje de deficiencia en la autenticación y seguridad de los recursos de red, los principales problemas son los siguientes:

- Servidor actual no permite el control adecuado de las políticas de seguridad.
- Autenticación de usuarios no autorizados para la manipulación de los equipos y recursos internos de la Cooperativa.
- Acceso libre a sitios web restringidos.
- Inconvenientes en el balanceo de carga y disponibilidad de la red.

Hoy en día, la Cooperativa de Ahorro y Crédito Escencia Indígena Ltda. han sido muy tolerantes con los empleados que han sido descubiertos usando Internet en asuntos no relacionados con su trabajo o en sitios web que podrían poner en riesgo a la misma.

1.3. Delimitación

Área Académica: Hardware y Redes.
Línea de Investigación: Sistemas Administradores de Recursos.
Sublíneas de investigación: Seguridad Informática.

Delimitación espacial

La presente investigación se realizará en la Cooperativa de Ahorro y Crédito Escencia Indígena Ltda. ubicada en la Av. Cevallos Y Eloy Alfaro, del cantón Ambato provincia de Tungurahua.

Delimitación temporal

La presente investigación se desarrollará en los seis meses posteriores a la aprobación del proyecto por parte del H. Concejo Directivo.

1.4. Justificación

Hoy en día, las Cooperativas de Ahorro y Crédito tienen un alto flujo de información que permite a la misma subsistir en el mercado laboral, de igual manera, tiene vulnerabilidad ante entes externos por la deficiencia en la autenticación y seguridad de los recursos de red, en tal razón, el presente proyecto es de gran interés, puesto que permitirá mejorar la autenticación de los usuarios y maximizar la seguridad de los recursos de red que maneja internamente la Cooperativa de Ahorro y Crédito Escencia Indígena y por ende permitirá a la misma prestar sus servicios de forma eficiente y rápida.

En la organización existe cierta información de uso confidencial para la institución financiera, que no se le puede dar a conocer a los subordinados, dicha información pueden ser accedidas solo por el personal autorizado como los ejecutivos de acuerdo al cargo que ocupe.

Los beneficiarios directos de este proyecto son el personal administrativo, administrador de red y usuarios que utilicen los equipos y los recursos de red de la Cooperativa.
El impacto de este proyecto a nivel de la institución es positivo, porque gracias a esta solución se podrá controlar la autenticación y la seguridad de los recursos de red de manera ágil.

El presente proyecto es factible ya que el Departamento de Sistemas facilitará la información necesaria para alcanzar los objetivos propuestos.

1.5. Objetivos

1.5.1. General

Implementar una distribución GNU/Linux LSBS para la autenticación de los usuarios y la seguridad de los recursos de red de la Cooperativa de Ahorro y Crédito Escencia Indígena Ltda.

1.5.2. Específicos

1. Realizar el análisis del servidor actual de autenticación y seguridad de recursos de red para conocer su funcionamiento, alcance y limitaciones.

2. Determinar la distribución GNU/Linux LSBS que mejor se ajuste a los requerimientos de autenticación y seguridad de recursos de la Cooperativa.

3. Analizar y definir las políticas de seguridad de la información según los cargos que ocupen en la Cooperativa.

4. Implementar la distribución GNU/Linux LSBS seleccionado.

CAPÍTULO 2

Marco Teórico

2.1. Antecedentes Investigativos

Revisado los archivos de tesis de universidades internacionales, nacionales, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, artículos publicados en revistas indexadas y capítulos de libros, con temas relacionados a la implementación una distribución GNU/Linux LSBS para la autenticación de los usuarios y la seguridad de los recursos de red, donde se extrae la información más relevante que aporta al tema de investigación.

En la investigación realizada por el Sr. Juan Pablo Esperanza Morocho se concluye que existen varios sistemas de seguridad de recursos de red que funciona transparentemente, es decir el usuario no se percatará que dentro del sistema se realizan verificaciones adicionales de seguridad, disponiendo de mayor seguridad en el ámbito de la información que contiene, ya que al ser una herramienta de código abierto existen más personas que lo utilizan y lo revisan, ayudando así a encontrar posibles errores o fallas de seguridad que podrían afectar el funcionamiento del sistema [3].

Luis Carlos Plasencia en su trabajo de investigación determina que el uso de las soluciones Open Source en las instituciones públicas se ha convertido en un punto fundamental ya que es indispensable poseer un esquema de seguridad de la información interna que manejan estas instituciones, además el uso de estas colusiones brinda cierto nivel de confianza en el ámbito de seguridad reduciendo en gran medida los costos de desarrollo y centralizando la administración de los recursos para mayor facilidad de las mismas [4].

Según el Ing. Santiago Gavilanes Vásquez en su proyecto de investigación llega a mencionar que las políticas y restricciones de seguridad que las empresas poseen para cada área deben ser controladas constantemente para brindar mayor seguridad a la información que circula por la red, por esta razón es muy importante el uso de las herramientas informáticas para tales soluciones [5].

En el trabajo de investigación realizado por Adriana Cumandá Salinas Perez en cuya conclusión nos indica que las políticas de seguridad deben ser plasmadas en el sistema de acuerdo a las políticas internas de seguridad de cada institución, en el cual se esté implementando la solución de seguridad de la información, puesto que aporta significativamente al crecimiento y la optimización de los recursos según los servicios que ofrece [6].

2.2. Fundamentación teórica

2.2.1. Seguridad de la Información

La seguridad de la información corporativa se ha vuelto en uno de los temas más preocupantes en todas las organizaciones, debido a la cual se ven obligados a implantar un sistema informático de seguridad para proteger la información "respecto al acceso no autorizado o la modificación de la información, ya sea en el almacenamiento, procesamiento o tránsito y contra la denegación de servicio para los usuarios no autorizados, incluyendo aquellas medidas necesarias para detectar, documentar y contrarrestar este tipo de amenazas" [7].

2.2.2. Software Open Source

Son aplicaciones que incluye el código fuente y está disponible, por lo general, sin cargo alguno. Para que una aplicación sea Open Source o código abierto debe tener ciertos requerimientos de software como: el software de ser libre de distribuir, se debe permitir modificaciones derivadas del mismo, la licencia no debe discriminar a ninguna persona y la licencia no debe limitar ningún campo de aplicación o emprendimiento [8].

La diferencia entre el software de Código Cerrado y Código Abierto es que el software de código cerrado no incluyen fuentes con los que se desarrollo la aplicación, mientras que el software de código abierto permite que varios desarrolladores puedan leer, modificar y redistribuir el código fuente de una aplicación, siempre y cuando se respete las condiciones de distribución del autor. Los desarrolladores lo mejoran, lo adaptan y corrigen los errores de la aplicación a una velocidad extraordinaria dando así como resultado la producción de un mejor software [8].

2.2.3. Sistema de autenticación

La función principal del sistema es el de "llevar a cabo la autenticación de las credenciales de usuario. Generalmente se suele emplear como servidor de autenticación remota de usuarios servidores RADIUS(Remote Authentication Dial In User Service), aunque se pueden emplear otros tipos, como, por ejemplo, DIAMETER. Adicionalmente, El servidor de autenticación puede contener política para ese usuario concreto que podría aplicar el punto de acceso" [9].

2.2.4. Directivas de grupo

El objeto de directiva de grupo en inglés Group Policy Object, es un conjunto de una o más políticas del sistema que controla el ambiente de trabajo de los usuarios y cuentas de equipos, esto permite al administrador realizar las configuraciones centralizadamente de acuerdo a las políticas de la empresa. La configuración que tiene mayor prioridad sobre los equipos locales, son las que se aplica por medio de las directivas de grupo ya que los equipos están unidos al dominio [10].

2.2.5. Usuarios

Se considera usuario a cada persona que puede acceder y usar un sistema informático en la ejecución de sus funciones como trabajador [11].

Cuenta de Usuario

La cuenta de usuario es utilizada para controlar las entradas y las acciones que realiza cada usuario durante la hora de trabajo y cierta información será almacenada como parte del historial del usuario que accedió al sistema [11].

Para que un determinado usuario pueda acceder al sistema es necesario que digite el nombre del usuarios y contraseña para que posteriormente un proceso llamado login proceda a verificar si los datos ingresados son correctos y otorgarle ciertas restricciones al usuario según el cargo que ocupe en la empresa. La forma de hacer login puede hacerlo de forma local (iniciar cesión en el mismo equipo) o en red (iniciar sesión remotamente desde otro equipo) [10].

2.2.6. Perfiles de usuario

Cada usuario tiene una carpeta de trabajo, pero el perfil de cada usuario es independiente del resto de usuarios, porque cada una tienen sus propias configuraciones.

Perfil de usuario local

Un perfil de usuario local se crea la primera vez que un usuario inicie sesión en su mismo equipo, la misma que se almacena en el disco duro local. Todas las configuraciones realizadas son específicos del mismo equipo [10].

Perfil de usuario móvil

Estos perfiles los crea el administrador del sistema y se almacena en un servidor centralizado. El perfil está disponible siempre que el usuario inicie sesión en cualquier equipo de la red, y los cambios efectuados se almacenan en el servidor [10].

Perfil de usuario obligatorio

Son perfiles que especifican configuraciones particulares de usuario o grupos de usuarios. Solamente administradores del sistema pueden realizar cambios en los perfiles obligatorios [10].

Perfil de usuario temporal

Se emite siempre que una condición de error impide la carga del perfil de los usuarios. Todos los cambios realizados por el usuario en la configuración del escritorio y los archivos se perderán cuando se cierra sesión [10].

2.2.7. Directorio Activo

Es un servicio establecido en uno o varios servidores de red, donde se almacena información como los recursos de red, con el objetivo de administrar el inicio de sesión de los usuarios, así como también administrar las políticas de grupo en toda la red. De este modo, se convierte en un medio de organizar, administrar y controlar centralizadamente, el acceso a los recursos de la red interna [11].

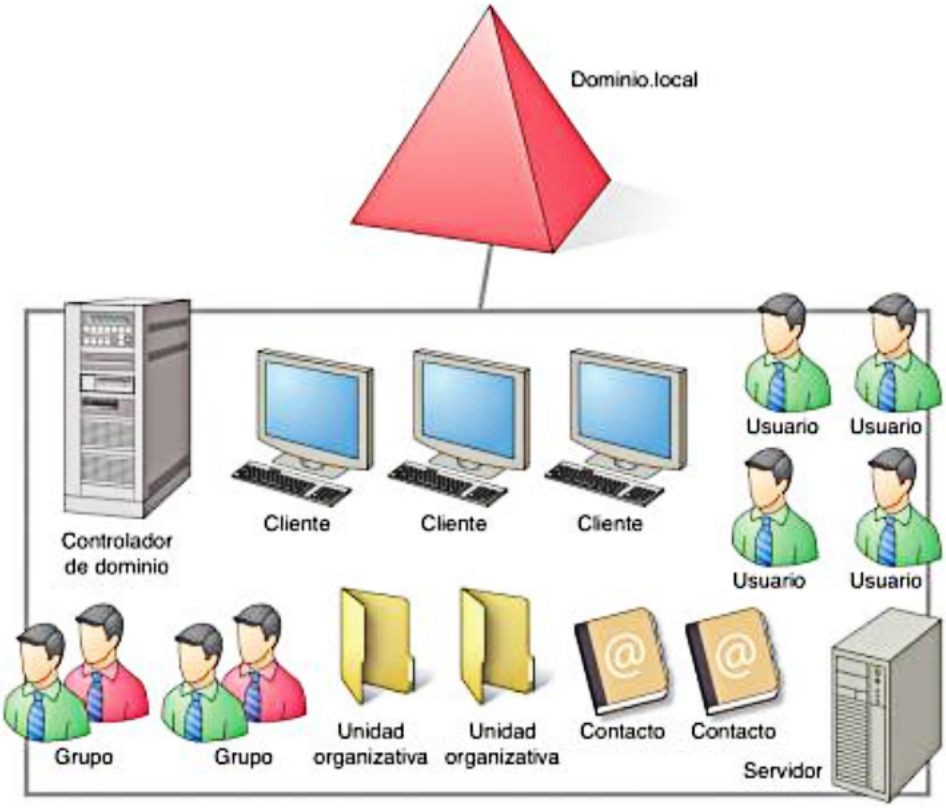


Figura 1: Estructura de un directorio activo
Fuente: Jesus Niño Camazón. Servicios de directorio (Sistemas operativos en red) Editorial Editext, 2011.

2.2.7.1. Dominio

Es la centralización de la información fundamental que agrupan todos los objetos como equipos y usuarios de una red de ordenadores, de forma que su gestión resulte más manejable y eficiente [11, 10].

2.2.7.2. Objetos

Los objetos principales (no los únicos) que se pueden manejar en Active Directory son:

- **Unidades Organizativas (OU, Organizational Unit):** Son contenedores donde se pueden colocar otros objetos, estos contenedores son las unidades más pequeñas sobre las que se pueden configurar directivas de grupo. Se utilizan para establecer una estructura jerárquica, por ejemplo, para representar la división en departamentos de una empresa.
- **Grupos:** Conjunto de objetos del mismo tipo, de modo que se trata como

si el conjunto fuera uno solo. Se utiliza fundamentalmente para asignar derechos de acceso a recursos.

- **Grupo de distribución:** Se utiliza para enviar correos electrónicos a un grupo de usuarios.
- **Grupo de seguridad:** Se utiliza para aplicar las políticas de acceso a recursos de red.

- **Usuarios:** Los usuarios tienen cuantas que les permiten identificarse en el sistema y poder así tener acceso a recursos. Las cuentas de usuarios son únicas.
- **Equipos:** Cada uno de los ordenadores que componen una red puede entrar a formar parte de un dominio. Desde el dominio se puede administrar cada uno de los equipos [10].

2.2.8. Linux Small Business Server (LSBS)

Es una distribución Linux para pequeñas y medianas empresas con 10 a 100 empleados, su principal objetivo es cubrir todas las necesidades de infraestructura de red en un solo servidor. Estas distribuciones tienen una gran gama de herramientas para el despliegue, virtualización, copia de seguridad y vigilancia, así como un equipo de personal administrativo que está muy pendiente del funcionamiento del servidor [12].

2.2.9. Firewall

Firewall también llamado como cortafuego es un dispositivo de hardware o una aplicación se software que esta exclusivamente diseñado para proteger los dispositivos de red de los usuarios externos, aplicaciones y archivos maliciosos que normalmente circula por la red externa que es el internet, gestionándolo de manera adecuada por medio de las políticas de seguridad [13].

2.2.10. Proxy

Es una aplicación que soporta peticiones de varios protocolos de internet como HTTP, HTTPS, FTP, entre otras. Sus funciones principales son el de otorgar acceso a internet a ciertas máquinas, permitir o denegar cierto tipo de tráfico, también posee una funcionalidad de cache que consiste en acelerar y mejorar el acceso a los servidores de información web [14].

2.2.11. Red privada Virtual(VPN)

Es una tecnología de red que permite una extensión de la red local sobre una red pública. Su principal función es la de transmitir los datos cifrados de forma que solamente el destinatario podrá descifrarla, de este modo los datos no están expuestos a que las manipulen en su camino por la red [15].

2.2.12. MikroTik - RouterOS

MikroTik, es una compañía que produce productos de tecnología inalámbrica como RouterBOARD o routers, también es conocido por el software que lo controla al mismo. El principal producto de esta compañía es el sistema operativo basado en Linux, conocido como MikroTik RouterOS que permite convertir una PC o una placa RouterBOARD en un ruteador dedicado con funciones relacionadas a las necesidades de un networking.
Este sistema operativo viene sin licencia a menos que se haya adquirido un RouterBoard. Para que el software pueda funcionar correctamente es necesario adquirir una licencia y activarla. Las licencias tienen costos diferentes y limitaciones en los servicios que contiene [16].

2.2.13. Winbox

Es una herramienta de servidor creada por la compañía MikroTik, que permite conectarse a un servidor MikroTik RouterOS, presentando una interfaz gráfica muy amigable, lo que hace que la configuración sea más fácil [16].

2.3. Propuesta de Solución

El presente proyecto ayudará a mejorar la autenticación de los usuarios y la seguridad de los recursos internos de la Cooperativa de Ahorro y Crédito Escencia Indígena Ltda. perfeccionando la calidad del servicio de la Cooperativa, ya que el servidor actual no proporciona las seguridades necesarias a los recursos de red, mientras que, el uso de una distribución GNU/Linux LSBS, potenciaría la seguridad de los recursos y reduciría los costos de licenciamiento en software. Además, esta distribución es adaptable a distintas Cooperativas de Ahorro y Crédito con la única diferencia que cada una tienen sus propias políticas de seguridad.

CAPÍTULO 3

Metodología

3.1. Modalidad de la investigación

Para realizar el análisis del servidor actual de autenticación y seguridad de recursos de red para conocer el funcionamiento, alcance y limitaciones, se aplicara de la investigación de campo, debido a que se acudirá a cada uno de los departamentos para obtener información necesaria, así también, se considerara la investigación descriptiva para determinar la distribución GNU/Linux que mejor se ajuste a los requerimientos de la Cooperativa, además, se utilizara el método científico para la definición de las políticas de seguridad, finalmente se adaptara a la investigación aplicada para la implementación de la distribución GNU/Linux seleccionada debido a que se aplicara los conocimientos adquiridos, esto conjuntamente con el modelado de escenarios para la simulación respectiva del ambiente de red de la Cooperativa.

3.2. Población y muestra

La presente investigación por su característica no requiere de población ni muestra.

3.3. Recolección de información

Para la recolección de la información se regirá en las siguientes técnicas:
Técnica Documental: Se considera esta técnica ya que se recurrirá a diferentes fuentes bibliográficas como: libros, artículos técnicos, tesis desarrolladas en Universidades nacionales e internacionales para profundizar sobre el tema de investigación.
Técnica de entrevista: La entrevista se lo realizara al director del Departamento de Sistemas, la cual permitirá obtener información útil para el desarrollo del presente proyecto.
Técnica de observación: Se considera esta técnica ya que se realizara la observación directa del funcionamiento de las políticas de seguridad en el servidor

actual, para detectar ciertos inconvenientes a la hora de la autenticación de los usuarios y el acceso a los recursos de red.

3.4. Procesamiento de la información

Para el procesamiento de la información obtenida a través de las entrevistas realizadas al director del Departamento de Sistemas, se desarrollará las siguientes actividades:

- Analizar los resultados obtenidos con relación al problema ya planteado.
- Recolección de la información mediante la investigación en documentos electrónicos referentes al tema.
- Identificar los problemas de seguridad del servidor actual.
- Redactar una síntesis de los resultados obtenidos.

3.5. Desarrollo del proyecto

- Identificación de los riesgos en la autenticación y seguridad de los recursos de red de la Cooperativa.
- Revisión de la estructura de las Políticas de Seguridad en la red de la Cooperativa.
- Identificación de las principales distribuciones GNU/Linux LSBS.
- Análisis de las diferentes distribuciones encontradas.
- Selección de una distribución GNU/Linux LSBS que se ajuste a los requerimientos de la Cooperativa.
- Revisión de las políticas seguridad de red de la Cooperativa.
- Establecer las políticas de seguridad según las políticas de la Cooperativa.
- Revisión de los requerimientos de hardware y software de la distribución seleccionada.
- Instalación y configuración de la distribución seleccionada.
- Pruebas de funcionalidad del servidor.

CAPÍTULO 4

DESARROLLO DE LA PROPUESTA

4.1. Identificación de los riesgos en la autenticación y seguridad de los recursos de red de la Cooperativa.

Según la entrevista llevada a cabo en Junio del 2015 al director del departamento de Sistemas, dio a conocer información pertinente de como se ha estado ejecutando las funciones y actividades no muy satisfactorios por la congestión de la red, ya que no se está aplicando las políticas de seguridad adecuadamente, la mayoría de los equipos de las distintas agencias no están unido al dominio del servidor actual, por lo cual los usuarios ingresan a páginas no permitidas provocando que el sistema corporativo no pueda procesar los datos de manera adecuada y eficaz al momento de realizar las diferentes transacciones.

Las principales páginas utilizadas por los usuarios de la entidad son:

- Intranet.
- Correo corporativo.
- Money Gram.
- Seps.
- Banco central.
- Banco de Guayaquil.

El servidor actual se encuentra configurado sobre una dirección IP pública, es decir que a este servidor se puede acceder desde cualquier lugar donde exista internet, esto se considera como punto positivo porque se puede administrar y extraer información desde cualquier lugar, así mismo, también se considera un punto negativo ya que está expuesta a ser manipulado por entes externos a la Cooperativa.

Actualmente los usuarios en los equipos tienen privilegios para:

- Modificar la dirección IP del equipo.
- Activar y desactivar las conexiones de red local del equipo.
- Cambiar el fondo de pantalla del equipo.
- Cambiar la apariencia de escritorio.
- Ejecutar cualquier instalador sin la debida autorización de los administradores de red.
- Insertar USBs o CDs en el equipo.
- Iniciar cesión en el equipo sin seguridad alguna.
- Ejecutar aplicaciones no necesarias para el trabajo diario.
- Actualizar el sistema operativo.
- Cambiar el tamaño de la barra de tareas.
- Mover la barra de tareas a otro sitio.
- Cambiar la hora del equipo.
- Acceso a páginas no autorizadas por el administrador.

4.2. Revisión de la estructura de las Políticas de Seguridad en la red de la Cooperativa.

Actualmente en la Cooperativa existen cuatro grupos de trabajo, dentro de estas no están especificadas los usuarios por agencias, por lo que se pudo observar el poco interés que le dan a dichos grupos de trabajo al momento de la creación de usuarios, como por ejemplo Skype, publicidad ibarra, diario escencia, soporte técnico, caja central, fitbank y caja comunal, generando dificultades al momento de buscar usuarios a los que se desea actualizar cierta información, el cual provoca los cuellos de botellas dentro de la actividad laboral.

La estructura de la política de seguridad actual está dividida en cuatro grupos de trabajo que son:

1. Administrador
2. Gerencial

3. Jefatura

4. Operativo

Basándose en la estructura de grupos de trabajo que posee actualmente en el servidor y el organigrama estructural de la Cooperativa se plantea crear las unidades organizativas necesarias para clasificar de mejor manera y agilizar la administración de los recursos de red, esta actividad se lo realizara mediante una clasificación adecuada de los departamento a cada uno de las unidades organizativas a las que pertenezca, además se creará una nueva unidad organizativa llamada Otros, donde se colocara los departamentos o usuarios que no se clasifique dentro de las unidades mencionadas.

Las principales páginas que el usuario ingresa provocando el rendimiento inadecuado en la ejecución de transacciones son:

1. Facebook.
2. Gmail.
3. Youtube.
4. Yahoo.
5. Twitter.
6. Outlook.
7. Hotmail.
8. Messenger.
9. Páginas de músicas en línea.
10. Páginas prohibidas.

Las políticas actuales que se encuentran en el servidor ClearOS tiene problemas conceptuales con respecto a la aplicación de listas de control de acceso (ACL), las políticas actuales se encuentran en el **Anexo C.1 y C.2 .**

4.3. Identificación de las principales distribuciones GNU/Linux LSBS.

Según la información obtenida del estudio de las diferentes distribuciones Linux Small Business Server realizada por Thomas Drilling en su libro Linux Small Business Distros, que según su análisis las distribuciones Zentyal, ClearOS y Serv-OS son las más recomendadas para empresas pequeñas y medianas.
Luego de haber realizado la entrevistas al director del departamento de Sistemas quien es la personas encargadas del servidor actual, se pudo sugerir las distribuciones recomendadas por Thomas Drilling que van a ser analizadas dependiendo de los requerimientos y la estructura de la red actual que posee la Cooperativa.

Las distribuciones catalogadas como las más recomendadas por Thomas Drilling son:

1. Zentyal
2. ClearOS
3. Serv-OS

4.4. Análisis de las diferentes distribuciones encontradas.

En esta sección se realiza el análisis de cada una de las alternativas catalogadas como recomendadas por el cumplimiento de los requerimientos de la Cooperativa, se realiza el análisis según ciertas características consideradas importantes para la implementación de la solución, para la selección de la distribución GNU/Linux se utilizó el proceso de Benchmarking.

En la Tabla 1 se detalla el análisis realizado entre las tres distribuciones recomendadas según su versión.
X = Si
x = Comienzo
"-" No aplica.
Como se puede observar la distribución Serv-OS no posee el soporte ni información necesaria para cubrir los objetivos planteados, esto lo descarta como una distribución a ser utilizada para el presente proyecto.
La distribución ClearOS es otra opción que se descarta porque la versión actual que está en funcionamiento en la Cooperativa tiene deficiencia en ciertos servicios instalados, de igual manera, es compatible con Windows Active Directory,

CARACTERÍSTICAS NECESARIAS	Zentyal 4	Zentyal 4.1	ClearOS Community release 6.5.0	ClearOS Community release 6.6.0	Serv-OS
Soporte para Microsoft Outlook® 2007, 2010, 2013	X	X	x	X	-
Compatibilidad nativa con Microsoft Active Directory®	X	X	-	-	X
Email, calendarios, contactos	X	X	X	X	X
Mail Filter	X	X	-	x	X
Packet Filter	X	X	-	-	
Redireccionamiento de puertos	X	X	X	X	
Interfaces estáticos y DHCP	X	X	X	X	
Gestión central del dominio de directorio	X	X	-	x	X
Usuarios, Grupos de Seguridad, Listas de Distribución, Contactos	X	X	X	X	
Múltiples Unidades Organizativas (OUs)	X	X	-	-	
Autenticación Single Sign-On (SSO)	X	X	-	-	
OS soportados: Windows® XP, Windows Vista®, Windows® 7, Windows® 8,Linux, Mac	X	X	-	x	
Compartición de ficheros en entornos Windows® (CIFS)	X	X	X	X	
Permisos de acceso y modificación de Usuarios & Grupos (ACLs)	X	X	X	X	
Gestión de impresoras	X	X	X	X	
DNS Server	X	X	X	X	X
NTP Server	X	X	X	X	
VPN Server y Client	X	X	X	X	X
Antivirus	X	-	X	X	
Web Proxy	X	-	X	X	X
CARACTERÍSTICAS ADICIONALES					
trafficshaping	X	-	X	X	-
l2tp	X	-	-	-	-
Soporte mejorado múltiples idiomas en los buzones	X	X	-	X	
REQUERIMIENTOS					
Servidor altamente disponible.	X	X	X	X	-
Estrictas políticas de filtrado de páginas web.	X		-	-	x
Seguridad en la autenticación de usuarios.	X	X	X	X	x
Integridad de la información.	X	X	X	X	X
Disponibilidad de la información.	X	X	-	X	X

Tabla 1: Análisis de diferentes distribuciones LSBS.
Fuente: Elaborado por investigador.

sin embargo tiene un costo por el servicio, por tal razón no cumple con los requerimientos de la Cooperativa.
Por último tenemos la distribución GNU/Linux que más se acopla a los requerimientos de la Cooperativa, ya que es compatible con Windows Active Directory, esto facilita la creación y manipulación de las políticas de seguridad para cada unidad organizativa.

4.5. Selección de una distribución GNU/Linux LSBS que se ajuste a los requerimientos de la Cooperativa.

Requerimientos de la Cooperativa.
Realizando la entrevista respectiva a la persona encargada del servidor se pudo obtener los siguientes requerimientos que es detalla a continuación:

- Servidor altamente disponible.
- Estrictas políticas de filtrado de páginas web.
- Seguridad en la autenticación de usuarios.
- Integridad de la información.
- Disponibilidad de la información.

En la entrevista también se pudo obtener las versiones de los sistemas operativos que están actualmente en funcionamiento tales como:

- Microsoft Windows 7 Professional
- Microsoft Windows 7 Ultimate
- Microsoft Windows 8.1
- Microsoft Windows 8.1 Pro
- Microsoft Windows XP Professional

Según la entrevista realizada al director del Departamento de Sistemas, dio a conocer que es preferible una distribución libre u Open Source para el presente proyecto, al conocer esta respuesta conjuntamente con los requerimientos de la Cooperativa se selecciona la distribución Linux Zentyal 4.0 por las características analizadas anteriormente en el Tabla 1, se selecciona esta opción por la accesibilidad de la documentación, lo cual facilita al desarrollo de la investigación permitiendo la culminación eficaz de la misma; así mismo por el cumplimiento de los requisitos y servicios necesarios para lograr los objetivos planteados.

4.5.1. Historia de Zentyal

El proyecto Zentyal se inició en el año de 2004 con el nombre de Ebox Plataform que integra más de 30 herramientas de código abierto para la administración de redes de manera centralizada en una sola tecnología, este sistema es una distribución GNU/Linux que deriva de Ubuntu Server desde el año 2007, una de las ventajas es que posee es que tiene más de 1000 descargas diarias, además de tener una comunidad activa de miles de miembros que ayuda al mejoramiento del sistema, convirtiéndose así en uno de los proyectos empresariales Open Source más populares en el mundo, tanto fue la popularidad que les llevó a crear un nuevo proyecto llamado Zentyal Cloud[17].
Si desea poseer de una herramienta completa, Zentyal posee una versión comercial en el cual el beneficiado debe pagar pequeñas cuotas mensuales ya que con este pago se tiene beneficios adicionales que garantiza la eficiencia y la estabilidad de la misma, Como una ventaja del sistema es que se puede instalar tanto en máquinas reales como en virtuales de manera exclusiva, además de tener la posibilidad de instalar aplicaciones adicionales pero de forma manual[18].

4.5.2. Principales módulos y características de Zentyal

- **Zentyal Gateway:** Permite que tu red sea más fiable, optimiza el ancho de banda así como ayuda a controlar lo que entra en la red.
- **Caché Transparente:** Si los usuarios visitan los mismos sitios web, los datos se descargarán una sola vez y la conexión estará disponible para tareas más importantes.
- **Control de Tráfico:** Una conexión de Internet sobrecargada es cosa del pasado. Asegurarse que el tráfico más crítico se sirve bien, independientemente de la carga de la red.
- **Balanceo de Carga y Disponibilidad:** Si se tiene más de una conexión a Internet, Zentyal puede distribuir los clientes de forma transparente y asegurar que se esté conectado aunque una de las conexiones esté inactiva.
- **Filtrado de Contenido:** Restringe el acceso a determinados sitios, o permite sólo a sitios específicos. Esta característica permite restringir la navegación inapropiada y ayuda a cumplir las políticas de uso de Internet en el lugar de trabajo.

- **Redes Privadas Virtuales:** Si se tienen múltiples oficinas en el mundo, se puede también conectarlas de forma segura y tener una sola oficina virtual.
- **Cortafuegos:** Permite sólo el tráfico necesario es un primer filtro estupendo contra intrusos no deseados.
- **Detección de Intrusos:** El IDS de Zentyal Snort informará de cualquier intento sospechoso y dejará analizarlos para evaluar los potenciales daños.
- **Objetos de Red:** Se puede elegir hasta qué nivel se quiere gestionar la red con Zentyal. Se puede cambiar la configuración de toda la red, de un departamento o de un solo ordenador.
- **Servidor DNS:** Se puede asignar una dirección y un nombre fijo a cada equipo de la red para facilitar la navegación por Intranet. Es más fácil recordar uci.cu que 10.0.0.2.
- **Zentyal Office:** Permite gestionar y compartir recursos de oficina, incluyendo perfiles de usuarios y grupos, ficheros, impresoras, calendarios, contactos, tareas y backups de datos.
- **Servicio de Directorio:** Zentyal Office permite la gestión de todos los usuarios y recursos desde un punto central. Decide quién tiene acceso y a qué datos. Zentyal se basa en estándares abiertos como LDAP así que es fácil integrarlo con otras aplicaciones y servicios.
- **Calendarios, Contactos y Tareas:** Zentyal permite compartir calendarios, contactos y tareas entre los miembros del mismo equipo.
- **Compartición de Ficheros e Impresoras:** Se pueden compartir fácilmente archivos con Zentyal y usarlos independientemente del sistema operativo que se esté utilizando.
- **Backups de Datos:** Permite automatizar los backups de datos para no tener que preocuparse de discos que fallan o de usuarios que borran un fichero por accidente.
- **Zentyal servidor de comunicaciones unificadas:** Gestiona todas las comunicaciones, incluyendo correo electrónico, mensajería instantánea y Voz IP.
- **Gestión de Usuarios:** Gestiona todos los usuarios y recursos desde un punto central. Los cuales no tienen que recordar distintos usuarios

y contraseñas para cada servicio. Además, es fácil y rápido proporcionar correo electrónico, una cuenta de IM y Voz IP a los usuarios.

- **Correo electrónico:** Zentyal viene con una solución de correo electrónico integrado, con tecnologías antispam y antivirus. Esta característica soporta todos los estándares habituales para que puedas seguir utilizando los clientes de correo electrónico favoritos.
- **Mensajería Instantánea:** Zentyal ofrece mensajería instantánea basada en el protocolo Jabber/XMPP, así que se puede utilizar cualquiera de los clientes existentes en cualquier plataforma, incluso en los teléfonos móviles.
- **Voz IP:** Con Zentyal puedes ofrecer a los usuarios su propia extensión y realizar llamadas internas y conferencias con facilidad. Con un proveedor también se puede obtener números de teléfono reales y dirigirlos al servidor Zentyal para hacer y recibir llamadas a un coste muy bajo[19].

4.5.3. Perfiles de Zentyal que se pueden instalar

- **Puerta de acceso:** Zentyal actúa como la puerta de enlace de la red local ofreciendo un acceso a Internet seguro y controlado. Zentyal protege la red local contra ataques externos, intrusiones, amenazas a la seguridad interna y posibilita la interconexión segura entre redes locales a través de Internet u otra red externa.
- **Infraestructura:** Zentyal gestiona la infraestructura de la red local con los servicios básicos: DHCP, DNS, NTP, servidor HTTP, etc.
- **Oficina:** Zentyal actúa como servidor de recursos compartidos, dominios y directorio de usuarios de la red local: ficheros, impresoras, calendarios, contactos, perfiles de usuarios y grupos, etc.
- **Comunicación:** Zentyal se convierte en el centro de comunicaciones de la empresa, incluyendo correo, mensajería instantánea y plataformas de trabajo en grupo.

4.6. Revisión de las políticas seguridad de red de la Cooperativa.

En la Cooperativa se puede observar que aún no se tienen establecidas las políticas seguridad, ya que las políticas constituidas actualmente en el servidor fueron establecidas por el Departamento de Sistemas sin ninguna sugerencia del departamento correspondiente.

4.7. Establecer las políticas de seguridad según las políticas de la Cooperativa.

Para establecer las políticas de seguridad se basa en la norma ISO 27002:2005 (Estándar de Seguridad de la Información), de la norma mencionada se utiliza el objetivo de control Políticas de Control de Acceso, en el cual menciona que se debe establecer las políticas de control de acceso en base a las necesidades de seguridad y de negocio de la organización, también, se considera la estructura de las políticas existentes del sistema actual, además del organigrama estructural de la Cooperativa, por esta razón en el presente proyecto se crean 5 unidades organizativas:

1. Administración.
2. Gerencial.
3. Jefatura.
4. Operativo.
5. Otros.

Dentro de cada una de ellas se establecen otras unidades organizativas para la mejor organización de las mismas, tales como:

1. **Administración** (Usuarios que tengan la función administrativa en la Cooperativa).
2. **Gerencial** (Usuarios con privilegios gerenciales).
3. **Jefatura** (Ibarra, Otavalo, Tulcán, Quito, Salcedo, Ambato Centro, Huachi, Cañar, Azogues, Cuenca).
4. **Operativo** (Ibarra, Otavalo, Tulcán, Quito, Salcedo, Ambato Centro, Huachi, Cañar, Azogues, Cuenca).
5. **Otros** (Skype, fitbank, publicidad, soporte, caja comunal y general).

Nota: En el caso de la unidad organizativa Jefatura, dentro de cada oficina se crea directamente los usuarios ya que solamente hay un jefe de agencia.
Además, se crea grupos como:

1. **Dirección:** En este grupo está conformado por el personal como contabilidad, talento humano, auditor interno, jefe de operaciones, entre otros.

2. **Cajas:** En este grupo está conformado por todo el personal de cajas a nivel de todas las agencias de la Cooperativa.

3. **Créditos:** En este grupo está conformado por todo el personal de créditos incluidos los asesores a nivel de todas las agencias de la Cooperativa.

4. **General:** En este grupo está conformado por todo el personal a nivel de todas las agencias de la Cooperativa excepto los usuarios que se encuentren en el grupo Otros.

5. **Gerencia:** En este grupo está conformado por a la gerencia y asesor de gerencia, además de otras entidades externas que sirven como apoyo al cargo mencionado.

6. **Información:** En este grupo está conformado por todo el personal de información a nivel de todas las agencias de la Cooperativa.

7. **Inversiones:** En este grupo está conformado por todo el personal de inversiones a nivel de todas las agencias de la Cooperativa.

8. **Jefatura:** En este grupo está conformado por todo el personal de jefatura a nivel de todas las agencias de la Cooperativa.

9. **Otros:** En este grupo está conformado por entidades externas a la Cooperativa.

10. **Secretaria:** En este grupo está conformado por todo el personal de secretaria a nivel de todas las agencias de la Cooperativa.

11. **Sistemas:** En este grupo está conformado por todo el personal del Departamento de Sistemas.

Nota: Estos grupos se crean para una mayor organización de los usuarios por departamento.

4.7.1. Políticas de seguridad

Para la creación de las políticas de seguridad se basa en la norma ISO 27002:2005 antes mencionada y se hace uso de los siguientes objetivos de control:

Gestión de acceso de usuario: su objetivo principal es garantizar a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información.

Responsabilidades de usuario: su objetivo es impedir el acceso de usuarios no autorizados y el compromiso o robo de información y recursos para el tratamiento de la información.
Control de acceso a la red: su objetivo es impedir el acceso no autorizado a los servicios en red.
Control de acceso al sistema operativo: su objetivo es impedir el acceso no autorizado al sistema operativo de los sistemas.
Control de acceso a las aplicaciones y a la información: su objetivo es impedir el acceso no autorizado a la información mantenida por los sistemas de las aplicaciones.

Basándose en los objetivos de controles anteriores, se realiza las políticas de seguridad que se detalla a continuación

- El usuario no puede modificar la dirección IP del equipo.
- El usuario no puede activar y desactivar las conexiones de red local del equipo.
- El usuario no puede cambiar el fondo de pantalla del equipo.
- El usuario no puede cambiar la apariencia de escritorio.
- El usuario no puede ejecutar cualquier instalador sin la debida autorización de los administradores de red.
- El usuario no debe insertar dispositivos de almacenamiento externos como USBs o CDs en el equipo.
- El usuario debe iniciar cesión en el equipo con la respectiva contraseña.
- Desconexión automática de terminales.
- El usuario debe ejecutar aplicaciones específicas como: Word, excel, internet explorer, Adobe Reader, entre otras aplicaciones necesarias para el trabajo diario de los usuarios.
- El usuario no debe actualizar el sistema operativo.
- El usuario no debe realizar cambios en la barra de tareas.
- El usuario no debe cambiar el tamaño de la barra de tareas.
- El usuario no tiene el privilegio de mover la barra de tareas a otro sitio.

- El usuario no tiene la autorización para cambiar la hora del equipo.
- El usuario no debe tener acceso a páginas no autorizadas por el administrador (Proxy).
- Bloqueo de ciertos puertos para mayor seguridad del sistema de información (Firewall).

4.7.2. Reglas de filtrado de paquetes (Firewall)

1. **Reglas de filtrado desde las redes internas a Zentyal.**
   - Samba
   - NTP
   - DNS
   - SSH
2. **Reglas de filtrado para las redes internas.**
   - Denegar acceso a facebook en modo seguro.
   - Denegar acceso a youtube en modo seguro.
   - Denegar acceso a gmail en modo seguro.
   - Denegar acceso a twitter en modo seguro.
   - Denegar acceso a messenger en modo seguro.
   - Denegar acceso a hotmail en modo seguro.
   - Denegar acceso a live en modo seguro.
3. **Reglas de filtrado desde las redes externas a Zentyal.**
   - Cualquier ICMP
   - TCP
   - UDP
4. **Reglas de filtrado para el tráfico saliente de Zentyal.**
   - Cualquier ICMP
   - TCP
   - UDP

4.7.3. Reglas de acceso proxy

Nota: Estas reglas de acceso son asignadas a los grupos creados.

1. **Administrativo**

   a) **Configuración**

   - Umbral filtrado de contenido Estricto.
   - Usar antivirus.

   b) **Reglas de dominios y URLs**

   - 192.168.0.203:8386
   - 192.168.0.244
   - 192.168.0.245
   - 192.168.0.246
   - iess.gob.ec
   - creditreport.com.ec
   - bancavirtual.bankguay.com
   - bancoguayaquil.com
   - bce.fin.ec
   - rapipago.ec
   - corporacionregistrocivil.gob.ec
   - easypagos.com
   - ecuadorlegalonline.com
   - ecuatransfer.com
   - wikipedia.org
   - escencia.com
   - escenciaindigena.com
   - google.com
   - iniglobe.com.pe
   - microsoft.com
   - perspeak.avira-update.com
   - pichincha.com

- registrosocial.gob.ec
- services.com
- skype.com
- switchorm.com
- teamviwer.com
- uta.edu.ec
- espe.edu.ec

c) **Extensiones de archivos**

- ade Microsoft Access project extension
- adp Microsoft Access project
- bas Microsoft Visual Basic class module
- bat Batch file
- cab Windows compressed setup file
- cmd Microsoft Windows NT command script
- exe Program url Internet shortcut
- rar RAR compressed file
- zip Zip compressed file
- asx Windows Media Audio and Video
- avi Movie file midi Audio file
- mov Quicktime file
- mp3 Music file
- mp4 Music file
- mpeg Movie file
- mpg Movie file
- ogg Music file
- pcd Photo CD image
- qt Quicktime file
- wav Audio file
- wma Windows Media Audio file
- wmf Movie file

- wmv Windows Media File

d) **Tipo MIME identificador de formato en internet**

- application/compress
- application/futuresplash
- application/gzip
- application/java-vm
- application/x-compress
- application/x-gzip
- application/x-shockwave-flash
- application/x-shockwave-flash2-preview
- application/zip
- audio/mpeg
- audio/x-mpeg
- audio/x-pn-realaudio
- audio/x-wav
- image/vnd.rn-realflash
- video/acorn-replay
- video/mpeg
- video/msvideo
- video/quicktime
- video/x-mpeg2
- video/x-msvideo

2. **Cajas**

a) **Configuración**

- Umbral filtrado de contenido Estricto.
- Usar antivirus.

b) **Reglas de dominios y URLs**

- 63.91.129.163
- 65.55.39.103

- 192.168.0.6
- 192.168.0.14
- 192.168.0.26
- 192.168.0.81
- 192.168.0.203:8386
- 192.168.0.205:8386
- 192.168.0.244
- 192.168.0.245
- 192.168.0.246
- 186.3.35.156
- 186.42.112.66:8080
- 186.42.112.68
- 190.152.22.157:20000
- 190.152.220.29
- 190.99.72.142
- 200.25.206.91
- 207.67.74.163
- 213.0.40.235
- 213.0.40.237
- iess.gob.ec
- creditreport.com.ec
- bancavirtual.bankguay.com
- bancoguayaquil.com
- rapipago.ec
- coonecta.com.ec
- corporacionregistrocivil.gob.ec
- ecuadorlegalonline.com
- escencia.com
- escenciaindigena.com
- services.com

- switchorm.com
- teamviwer.com
- registrosocial.gob.ec
- uta.edu.ec
- espe.edu.ec

c) **Extensiones de archivos**

- bas Microsoft Visual Basic class module
- bat Batch file
- cab Windows compressed setup file
- cmd Microsoft Windows NT command script
- exe Program url Internet shortcut
- rar RAR compressed file
- zip Zip compressed file
- mov Quicktime file
- mpeg Movie file
- mpg Movie file
- pcd Photo CD image
- qt Quicktime file

d) **Tipo MIME identificador de formato en internet**

- application/compress
- application/futuresplash
- application/gzip
- application/java-vm
- application/x-compress
- application/x-gzip
- application/x-shockwave-flash
- application/x-shockwave-flash2-preview
- application/zip
- audio/mpeg

- audio/x-mpeg
- audio/x-pn-realaudio
- audio/x-wav
- image/vnd.rn-realflash
- video/acorn-replay
- video/mpeg
- video/msvideo
- video/quicktime
- video/x-mpeg2
- video/x-msvideo

3. **Créditos**

   a) **Configuración**

   - Umbral filtrado de contenido Estricto.
   - Usar antivirus.

   b) **Reglas de dominios y URLs**

   - 192.168.0.203:8386
   - 192.168.0.244
   - 192.168.0.245
   - 192.168.0.246
   - iess.gob.ec
   - creditreport.com.ec
   - corporacionregistrocivil.gob.ec
   - escencia.com
   - escenciaindigena.com
   - registrosocial.gob.ec
   - teamviwer.com
   - registrosocial.gob.ec
   - uta.edu.ec
   - espe.edu.ec

c) **Extensiones de archivos**

- bat Batch file
- cmd Microsoft Windows NT command script
- exe Program url Internet shortcut
- rar RAR compressed file
- zip Zip compressed file
- mov Quicktime file
- qt Quicktime file

d) **Tipo MIME identificador de formato en internet**

- application/compress
- application/futuresplash
- application/gzip
- application/java-vm
- application/x-compress
- application/x-gzip
- application/x-shockwave-flash
- application/x-shockwave-flash2-preview
- application/zip
- audio/mpeg
- audio/x-mpeg
- audio/x-pn-realaudio
- audio/x-wav
- image/vnd.rn-realflash
- video/acorn-replay
- video/mpeg
- video/msvideo
- video/quicktime
- video/x-mpeg2
- video/x-msvideo

4. **Gerencia**

   a) **Configuración**

   - Umbral filtrado de contenido Estricto.
   - Usar antivirus.

   b) **Reglas de dominios y URLs**

   - 192.168.0.203:8386
   - 192.168.0.245
   - 192.168.0.246
   - 190.152.22.157
   - iess.gob.ec
   - creditreport.com.ec
   - corporacionregistrocivil.gob.ec
   - easypagos.com
   - escencia.com
   - escenciaindigena.com
   - microsoft.com
   - moneygram.com
   - motorlink.ec
   - pctools.com
   - perspeak.avira-update.com
   - pichincha.com
   - registrosocial.gob.ec
   - servientrega.com.ec
   - service.com
   - skype.com
   - switchorm.com
   - teamviwer.com
   - uta.edu.ec
   - espe.edu.ec

c) **Extensiones de archivos**

- ade Microsoft Access project extension
- adp Microsoft Access project
- bas Microsoft Visual Basic class module
- bat Batch file
- cab Windows compressed setup file
- cmd Microsoft Windows NT command script
- exe Program url Internet shortcut
- rar RAR compressed file
- zip Zip compressed file
- asx Windows Media Audio and Video
- avi Movie file midi Audio file
- mov Quicktime file
- mp3 Music file
- mp4 Music file
- mpeg Movie file
- mpg Movie file
- ogg Music file
- pcd Photo CD image
- qt Quicktime file
- wav Audio file
- wma Windows Media Audio file
- wmf Movie file
- wmv Windows Media File

d) **Tipo MIME identificador de formato en internet**

- application/compress
- application/futuresplash
- application/gzip
- application/java-vm
- application/x-compress

- application/x-gzip
- application/x-shockwave-flash
- application/x-shockwave-flash2-preview
- application/zip
- audio/mpeg
- audio/x-mpeg
- audio/x-pn-realaudio
- audio/x-wav
- image/vnd.rn-realflash
- video/acorn-replay
- video/mpeg
- video/msvideo
- video/quicktime
- video/x-mpeg2
- video/x-msvideo

5. **Información**

   a) **Configuración**

   - Umbral filtrado de contenido Estricto.
   - Usar antivirus.

   b) **Reglas de dominios y URLs**

   - 192.168.0.203:8386
   - 192.168.0.244
   - 192.168.0.245
   - 192.168.0.246
   - iess.gob.ec
   - creditreport.com.ec
   - moneygram.com
   - rapipago.ec
   - corporacionregistrocivil.gob.ec

- easypagos.com
- escencia.com
- escenciaindigena.com
- microsoft.com
- moneygram.com
- registrosocial.gob.ec
- servientrega.com.ec
- service.com
- teamviwer.com
- switchorm.com
- uta.edu.ec
- espe.edu.ec

c) **Extensiones de archivos**

- bat Batch file
- cmd Microsoft Windows NT command script
- exe Program url Internet shortcut
- rar RAR compressed file
- zip Zip compressed file

d) **Tipo MIME identificador de formato en internet**

- application/compress
- application/futuresplash
- application/gzip
- application/java-vm
- application/x-compress
- application/x-gzip
- application/x-shockwave-flash
- application/x-shockwave-flash2-preview
- application/zip
- audio/mpeg

- audio/x-mpeg
- audio/x-pn-realaudio
- audio/x-wav
- image/vnd.rn-realflash
- video/acorn-replay
- video/mpeg
- video/msvideo
- video/quicktime
- video/x-mpeg2
- video/x-msvideo

6. **Inversiones**

   a) **Configuración**

   - Umbral filtrado de contenido Estricto.
   - Usar antivirus.

   b) **Reglas de dominios y URLs**

   - 192.168.0.203:8386
   - 192.168.0.245
   - 192.168.0.246
   - 213.0.40.235
   - 213.0.40.237
   - iess.gob.ec
   - creditreport.com.ec
   - corporacionregistrocivil.gob.ec
   - escencia.com
   - escenciaindigena.com
   - pichincha.com
   - registrosocial.gob.ec
   - servientrega.com.ec
   - teamviwer.com

- uta.edu.ec
- espe.edu.ec

c) **Extensiones de archivos**

- bat Batch file
- cmd Microsoft Windows NT command script
- exe Program url Internet shortcut
- rar RAR compressed file
- zip Zip compressed file

d) **Tipo MIME identificador de formato en internet**

- application/compress
- application/futuresplash
- application/gzip
- application/java-vm
- application/x-compress
- application/x-gzip
- application/x-shockwave-flash
- application/x-shockwave-flash2-preview
- application/zip
- audio/mpeg
- audio/x-mpeg
- audio/x-pn-realaudio
- audio/x-wav
- image/vnd.rn-realflash
- video/acorn-replay
- video/mpeg
- video/msvideo
- video/quicktime
- video/x-mpeg2
- video/x-msvideo

7. **Jefatura**

   a) **Configuración**

   - Umbral filtrado de contenido Estricto.
   - Usar antivirus.

   b) **Reglas de dominios y URLs**

   - 192.168.0.1
   - 192.168.0.203:8386
   - 192.168.0.245
   - 192.168.0.246
   - 213.0.40.235
   - 213.0.40.237
   - iess.gob.ec
   - creditreport.com.ec
   - corporacionregistrocivil.gob.ec
   - coonecta.com.ec
   - escencia.com
   - escenciaindigena.com
   - google.com
   - registrosocial.gob.ec
   - servientrega.com.ec
   - seps.gob.ec
   - skype.com
   - teamviwer.com
   - funcionjudicial-tungurahua.gob.ec
   - uta.edu.ec
   - espe.edu.ec

   c) **Extensiones de archivos**

   - bat Batch file
   - cmd Microsoft Windows NT command script

- exe Program url Internet shortcut
- rar RAR compressed file
- zip Zip compressed file

d) **Tipo MIME identificador de formato en internet**

- application/compress
- application/futuresplash
- application/gzip
- application/java-vm
- application/x-compress
- application/x-gzip
- application/x-shockwave-flash
- application/x-shockwave-flash2-preview
- application/zip
- audio/mpeg
- audio/x-mpeg
- audio/x-pn-realaudio
- audio/x-wav
- image/vnd.rn-realflash
- video/acorn-replay
- video/mpeg
- video/msvideo
- video/quicktime
- video/x-mpeg2
- video/x-msvideo

8. **Otros**

a) **Configuración**

- Umbral filtrado de contenido Estricto.
- Usar antivirus.

b) **Reglas de dominios y URLs**

- 192.168.0.203:8386
- 192.168.0.244
- 192.168.0.245
- 192.168.0.246
- iess.gob.ec
- creditreport.com.ec
- corporacionregistrocivil.gob.ec
- escencia.com
- escenciaindigena.com
- registrosocial.gob.ec
- teamviwer.com
- registrosocial.gob.ec

c) **Extensiones de archivos**

- ade Microsoft Access project extension
- adp Microsoft Access project
- bas Microsoft Visual Basic class module
- bat Batch file
- cab Windows compressed setup file
- cmd Microsoft Windows NT command script
- exe Program url Internet shortcut
- rar RAR compressed file
- zip Zip compressed file
- asx Windows Media Audio and Video
- avi Movie file midi Audio file
- mov Quicktime file
- mp3 Music file
- mp4 Music file
- mpeg Movie file
- mpg Movie file
- ogg Music file

- pcd Photo CD image
- qt Quicktime file
- wav Audio file
- wma Windows Media Audio file
- wmf Movie file
- wmv Windows Media File

d) **Tipo MIME identificador de formato en internet**

- application/compress
- application/futuresplash
- application/gzip
- application/java-vm
- application/x-compress
- application/x-gzip
- application/x-shockwave-flash
- application/x-shockwave-flash2-preview
- application/zip
- audio/mpeg
- audio/x-mpeg
- audio/x-pn-realaudio
- audio/x-wav
- image/vnd.rn-realflash
- video/acorn-replay
- video/mpeg
- video/msvideo
- video/quicktime
- video/x-mpeg2
- video/x-msvideo

9. **Secretaria**

a) **Configuración**

- Umbral filtrado de contenido Estricto.
- Usar antivirus.

b) **Reglas de dominios y URLs**

- 192.168.0.203:8386
- 192.168.0.245
- 192.168.0.246
- iess.gob.ec
- creditreport.com.ec
- corporacionregistrocivil.gob.ec
- easypagos.com
- wikipedia.org
- escencia.com
- escenciaindigena.com
- microsoft.com
- moneygram.com
- pichincha.com
- registrosocial.gob.ec
- servientrega.com.ec
- service.com
- skype.com
- switchorm.com
- teamviwer.com
- uta.edu.ec
- espe.edu.ec

c) **Extensiones de archivos**

- ade Microsoft Access project extension
- adp Microsoft Access project
- bas Microsoft Visual Basic class module
- bat Batch file

- cab Windows compressed setup file
- cmd Microsoft Windows NT command script
- exe Program url Internet shortcut
- rar RAR compressed file
- zip Zip compressed file
- asx Windows Media Audio and Video
- avi Movie file midi Audio file
- mov Quicktime file
- mp3 Music file
- mp4 Music file
- mpeg Movie file
- mpg Movie file
- ogg Music file
- pcd Photo CD image
- qt Quicktime file
- wav Audio file
- wma Windows Media Audio file
- wmf Movie file
- wmv Windows Media File

d) **Tipo MIME identificador de formato en internet**

- application/compress
- application/futuresplash
- application/gzip
- application/java-vm
- application/x-compress
- application/x-gzip
- application/x-shockwave-flash
- application/x-shockwave-flash2-preview
- application/zip
- audio/mpeg

- audio/x-mpeg
- audio/x-pn-realaudio
- audio/x-wav
- image/vnd.rn-realflash
- video/acorn-replay
- video/mpeg
- video/msvideo
- video/quicktime
- video/x-mpeg2
- video/x-msvideo

10. **Sistemas**

a) **Configuración**

- Umbral filtrado de contenido Estricto.
- Usar antivirus.

b) **Reglas de dominios y URLs**

- 63.91.129.163
- 65.55.39.103
- 192.168.0.6
- 192.168.0.14
- 192.168.0.26
- 192.168.0.81
- 192.168.0.203:8386
- 192.168.0.205:8386
- 192.168.0.244
- 192.168.0.245
- 192.168.0.246
- 186.3.35.156
- 186.42.112.66:8080
- 186.42.112.68

- 190.152.22.157:20000
- 190.152.220.29
- 190.99.72.142
- 200.25.206.91
- 207.67.74.163
- 213.0.40.235
- 213.0.40.237
- iess.gob.ec
- creditreport.com.ec
- moneygram.com
- bancavirtual.bankguay.com
- bancoguayaquil.com
- bce.fin.ec
- rapipago.ec
- coonecta.com.ec
- corporacionregistrocivil.gob.ec
- easypagos.com
- ecuadorlegalonline.com
- ecuatransfer.com
- wikipedia.org
- escencia.com
- escenciaindigena.com
- google.com
- iniglobe.com.pe
- maps.yahoo.com
- microsoft.com
- moneygram.com
- motorlink.ec
- pctools.com
- perspeak.avira-update.com

- pichincha.com
- radioambato.com
- registrosocial.gob.ec
- services.com
- servientrega.com.ec
- skype.com
- switchorm.com
- teamviwer.com
- verisign.com
- wlxrs.com
- registrosocial.gob.ec
- uta.edu.ec
- espe.edu.ec

c) **Extensiones de archivos**

- ade Microsoft Access project extension
- adp Microsoft Access project
- bas Microsoft Visual Basic class module
- bat Batch file
- cab Windows compressed setup file
- cmd Microsoft Windows NT command script
- exe Program url Internet shortcut
- rar RAR compressed file
- zip Zip compressed file
- asx Windows Media Audio and Video
- avi Movie file midi Audio file
- mov Quicktime file
- mp3 Music file
- mp4 Music file
- mpeg Movie file
- mpg Movie file

- ogg Music file
- pcd Photo CD image
- qt Quicktime file
- wav Audio file
- wma Windows Media Audio file
- wmf Movie file
- wmv Windows Media File

d) **Tipo MIME identificador de formato en internet**

- application/compress
- application/futuresplash
- application/gzip
- application/java-vm
- application/x-compress
- application/x-gzip
- application/x-shockwave-flash
- application/x-shockwave-flash2-preview
- application/zip
- audio/mpeg
- audio/x-mpeg
- audio/x-pn-realaudio
- audio/x-wav
- image/vnd.rn-realflash
- video/acorn-replay
- video/mpeg
- video/msvideo
- video/quicktime
- video/x-mpeg2
- video/x-msvideo

e) **Tipo MIME identificador de formato en internet**

- application/compress
- application/futuresplash
- application/gzip
- application/java-vm
- application/x-compress
- application/x-gzip
- application/x-shockwave-flash
- application/x-shockwave-flash2-preview
- application/zip
- audio/mpeg
- audio/x-mpeg
- audio/x-pn-realaudio
- audio/x-wav
- image/vnd.rn-realflash
- video/acorn-replay
- video/mpeg
- video/msvideo
- video/quicktime
- video/x-mpeg2
- video/x-msvideo

4.8. Revisión de los requerimientos de hardware y software de la distribución seleccionada.

Los requerimientos mínimos de hardware para un servidor Zentyal dependen de los módulos o servicios que vayan a ser instalados, además del número de usuarios que vayan a utilizar los servicios. En la Figura 2, se muestra una tabla con los requerimientos mínimos para la instalación de un servidor Zentyal.

PERFIL DE ZENTYAL	USUARIOS	CPU	MEMORIA	DISCO	TARJETAS DE RED
Puerta de acceso	<50	P4 o superior	2G	80G	2 ó más
	50 ó más	Xeon Dual core o superior	4G	160G	2 ó más
Infraestructura	<50	P4 o superior	1G	80G	1
	50 ó más	P4 o superior	2G	160G	1
Oficina	<50	P4 o superior	1G	250G	1
	50 ó más	Xeon Dual core o superior	2G	500G	1
Comunicaciones	<100	Xeon Dual core o equivalente	4G	250G	1
	100 ó más	Xeon Dual core o equivalente	8G	500G	1

Figura 2: Requerimientos Mínimos para instalar Zentyal
Fuente: https://wiki.zentyal.org/wiki/Es/3.5/Instalacion

Como se puede observar existen diferentes perfiles para poder instalar en el servidor Zentyal, en el presente proyecto se instala los perfiles **Puerta de acceso** y **Oficina**, ya que esto trabajara como puerta de enlace para seguridad contra entes externos a la institución y también como servidor de recursos compartidos.

4.9. Instalación y configuración de la distribución seleccionada.

ESQUEMA DE PRUEBA

Debido a que la Cooperativa no cuenta con los equipos necesarios para las pruebas de funcionalidad correspondiente, se optó por simular el ambiente de la institución utilizando equipos virtualizados, los equipos virtualizados necesarios son:

- **2 Sistemas MikroTik RouterOS:** es un sistema operativo basado en el kernel de Linux 2.6 que simulara los routers de la Cooperativa.
- **2 Servidores Zentyal 4.0:** un servidor principal y un servidor secundario que se encuentra en distintas agencias, lo que se propone con este esquema es que los dos servidores se sincronicen mutuamente para cumplir los requerimientos de la Cooperativa, que es tener un servidor disponible en todo momento y que no dependa solo del servidor principal.
- **1 Servidor Windows Server 2008:** este es el servidor que posee actualmente la Cooperativa que no le está dando el uso debido, este se va ha utilizar como un controlador de dominio Windows para facilitar la creación de las políticas de seguridad, unidades organizativas y usuarios.
- **2 Equipos Windows 7:** estos equipos simula los clientes que deben ser unidos al dominio Zentyal.

- **WinBox:** Es un software que permite la conexión al sistema MikroTik para facilitar su configuración.

En la Figura 3, se muestra el esquema de pruebas.

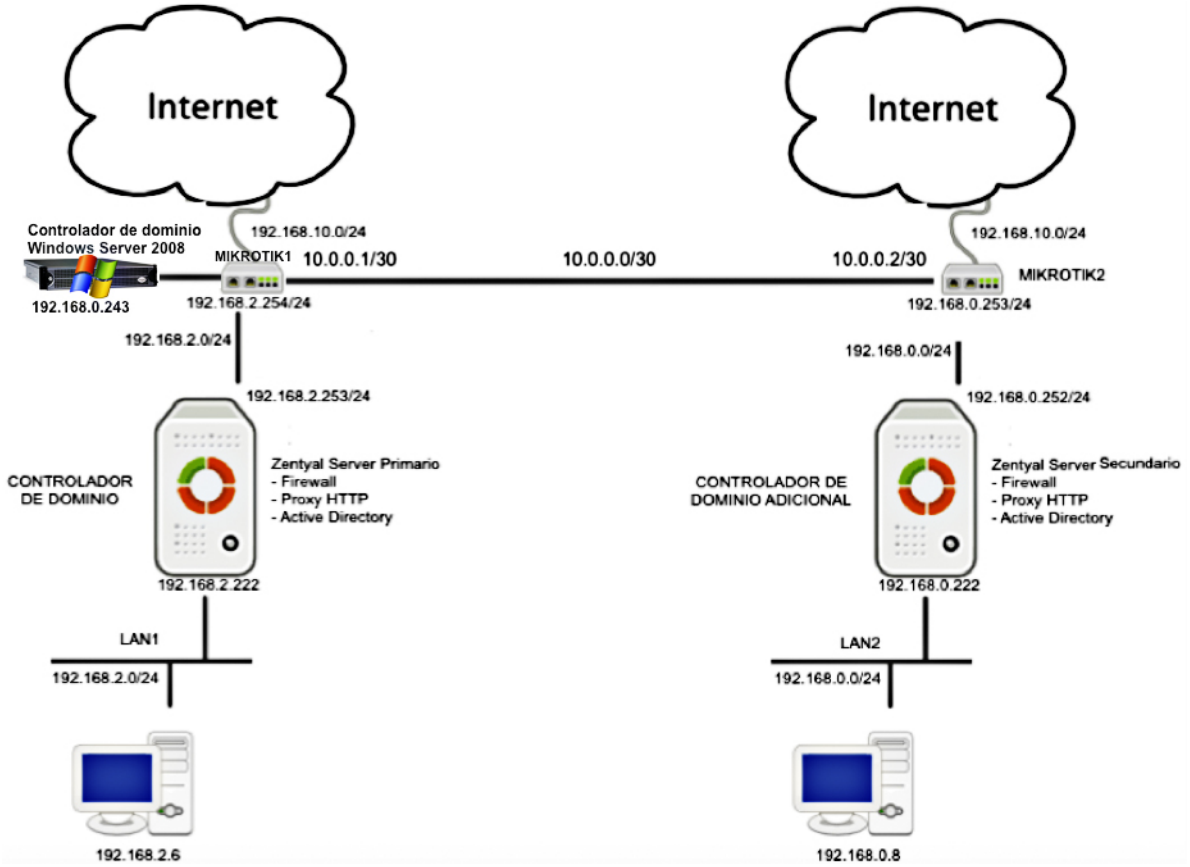


Figura 3: Esquema de pruebas.
Fuente: Elaborado por investigador.

Nota: La red LAN1 pertenece a la oficina matriz, mientras que la red LAN2 pertenece a la agencia de Ibarra.

4.9.1. Instalación de Zentyal 4.0

Para la instalación se Zentyal 4.0 se debe considerar los requerimientos de hardware del apartado 4.8, por lo que es necesario contar con otra tarjeta de red, ya que la versión de Zentyal que va ha ser instalada trabajara como puerta de acceso y servidor de recursos.

A continuación se detalla de las características de hardware necesario tanto para el servidor de dominio principal como secundario.

- 2 tarjetas de red.
- Memoria RAM de 1GB.
- Disco duro de 64 GB.

En la Figura 4, se muestra la configuración de hardware.

Figura 4: Resultado de la configuración física.
Fuente: Elaborado por investigador.

A continuación, en la Figura 5, se muestra la selección del idioma **Español** e **Install Zentyal 4.0 (delete all disk)** para la instalación correspondiente en el disco duro sin ninguna partición extra.

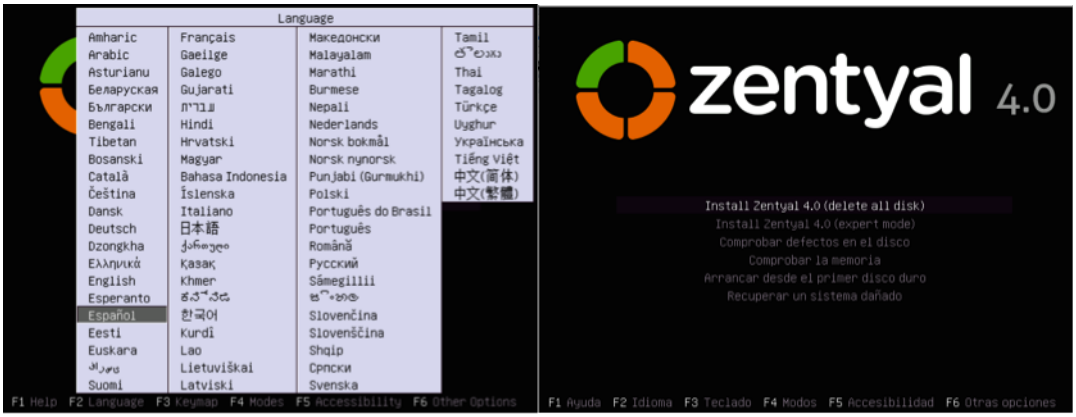


Figura 5: Selección de idioma Zentyal 4.0
Fuente: Elaborado por investigador.

Una vez que se selecciona el idioma se procede a seleccionar el nombre del país a donde se pertenece, la cual permite a Zentyal 4.0 fijar la zona horaria,

a continuación se muestra en la Figura 6 la selección de la ubicación para posteriormente definir la zona horaria del servidor.

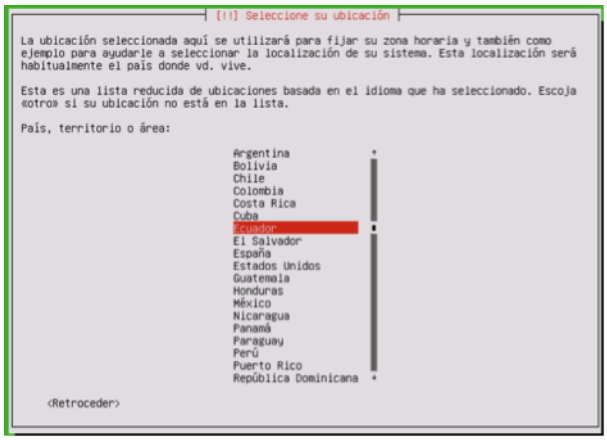


Figura 6: Selección de la ubicación para definir zona horaria.
Fuente: Elaborado por investigador.

A continuación se procede a la configuración del teclado, esto se lo realiza posicionado en la opción NO, esto ayudándose con la tecla Tab; en la Figura 7, se muestra la selección de la configuración de teclado según el idioma.

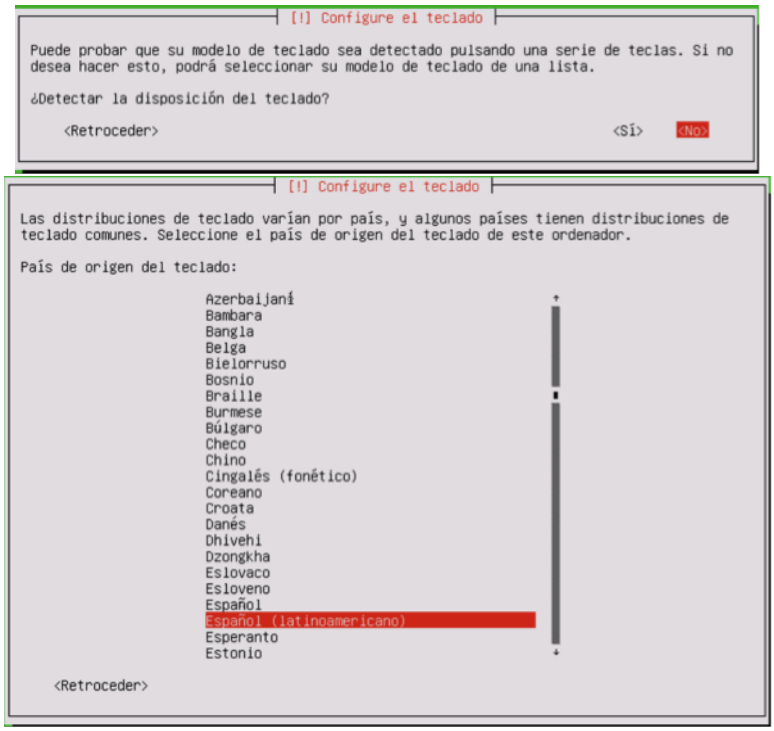


Figura 7: Selección de configuración de teclado según el idioma.
Fuente: Elaborado por investigador.

En el transcurso del proceso se solicita cierta información para continuar con

la instalación, como anteriormente en la configuración de hardware del servidor Zentyal se agregó una tarjeta de red adicional, entonces muestra una pantalla solicitando la selección de la tarjeta de red principal que sirve como enlace externo que en este caso es la del proveedor de internet.
A continuación se puede observar en la Figura 8 la selección de la tarjeta de red principal.

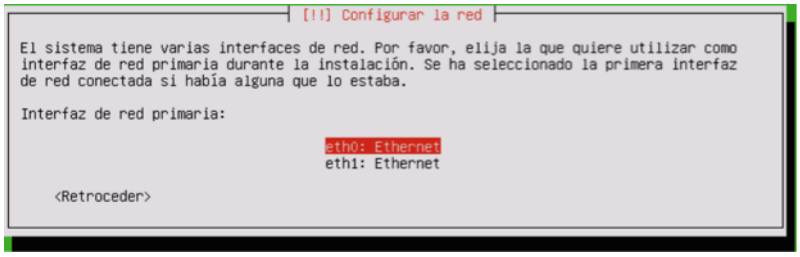


Figura 8: Selección de la tarjeta de red principal.
Fuente: Elaborado por investigador.

Seguidamente solicita el nombre del servidor Zentyal 4.0, que para el presente proyecto se lo ha llamado **ADEscencia,** en la Figura 9 se muestra el ingreso del nombre del servidor.

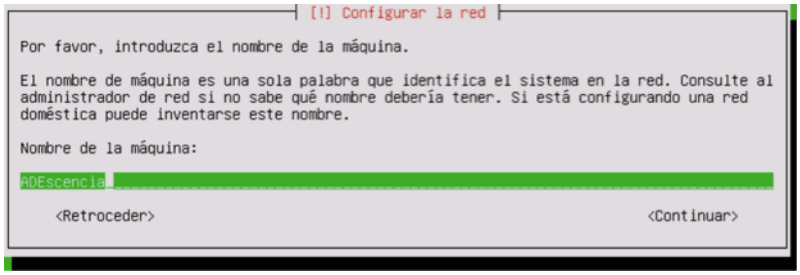


Figura 9: Asignación de nombre del servidor Zentyal 4.0.
Fuente: Elaborado por investigador.

En la Figura 10, se muestra el ingreso del nombre de usuario con el cual se puede ingresar al servidor; seguidamente, solicita el ingreso de la contraseña correspondiente al nuevo usuario que debe ser compleja para mayor seguridad.

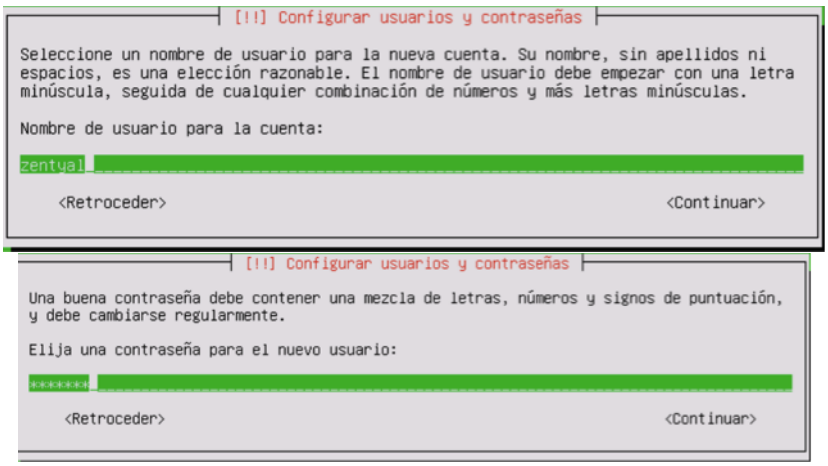


Figura 10: Asignación de nombre de usuarios y contraseña para ingreso al servidor Zentyal.
Fuente: Elaborado por investigador.

A continuación se muestra una pantalla de confirmación, donde se debe afirmar la zona horaria de la región geográfica donde se instala el servidor, así como se muestra en la Figura 11.

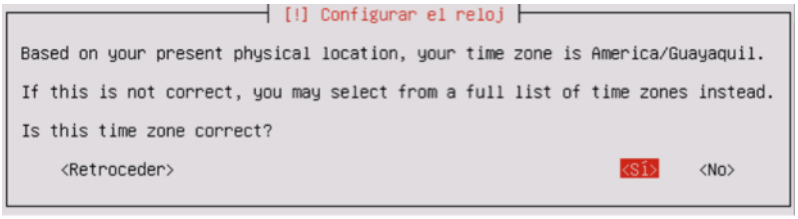


Figura 11: Confirmación de zona horaria.
Fuente: Elaborado por investigador.

Una vez confirmada la zona horaria, muestra una pantalla donde confirmando la culminación correcta de la instalación y posteriormente se procede a reiniciar el servidor.
Una vez que el servidor se haya reiniciado muestra una ventana de login donde se debe ingresar el usuarios y contraseña que fue creada en el transcurso de la instalación, así como se muestra en la Figura 12.

Figura 12: Inicio de sesión Zentyal 4.0.
Fuente: Elaborado por investigador.

4.9.2. Instalación de servicios necesarios en Zentyal 4.0

Una vez iniciado sesión se debe instalar los paquetes necesarios para el proyecto planteado, a continuación, en la Figura 13, se muestra la ventana de inicial de Zentyal para la instalación de los paquetes. A continuación se pulsa en continuar para proceder con la instalación de los paquetes necesarios.

Figura 13: Ventana inicial para instalación de paquetes.
Fuente: Elaborado por investigador.

Seguidamente muestra varios paquetes disponibles para ser instalados, del cual se selecciona **Domain Controller and File Sharing** como se muestra en la Figura 14, donde abarca todos los servicios necesarios.

Figura 14: Selección de paquetes a instalar.
Fuente: Elaborado por investigador.

En la siguiente Figura 15, se muestra el resumen de los paquetes que van a ser instalados posteriormente.

Figura 15: Resumen de los paquetes a ser instalados.
Fuente: Elaborado por investigador.

A continuación se procede a configurar las interfaces de red eth0 y eth1. Se selecciona eth0 como External, ya que por esta interfaz debe conectar a internet y el eth1 como Internal, ya que esto pertenece a la red LAN. La configuración se muestra en la Figura 16.

Figura 16: Configuración de tipos de interfaces.
Fuente: Elaborado por investigador.

En este paso se debe seleccionar el método de obtención de dirección IP, en este caso se elige eth0 con el método DHCP, porque no se conoce la dirección por la que sale a internet y eth1 con el método Static, donde se ingresa la dirección IP del servidor que es 192.168.2.222, como se muestra en la Figura 17.

Figura 17: Asignación de método de obtención de dirección IP.
Fuente: Elaborado por investigador.

Posteriormente se debe seleccionar el tipo se servidor que debe ser Servidor stand-alone ya que el servidor que se está configurando trabajará como servidor principal y estará ubicado en la Matriz. A continuación, digitar el nombre del dominio Zentyal, tal como se muestra en la Figura 18.

Figura 18: Selección de tipo de servidor e ingreso del nombre del dominio.
Fuente: Elaborado por investigador.

Cuando se da clic en **Finalizar** se muestra una ventana emergente donde notifica que se cambiará el nombre del host existente a la cual se confirma dando clic en **Ok**, como se muestra en la Figura 19.

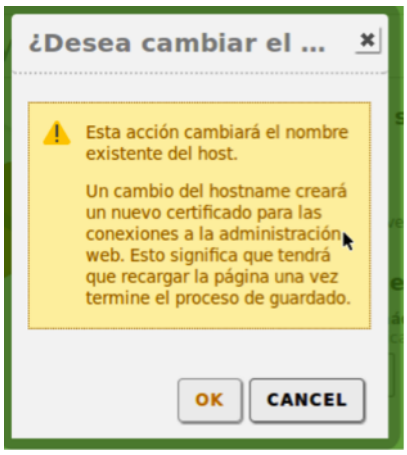


Figura 19: Notificación del cambio de nombre de host.
Fuente: Elaborado por investigador.

Nota: Cuando se haya instalado completamente se muestra una notificación de instalación completa, luego se hace clic en **Ir al Dashboard,** a continuación, se inicia Zentyal con todos los paquetes instalados, se recomienda que se actualice los paquetes para un mejor rendimiento del servidor.

4.9.3. Unir Windows Server 2008 como controlador de dominio a Zentyal

4.9.3.1. Instalación de características necesarias en Windows Server 2008.

Para proceder a la unir Windows Server 2008 como controlador de dominio a Zentyal se debe seguir los siguientes pasos:

1. En primer lugar se procede a instalar las características de Windows Server para manejo de Active Directory, para esto, se debe dirigir a **Inicio>Panel de control>Programas y características>Activar o desactivar las características de Windows,** así como se muestra en la Figura 20

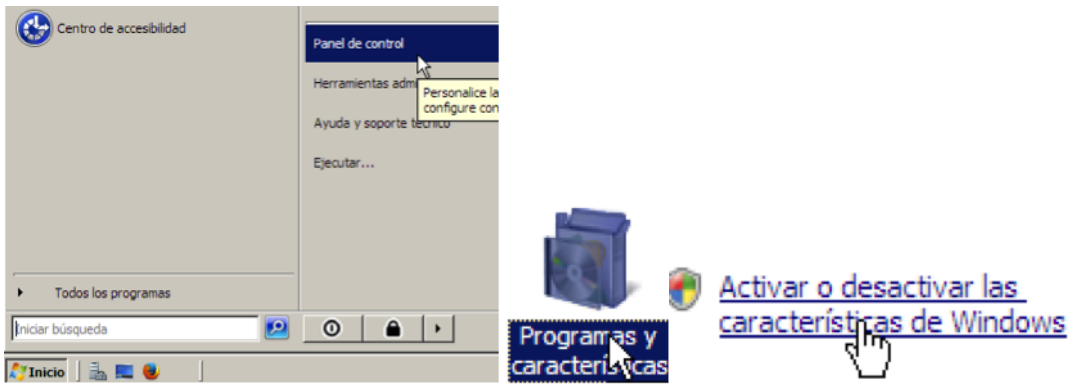


Figura 20: Activar características de Windows.
Fuente: Elaborado por investigador.

2. A continuación se muestra una ventana en el cual se debe ubicar en la pestaña **Resumen de características**; seguidamente, hacer clic en **Agregar características** y luego de se debe seleccionar las características **Administración de directivas de grupo y Herramientas del controlador de dominio de Active Directory**, finalmente dar clic en instalar para que se proceda a la instalación de las características seleccionadas, esto se muestra en la Figura 21.

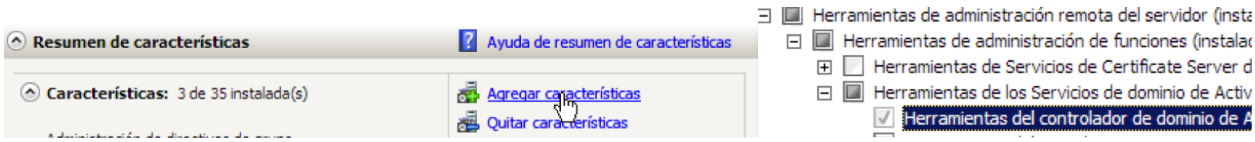


Figura 21: Selección de herramientas de controlador de dominio.
Fuente: Elaborado por investigador.

En la Figura 22, se muestra el proceso final de la instalación de las características seleccionadas en este paso.

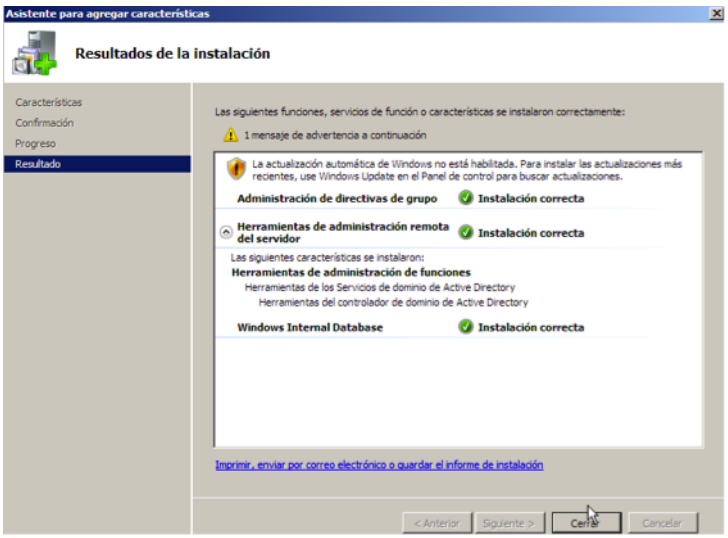


Figura 22: Proceso de instalación.
Fuente: Elaborado por investigador.

3. Una vez realizada la instalación de las características es necesario reiniciar el servidor para que los cambios se efectúen.

4.9.3.2. Unir al dominio de Zentyal

1. En Windows Server 2008 se procede a cambiar la configuración de red, para esto, se debe dirigir a la parte inferior derecha del escritorio y hacer clic derecho en el icono de red y posteriormente hacer clic en **Centro de redes y recursos compartidos > Administrar conexiones de red**, a continuación, hacer clic derecho en **conexión de área local** y hacer clic en **Propiedades**, como se muestra a continuación en la Figura 23.

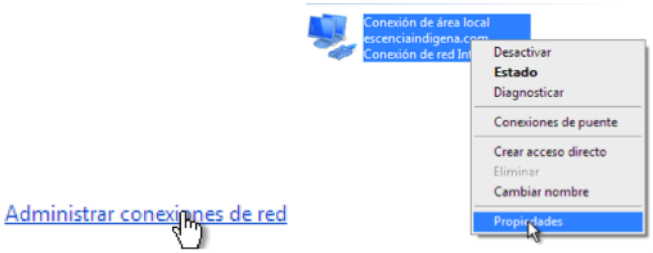


Figura 23: Configuración se red.
Fuente: Elaborado por investigador.

2. En este paso se debe seleccionar **Protocolo de internet versión 4 (TCP/IPv4)** para continuar con la configuración de la conexión de red, así como se muestra en la Figura 24.

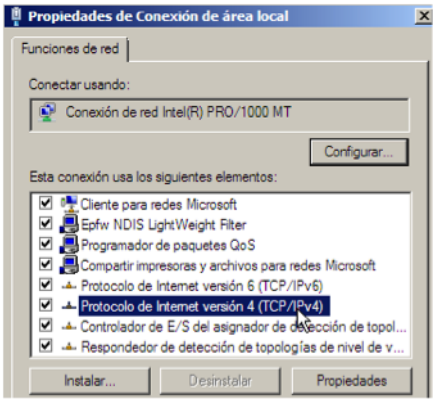


Figura 24: Propiedad de Conexión de área local.
Fuente: Elaborado por investigador.

3. En este paso se debe digitar la dirección IP del servidor Zentyal que es 192.168.2.222 como Servidor de DNS preferido para luego proceder a unir al dominio, así como se muestra en la Figura 25.

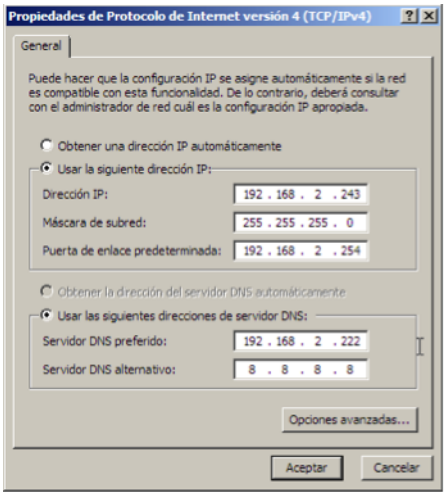


Figura 25: Configuración de DNS en Windows Server 2008.
Fuente: Elaborado por investigador.

4. Una vez cambiado la configuración de la red, se procede a comprobar la resolución del nombre del dominio con el comando **ping** desde el símbolo de sistema (CMD) de Windows, así como se muestra en la Figura 26.

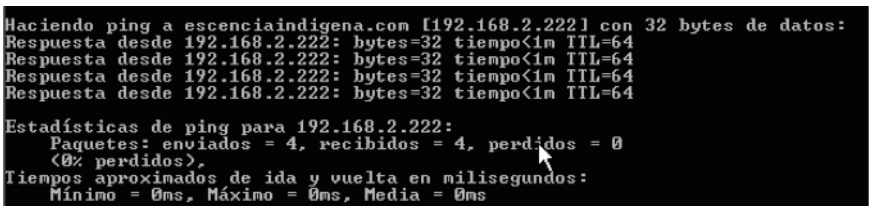


Figura 26: Prueba de conectividad de Windows a Zentyal.
Fuente: Elaborado por investigador.

5. Para unir al dominio Zentyal se debe dirigir al menú **Inicio**>Clic derecho en **Equipo>Propiedades>Cambiar configuración**, esta acción se muestra claramente en la Figura 27.

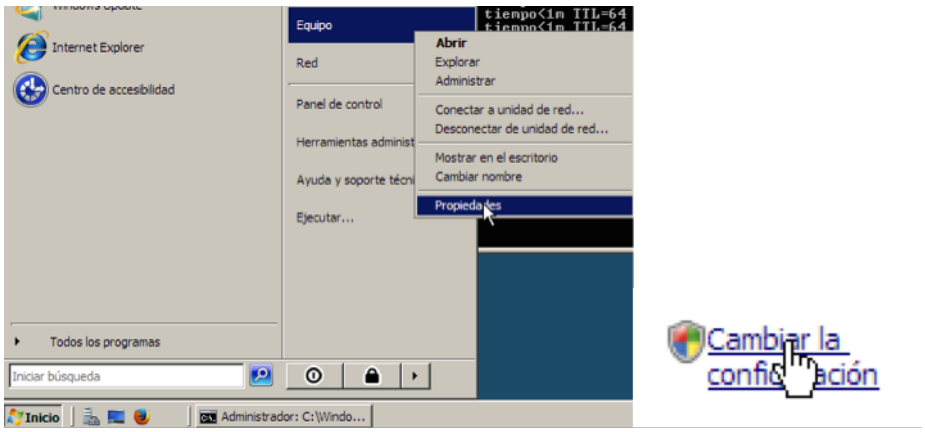


Figura 27: Unión de Windows Server 2008 a Zentyal.
Fuente: Elaborado por investigador.

6. A continuación se muestra otra ventana donde se debe hacer clic en **Cambiar**, posteriormente se selecciona **Dominio** y se procede a digitar el nombre del dominio Zentyal que es "escenciaindigena.com", finalmente hacer clic en **Aceptar** para que proceda a unir al dominio, esta acción se muestra en la Figura 28.

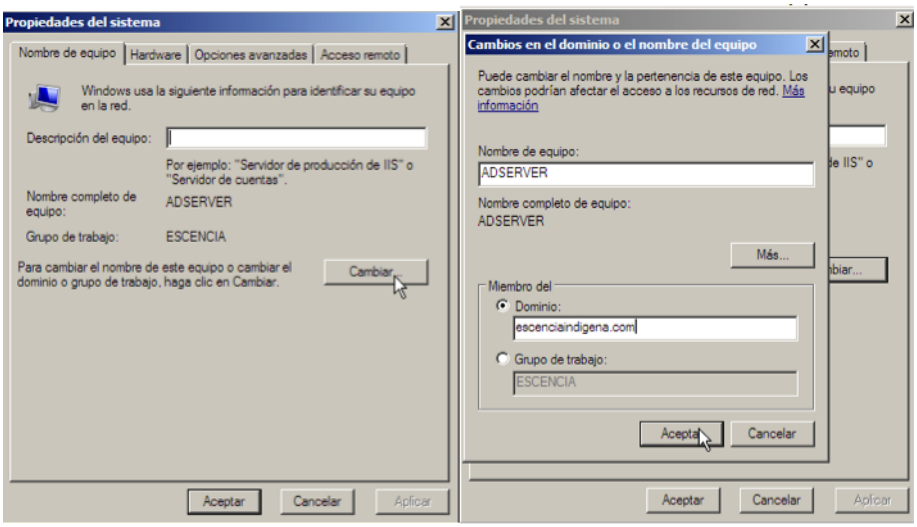


Figura 28: Agregar Windows Server 2008 al dominio Zentyal.
Fuente: Elaborado por investigador.

7. Seguidamente se puede visualizar otra ventana donde se solicita el ingreso del usuario administrador de Zentyal con su respectiva contraseña, como se muestra en la Figura 29.

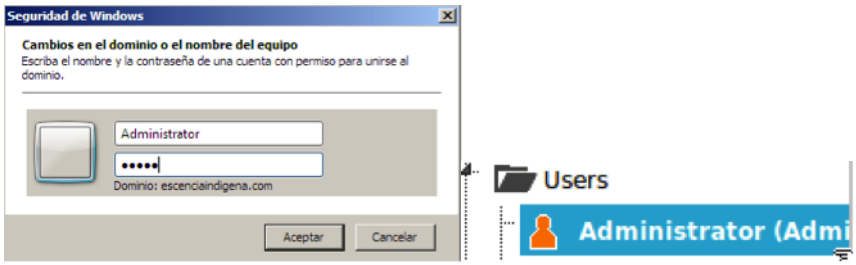


Figura 29: Login de usuario Zentyal en Windows Server y usuario Administrador de Zentyal.
Fuente: Elaborado por investigador.

8. Si se ingresó correctamente el usuario administrador de Zentyal se muestra un mensaje en el cual se notifica que se unió correctamente al dominio Zentyal y para que los cambios se apliquen se debe reiniciar el equipo, esta acción se muestra en la Figura 30.

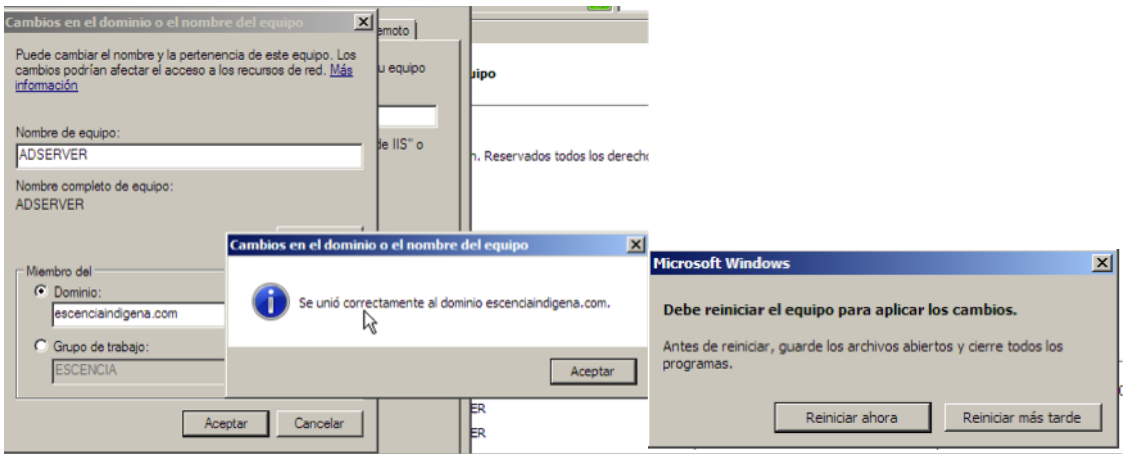


Figura 30: Notificación de unión exitosa al dominio Zentyal.
Fuente: Elaborado por investigador.

9. Una vez que se haya reiniciado el equipo solicita la contraseña del administrador del equipo, Figura 31. A esto se debe hacer clic en Cambiar de usuario, donde solicita el usuario administrador y contraseña del usuario administrador del servidor Zentyal, Figura 32.

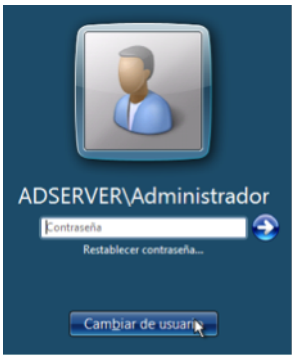


Figura 31: Login del usuario local del Administrador de Windows Server 2008.
Fuente: Elaborado por investigador.

Figura 32: Login del usuario Administrador de Zentyal.
Fuente: Elaborado por investigador.

10. Para comprobar que Windows Server 2008 se unió correctamente con el servidor Zentyal, se debe dirigir al menú **Inicio > Herramientas administrativas > Administración de directivas de grupo,** esta acción se muestra en la Figura 33.

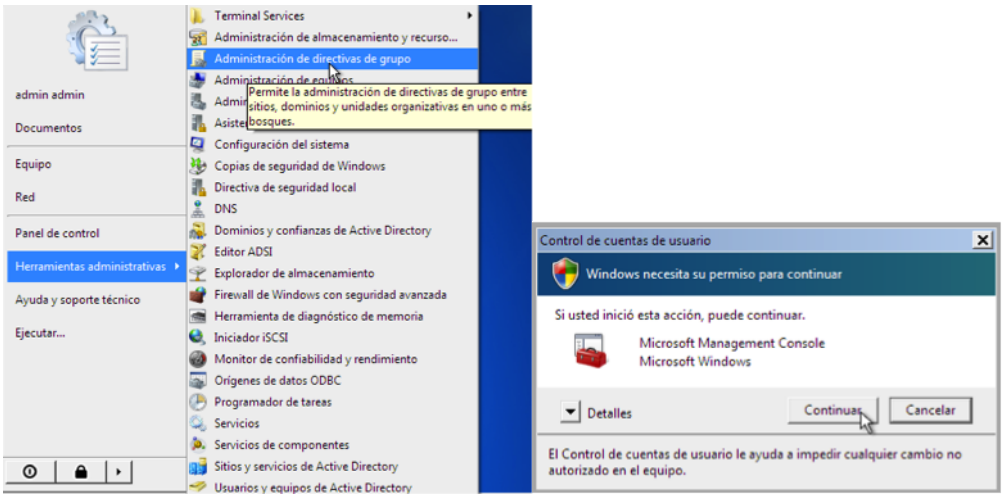


Figura 33: Comprobación de la unión correcta al dominio.
Fuente: Elaborado por investigador.

11. Como se puede observar el la Figura 34, las unidades organizativas del servidor Zentyal se refleja en el servidor Windows Server 2008 que está configurada como controlador de dominio, esto dando como un punto positivo para la administración de las directivas de grupo ya que se lo puede realizar desde el controlador de dominio o también del servidor Zentyal.

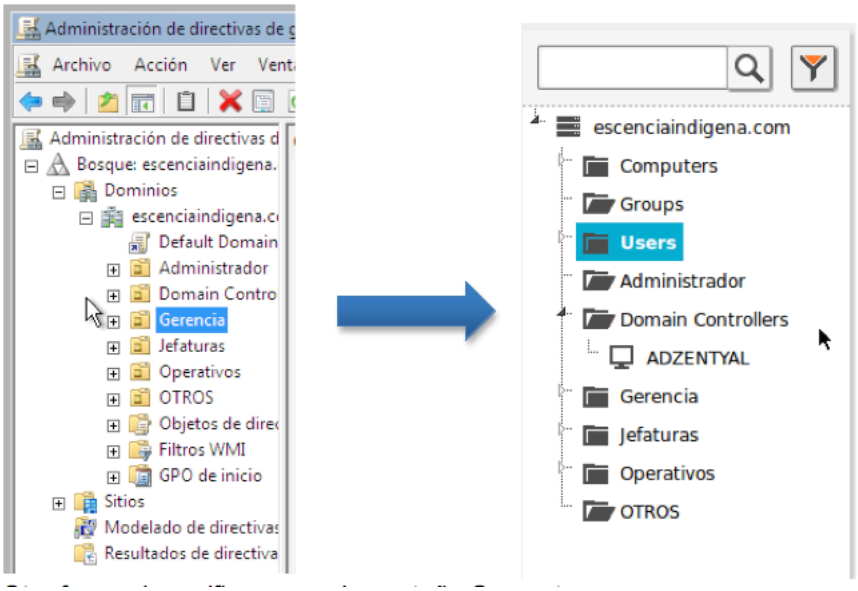


Figura 34: Prueba de sincronización entre el servidor Zentyal y el controlador de dominio.

Fuente: Elaborado por investigador.

4.9.4. Unir Windows 7 al dominio Zentyal

Para unir Windows 7 al dominio de Zentyal se debe seguir los siguientes pasos:

1. Hacer clic derecho en el icono de red de acceso rápido que se encuentra en la parte inferior derecha del escritorio, posteriormente hacer clic en la opción **Abrir Centro de redes y recursos compartidos > Cambiar configuración del Adaptador**, se muestra la conexión de área local en el cual se debe hacer clic derecho y seleccionar la opción **Propiedades**. Seleccionar el **Protocolo de Internet versión 4(TCP/Ipv4)** y hacer clic en el botón **Propiedades**, así como se muestra en la Figura 35.

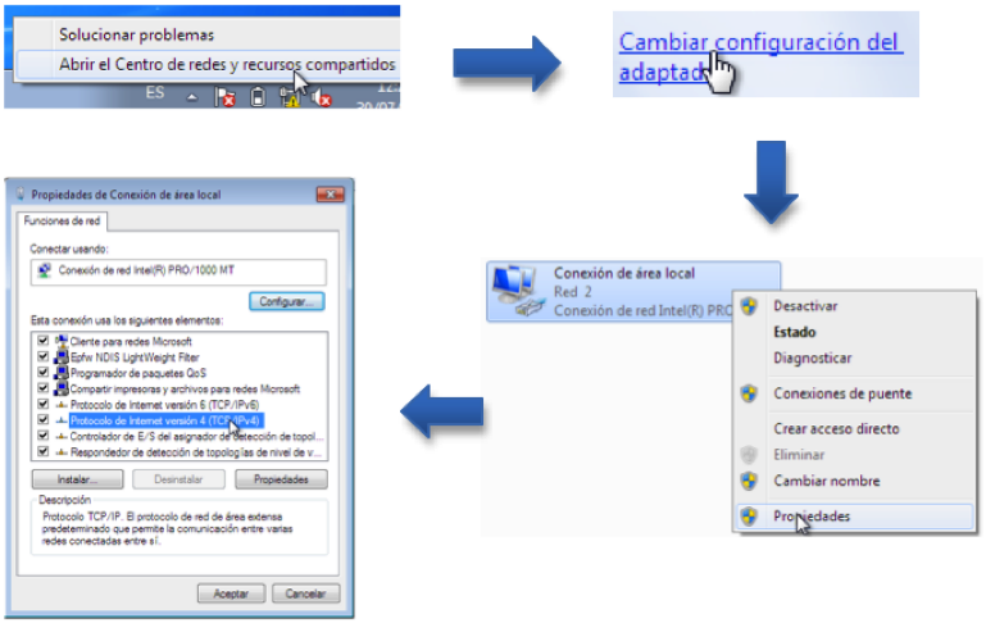


Figura 35: Proceso de cambio de dirección IP.
Fuente: Elaborado por investigador.

2. A continuación se asigna la dirección IP según la **tabla de distribución de direcciones IP** de la Cooperativa esta tabla se muestra en el **Anexo A.1**, como se muestra en la Figura 36.

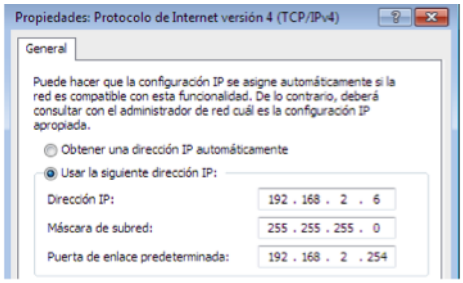


Figura 36: Asignación de IP según tabla de distribución de dirección IP de Cooperativa.
Fuente: Elaborado por investigador.

3. También se debe asignar el Servidor DNS que es la dirección IP del servidor Zentyal, este proceso se muestra en la Figura 37.

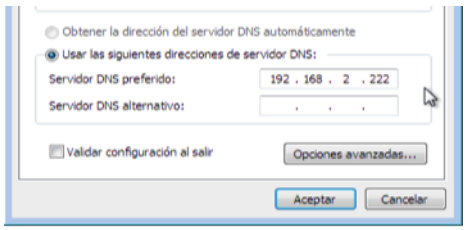


Figura 37: Asignación de servidor DNS.
Fuente: Elaborado por investigador.

Nota: el cambio de la dirección IP se puede verificar con el comando **ipconfig** desde el sistema de comandos (CMD) de Windows.

4. Luego del paso anterior debe dirigirse a **Inicio > Equipo >** Clic derecho **> Propiedades**, como se muestra en la Figura 38.

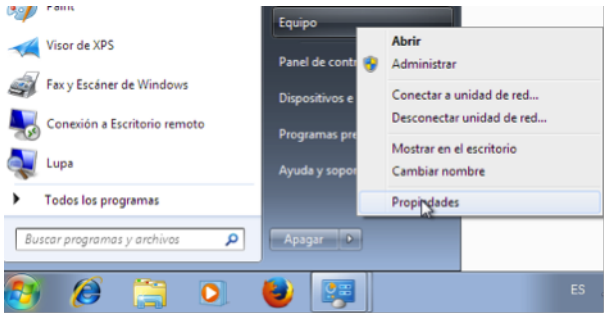


Figura 38: Propiedad del equipo a ser unido al dominio.
Fuente: Elaborado por investigador.

5. A continuación se debe dirigir a la parte inferior derecha de aquella ventana y hacer clic en **Cambiar configuración**.

6. Seguidamente de debe hacer clic en el botón Cambiar y posteriormente se ingresar el dominio creado en el servidor Zentyal que es **escenciaindigena.com**, finalmente hacer clic en **Aceptar** para que se efectúen los cambios, este proceso se muestra en la Figura 39.

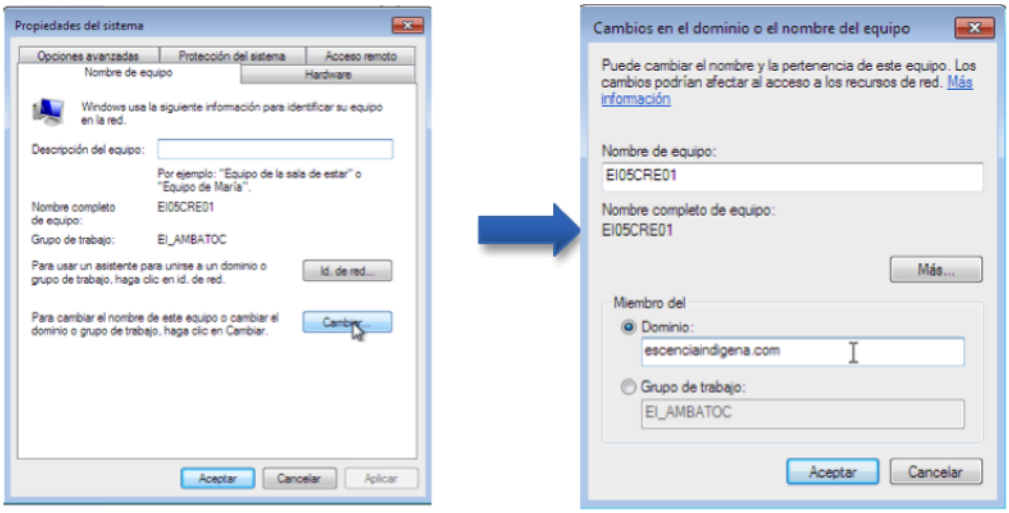


Figura 39: Ingreso del dominio Zentyal 4.0 en el equipo usuario.
Fuente: Elaborado por investigador.

7. A continuación aparece una ventana emergente donde solicita el ingreso del nombre del usuario y contraseña del administrador del servidor Zentyal, esta acción se muestra en la Figura 40.

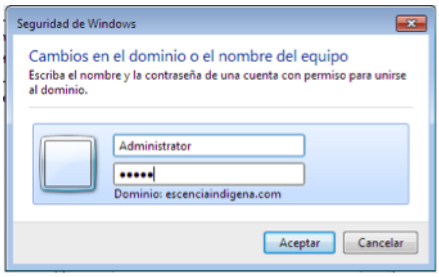


Figura 40: Ingreso del usuario administrador de Zentyal 4.0 para unirse al dominio.
Fuente: Elaborado por investigador.

8. Si se ingresó correctamente muestra un mensaje en el cual se notifica que se unió correctamente al dominio y para que los cambios se apliquen se debe reiniciar el equipo. Esta acción se muestra en la Figura 41.

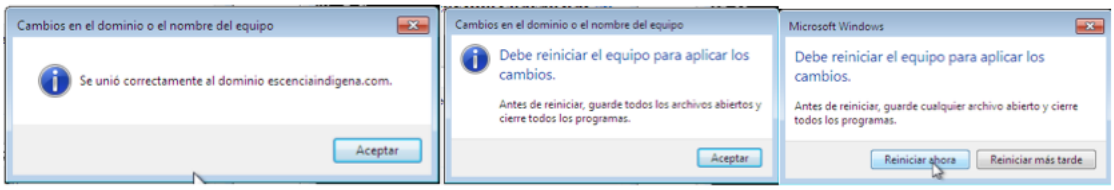


Figura 41: Secuencia de ventanas emergentes antes de reiniciar el equipo.
Fuente: Elaborado por investigador.

9. Una vez que se haya reiniciado el equipo aparece un inicio de sesión similar a la Figura 42, a esto se debe hacer clic en el botón **Cambiar Usuario** para posteriormente ingresar el usuario y contraseña del usuario que ha sido creado en el servidor Zentyal.

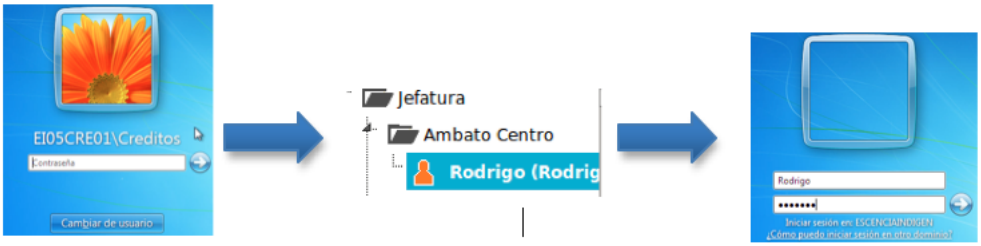


Figura 42: Ventana de inicio de sesión usuario.
Fuente: Elaborado por investigador.

10. Existen varias formas de verificar que el equipo se encuentra unido correctamente al dominio, la primera es directamente desde el equipo mismo en el Menú **inicio** en el cual muestra el nombre del usuario, la segunda es desde el servidor Zentyal en el menú **Usuarios y Equipos> Gestionar**. Estas acciones se muestran en las Figura 43.

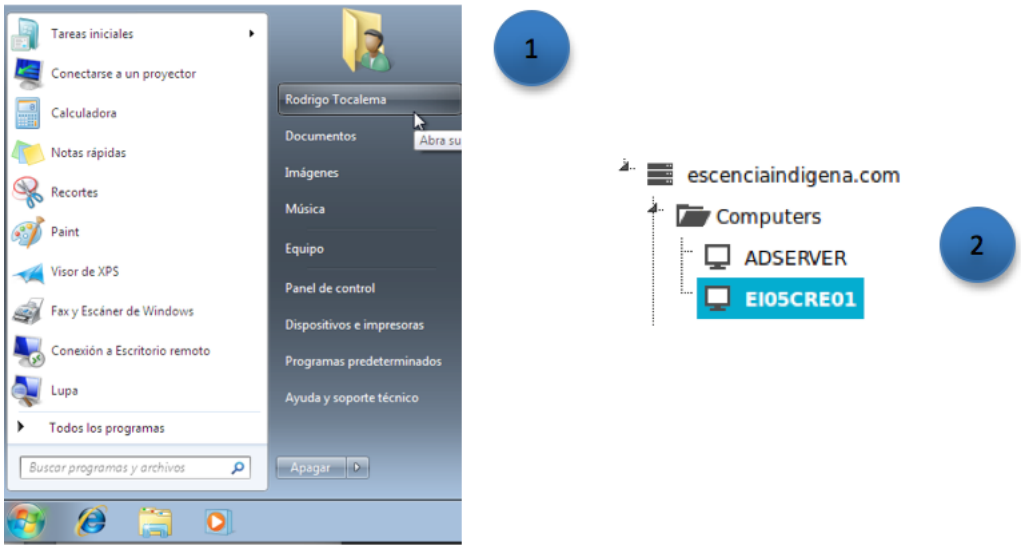


Figura 43: Formas de comprobar la unión correcta al dominio Zentyal.
Fuente: Elaborado por investigador.

4.9.5. Unir Zentyal secundario como controlador de dominio adicional

Para realizar la unión del servidor secundario al servidor principal se procede con los siguientes pasos:

En primer lugar se debe revisar las siguientes informaciones independientemente del servidor al que pertenezca.

- **Servidor Principal (Controlador del dominio)**
  - Dirección IP: 192.168.2.222
  - Dominio: escenciaindigena.com
  - Nombre de Maquina: ADEscencia
  - Nombre de dominio NetBIOS: escencia
  - DNS: 192.168.2.222
- **Servidor Secundario (Controlador de dominio adicional)**
  - Dirección IP: 192.168.0.222
  - Dominio: escenciaindigena.com
  - Nombre de Maquina: ADEscencia2
  - Nombre de dominio NetBIOS: escencia
  - DNS: 192.168.0.222 y 192.168.2.222

Nota: En caso de no tener esta configuración se debe realizar los cambios necesarios.

A continuación se comprueba que el servidor secundario tiene conectividad con el servidor principal, también es necesario verificar si resuelve el nombre de dominio del servidor principal como **ADEscencia.escenciaindigena.com**, esta verificación se lo debe hacer desde el servidor secundario, si no tiene ninguna conexión se debe agregar la dirección IP del servidor principal al DNS del servidor secundario.
En el servidor Zentyal principal se debe dirigir al menú **Dominio> Configuración,** en este apartado muestra la información del servidor principal que se encuentra configurado como controlador de dominio, esta acción se muestra e la Figura 44.

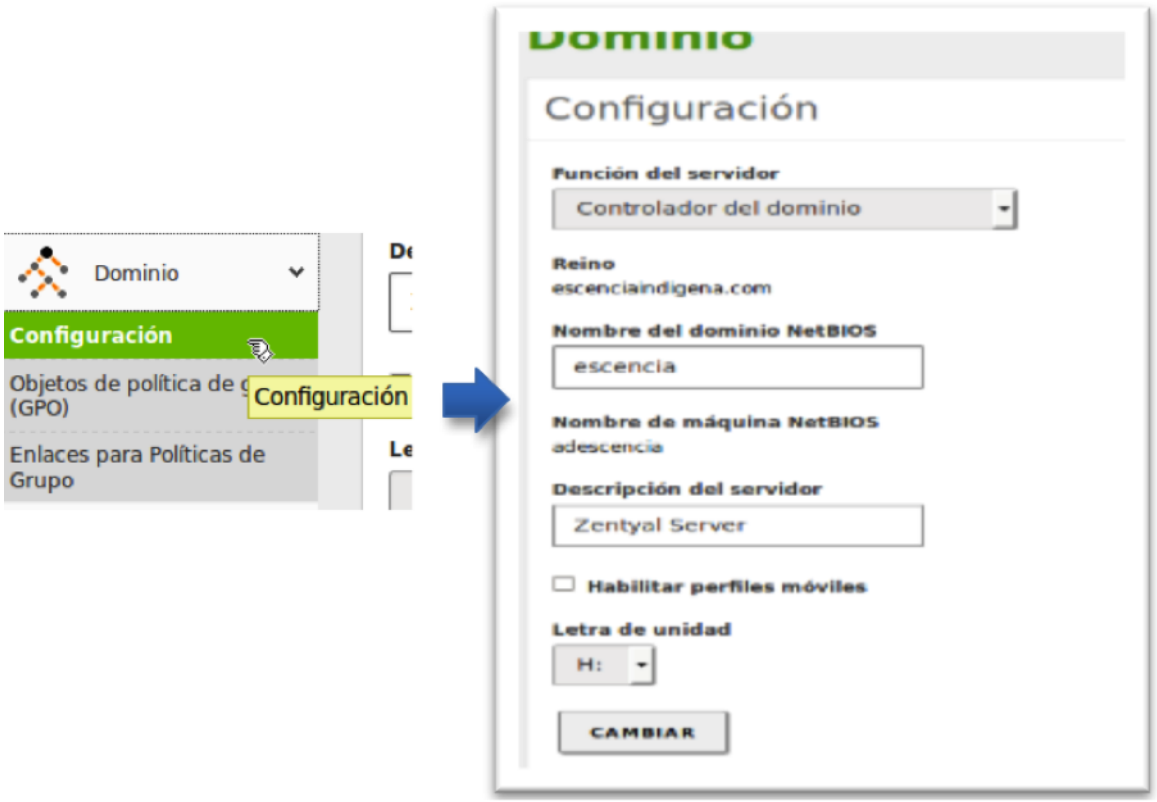


Figura 44: Inicio de configuración de Controlador de Dominio.
Fuente: Elaborado por investigador.

En el servidor secundario se debe dirigir al mismo menú, pero en este servidor se debe configurar como servidor de dominio adicional, para esto, se debe seleccionar la opción Controlador de dominio adicional. A continuación se debe llenar los campos necesarios con la información del servidor principal, así como se muestra en la Figura 45.

Figura 45: Configuración del controlador de dominio adicional.
Fuente: Elaborado por investigador.

Una vez ingresado los campos necesarios se procede a guardar los cambios, en este proceso muestra dos ventanas emergentes consecutivamente, en la primera ventana advierte que si se une al dominio se perderá todos los usuarios y grupos del servidor secundario, la segunda ventana emergente confirma que ha sido guardado correctamente los cambios, esta acción se muestra en la Figura 46.

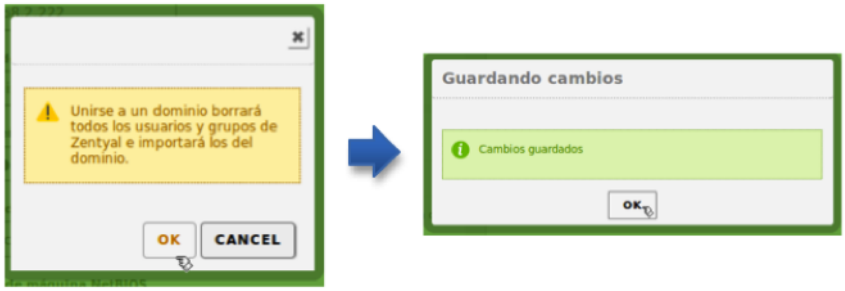


Figura 46: Ventanas de notificación.
Fuente: Elaborado por investigador.

4.9.6. Configuración del servidor

4.9.6.1. Creación de unidades organizativas

Para la creación de unidades organizativas se procede con los siguientes pasos:

1. En el servidor Zentyal 4.0 se debe dirigir a **Usuarios y Equipos** > **Gestionar** donde se muestra los usuarios y unidades organizativas que

viene por defecto en el servidor, esta acción se muestra en la Figura 47.

Figura 47: Usuarios y Equipos
Fuente: Elaborado por investigador.

2. En la parte inferior hacer clic en **Añadir Nuevo** en el cual posteriormente aparece una ventana emergente donde solicita el ingreso del nombre de la unidad organizativa, en la Figura 48, se muestra la acción mencionada.

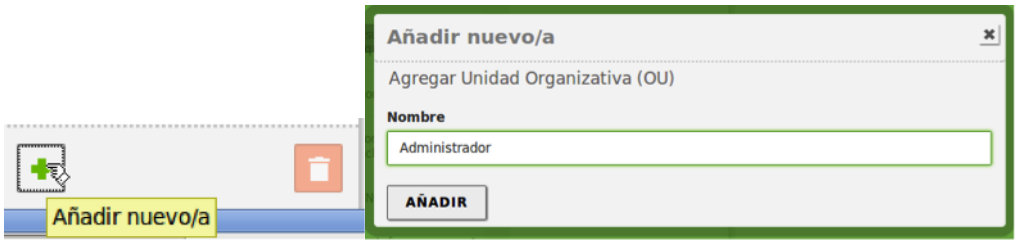


Figura 48: Creación de la unidad organizativa.
Fuente: Elaborado por investigador.

3. Se deben crear las unidades organizativas mencionadas en el apartado **4.7** del presente proyecto.

4.9.6.2. Creación de grupos de trabajo

En el servidor Zentyal 4.0 se debe situar en la carpeta **Grupos** y posteriormente hacer clic en **Añadir nuevo**. A continuación se debe seleccionar **Grupo de seguridad** y proceder con el llenado de los campos necesarios, finalmente se debe hacer clic en **Añadir** para la creación de la misma.
A continuación, en la Figura 49, se muestra el proceso de creación de Grupos de trabajo.

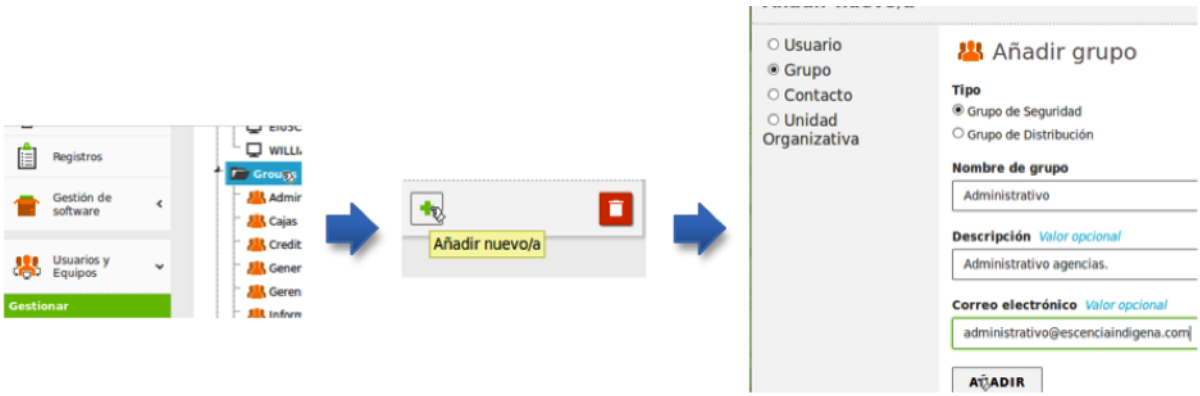


Figura 49: Proceso para la creación de grupos de trabajo.
Fuente: Elaborado por investigador.

Nota: Se creó los grupos como antes ya se ha mencionado en el apartado **4.7** del presente proyecto.

4.9.6.3. Creación y asignación de directivas de grupo

Para crear las políticas de seguridad se procede a seguir los siguientes pasos:

1. Dirigirse a **Inicio > Herramientas administrativas > Administración de directivas de grupo**; seguidamente, hacer clic en el dominio y finalmente hacer clic en Objetos de directivas de grupo, así como se muestra en la Figura 50.

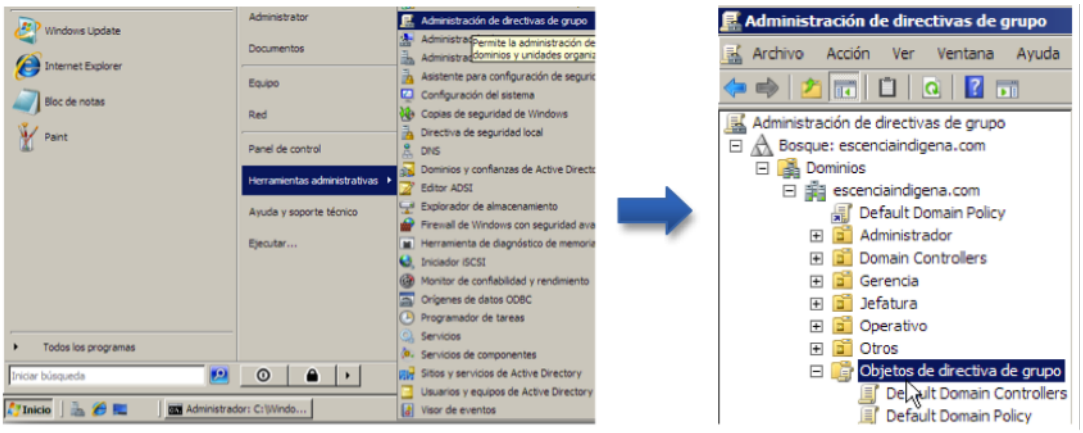


Figura 50: Pasos para el ingreso al Administrador de directivas de grupo.
Fuente: Elaborado por investigador.

2. El siguiente paso es crear unas directivas de grupos llamados Administrador, Operativos, Jefaturas, Gerencia y Otros, para esto, se debe dar clic derecho en el apartado donde se encuentran las directivas de grupo y seleccionar

Nuevo; seguidamente, solicita el ingreso del nombre de la directiva de grupo, este proceso se muestra en la Figura 51.

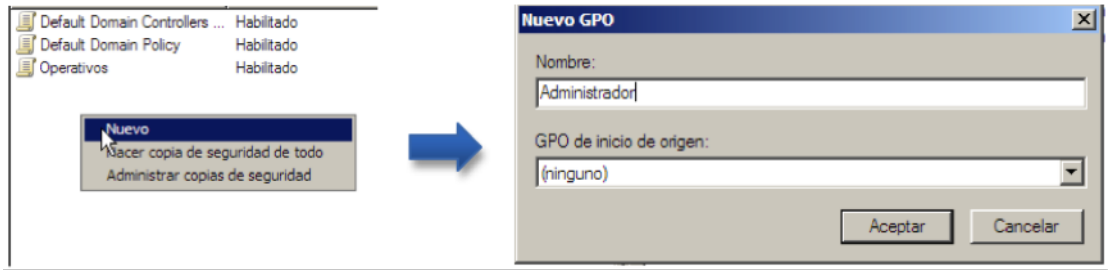


Figura 51: Creación de GPOs.
Fuente: Elaborado por investigador.

3. Luego de la creación de las directivas de grupo se despliega la unidad organizativa **Operativo** para proceder a asignar la política creada para dicha unidad organizativa, para esto, se debe arrastrar la directiva de grupo a cada una de las sub unidades organizativas al que pertenece independientemente, esta acción se muestra más detalladamente en la Figura 52.

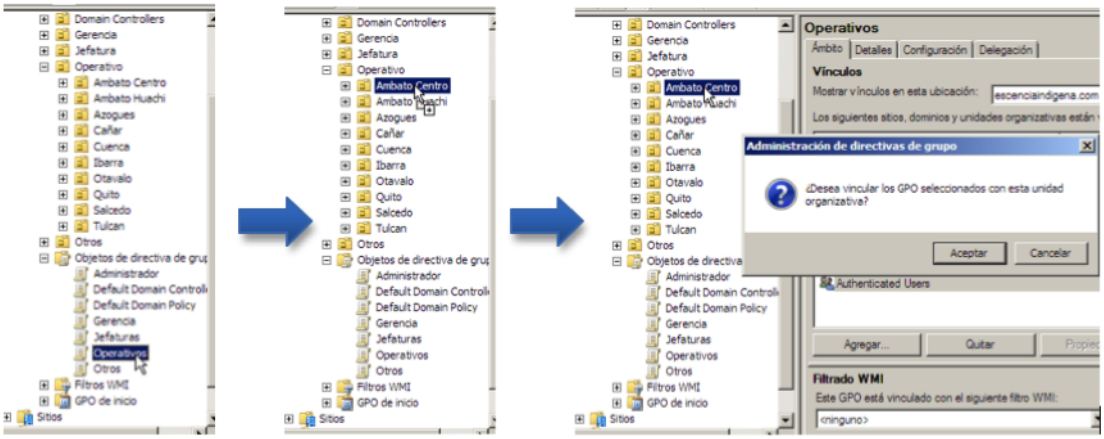


Figura 52: Asignación de GPOs a las unidades organizativas.
Fuente: Elaborado por investigador.

Nota: Una vez arrastre la directiva de grupo a su respectiva unidad organizativa muestra una ventana emergente donde se debe confirmar que si desea vincular el GPO seleccionado con la unidad organizativa.

4.9.6.4. Edición de las políticas de seguridad

Para la edición de las directivas de grupo se procede a hacer clic derecho en la política de grupo y seleccionar **Editar**. A continuación se abre una ventana donde

se debe dirigir a **Configuración** de usuario, desplegar la carpeta **Directivas> Plantillas administrativas**, esta acción se muestra en la Figura 53.

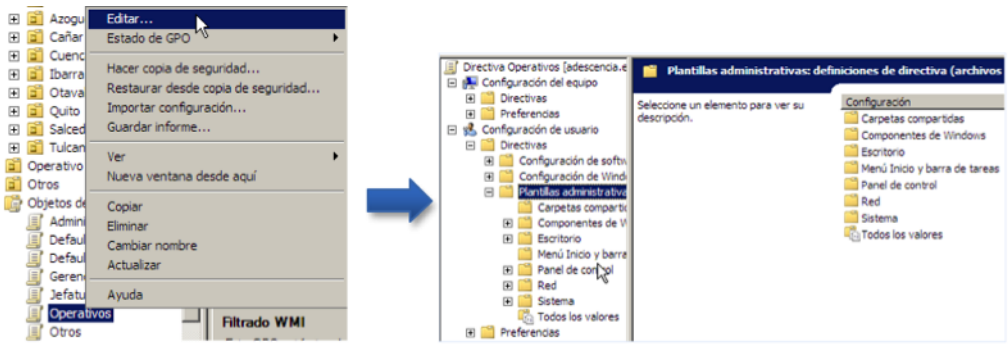


Figura 53: Edición de la GPO.
Fuente: Elaborado por investigador.

4.9.6.5. Implementación de las Políticas de Seguridad en el servidor Zentyal

Para la creación de políticas de seguridad se utiliza el controlador de dominio Windows Server 2008 que la Cooperativa posee actualmente.

1. El usuario no puede modificar la dirección IP del equipo.

   a) Esta configuración se encuentra en **Directivas>Plantillas administrativas>Red>Conexiones de red > Prohibir el acceso a las propiedades de una conexión LAN**, en la cual solo se debe habilitar, esta acción se muestra en la Figura 54.

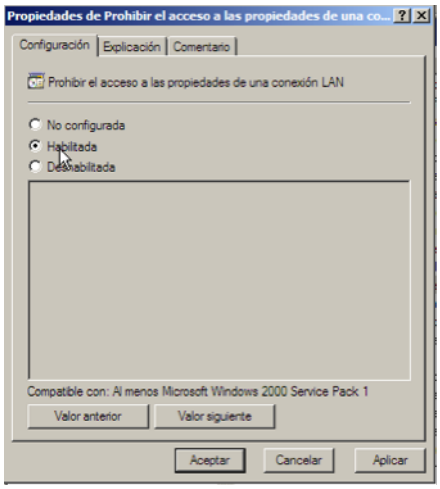


Figura 54: Habilitación de propiedad de prohibir el acceso a las propiedades de una conexión LAN.
Fuente: Elaborado por investigador.

b) A continuación, en la Figura 55, se muestra el resultado de la configuración realizada.

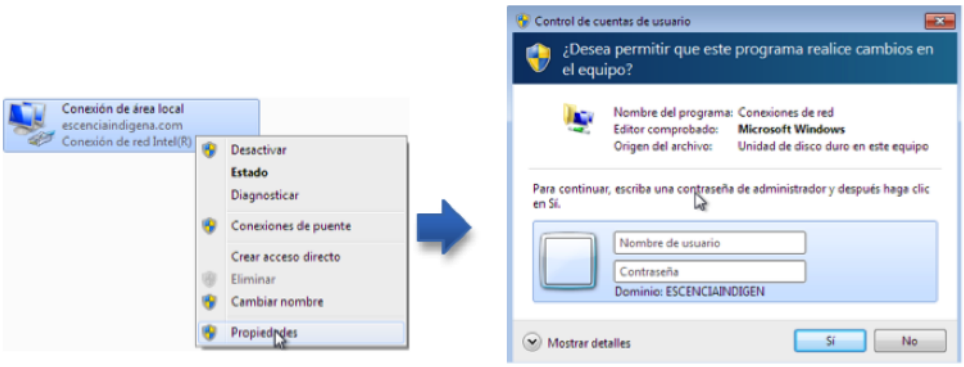


Figura 55: Resultado de configuración.
Fuente: Elaborado por investigador.

2. El usuario no puede activar y desactivar las conexiones de red local del equipo.

   a) Esta configuración se encuentra en **Directivas > Plantillas administrativas > Red > Conexiones de red > Capacidad de habilitar y deshabilitar una conexión LAN**, en la cual solo se debe habilitar, esta acción se muestra en la Figura 56.

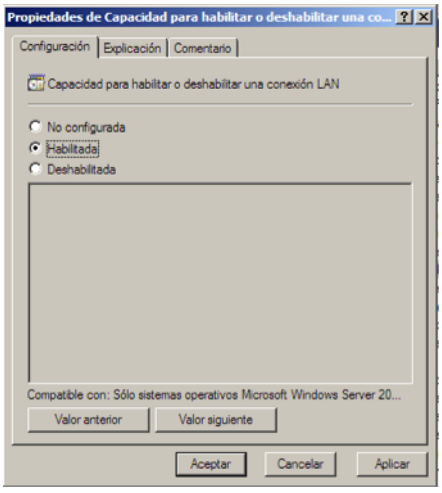


Figura 56: Habilitación de propiedad de capacidad para habilitar o deshabilitar una conexión LAN.
Fuente: Elaborado por investigador.

   b) A continuación, en la Figura 57, se muestra el resultado de la configuración realizada.

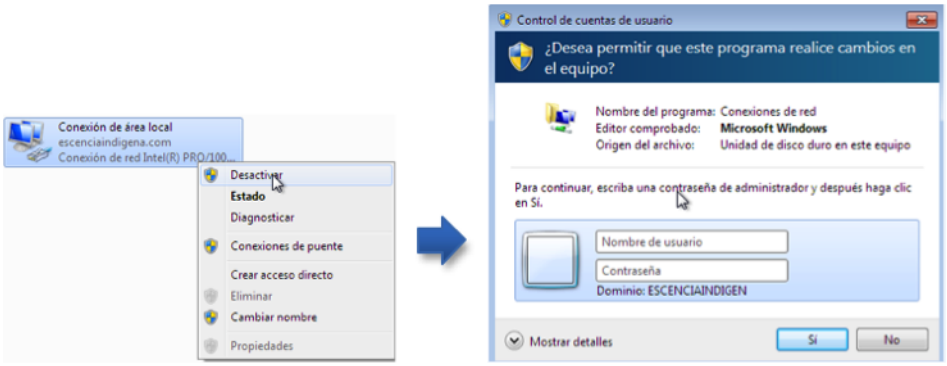


Figura 57: Resultado de configuración.
Fuente: Elaborado por investigador.

3. El usuario no puede cambiar el fondo de pantalla del equipo.

   a) Para cumplir con esta restricción en la directiva de grupo **Directivas > Plantillas administrativas > Escritorio > Escritorio > Tapiz del escritorio**, como se muestra en la Figura 58.

Figura 58: Ubicación de la propiedad Tapiz del escritorio.
Fuente: Elaborado por investigador.

   b) Seleccionar la opción habilitada e ingresar la dirección de la carpeta compartida del servidor donde se encuentran la imagen de fondo para el escritorio, si se desea también se puede modificar el estilo del papel tapiz, así como se muestra en la Figura 59.

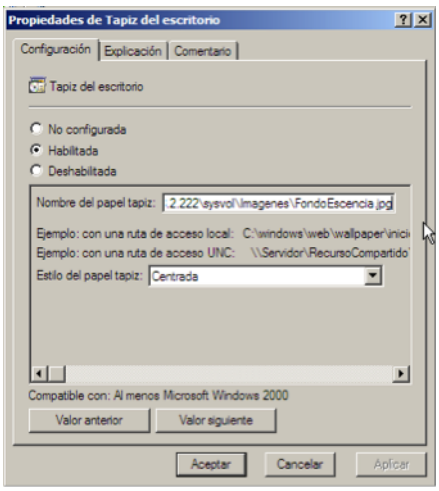


Figura 59: Habilitación de propiedad Tapiz del escritorio.
Fuente: Elaborado por investigador.

Nota: la carpeta compartida debe estar en el servidor Zentyal, por defecto la carpeta compartida es \\192.168.2.222\sysvol.

c) A continuación se habilita la configuración que se encuentra en **Directivas>Plantillas administrativas>Panel de control>Pantalla>Impedir cambios en el papel tapiz**, así como se muestra en la Figura 60.

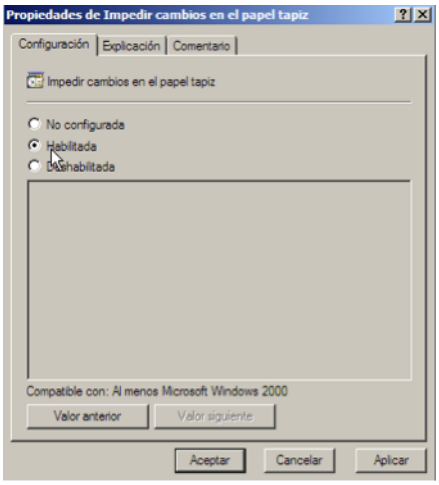


Figura 60: Habilitación de propiedad de impedir cambios en el papel tapiz.
Fuente: Elaborado por investigador.

d) Finalmente hacer clic en Aceptar para que se efectúe los cambios y en el equipo de usuario se debe cerrar sesión e iniciarlo nuevamente.

e) A continuación, en las Figuras 61 y 62, se muestra el resultado de la política configurada independientemente a las propiedades habilitadas.

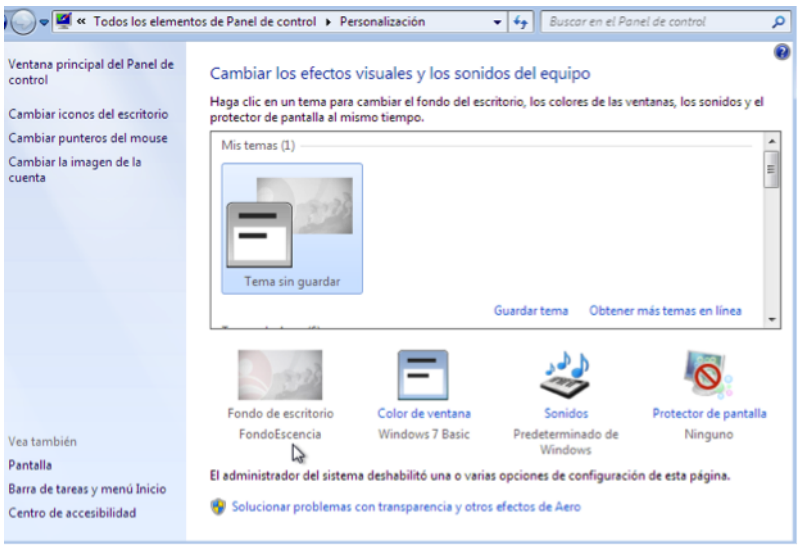


Figura 61: Resultado de impedir cambio de papel tapiz
Fuente: Elaborado por investigador.

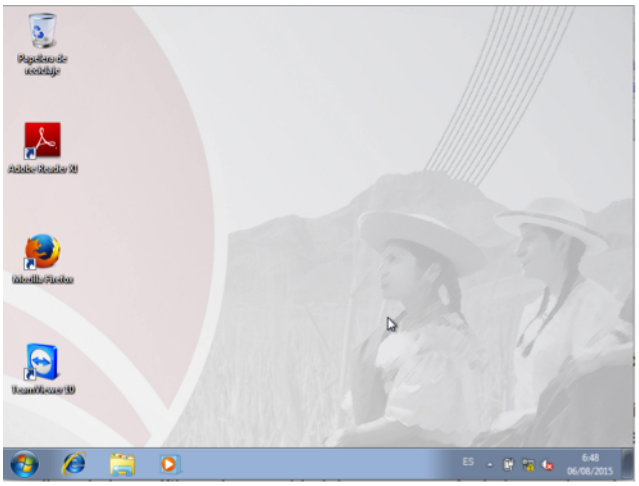


Figura 62: Resultado de Tapiz de escritorio.
Fuente: Elaborado por investigador.

4. El usuario no puede cambiar la apariencia de escritorio.

   a) Esta configuración se encuentra en **Directivas > Plantillas administrativas > Panel de control > Pantalla > Temas del Escritorio > Quitar la opción tema**, solo tiene que habilitarlo como se muestra en la Figura 63.

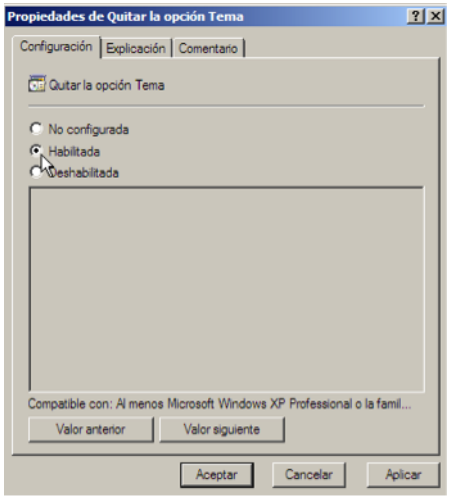


Figura 63: Habilitación de propiedad de quitar la opción Tema.
Fuente: Elaborado por investigador.

b) A continuación, en la Figura 64, se muestra el resultado de la configuración realizada, como se puede observar los temas se han bloqueado para que no puedan hacer cambios.

Figura 64: Resultado de quitar opción tema.
Fuente: Elaborado por investigador.

5. El usuario no puede ejecutar cualquier instalador sin la debida autorización de los administradores de red.

   a) Esta configuración se encuentra en **Directivas > Plantillas administrativas > Componentes de Windows > Windows Installer > Instalar siempre con privilegios elevados**, solo tiene que habilitarse como se muestra en la Figura 65.

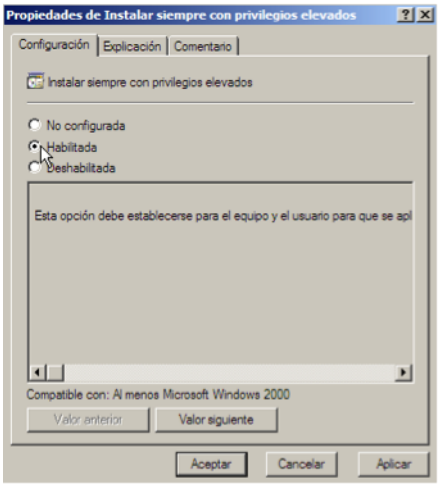


Figura 65: Habilitación de propiedad de instalar con privilegios elevados.
Fuente: Elaborado por investigador.

b) A continuación, en la Figura 66, se muestra el resultado de la configuración realizada, como se puede observar es necesario tener privilegio de administrador para instalar cualquier aplicación.

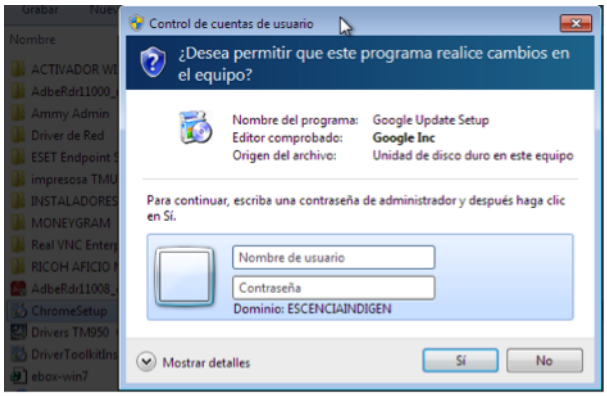


Figura 66: Resultado de la instalación con privilegios.
Fuente: Elaborado por investigador.

6. El usuario no debe insertar dispositivos de almacenamiento externos como USBs o CDs en el equipo.

   a) Esta configuración se encuentra en **Directivas > Plantillas administrativas > Sistema > Acceso de almacenamiento extraíble > Todas las clases de almacenamiento extraíble**, solo tiene que habilitarse como se muestra en la Figura 67.

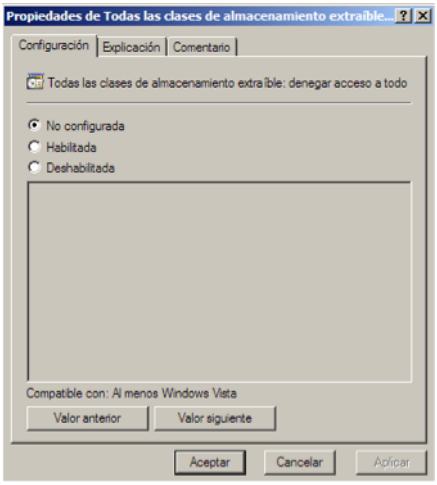


Figura 67: Habilitación de propiedad para denegar el acceso a toda clase de almacenamiento extraíble.
Fuente: Elaborado por investigador.

b) A continuación, en la Figura 68, se muestra el resultado de la configuración realizada.

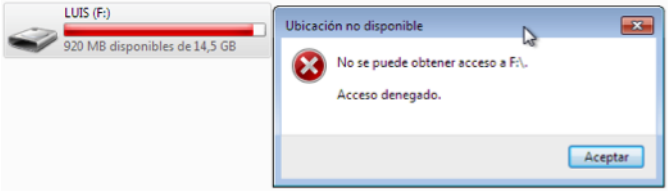


Figura 68: Resultado denegación de acceso a medios de almacenamientos extraíbles.
Fuente: Elaborado por investigador.

7. El usuario no debe iniciar cesión en el equipo sin seguridad alguna.

a) Esto se lo resuelve con tal solo unir al dominio Zentyal, ya que los usuarios con sus respectivas claves están almacenados en el servidor. A continuación se muestra en la Figura 69.

Figura 69: Inicio de sesión terminal de usuario.
Fuente: Elaborado por investigador.

8. El usuario debe ejecutar aplicaciones específicas como: Word, Excel, internet Explorer, Adobe Reader, entre otras aplicaciones necesarias para el trabajo diario de los usuarios.

   a) Para esta configuración se procede a ir a **Directivas > Plantillas administrativas > Sistema > Ejecutar solo aplicaciones específicas de Windows**, en el cual solo se debe habilitar y agregar las extensiones de las aplicaciones, esta acción se muestra en la Figura 70.

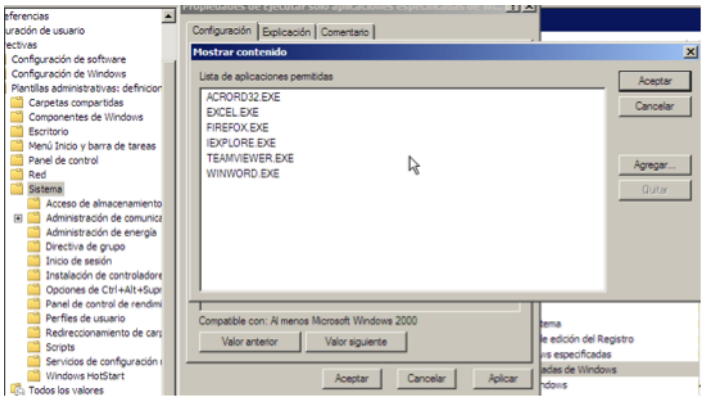


Figura 70: Ingreso aplicaciones permitidas.
Fuente: Elaborado por investigador.

   b) A continuación, en la Figura 71 y 72, se muestra el resultado de la configuración realizada.

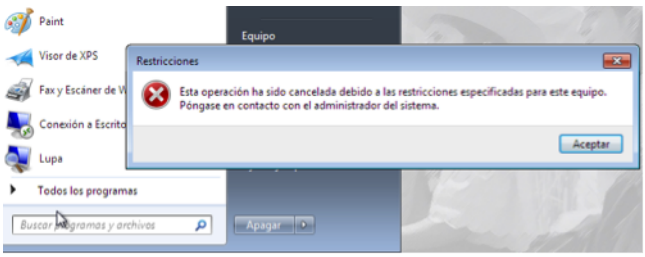


Figura 71: Resultado de aplicaciones restringidas.
Fuente: Elaborado por investigador.

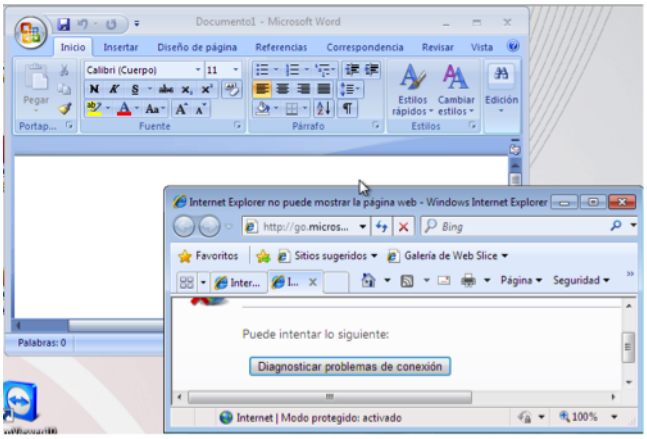


Figura 72: Resultado de las aplicaciones permitidas.
Fuente: Elaborado por investigador.

9. El usuario no debe actualizar el sistema operativo.

   a) Esta configuración se encuentra en **Directivas > Plantillas administrativas > Sistema > Actualizaciones automáticas de Windows**, en el cual solo se debe habilitar, esta acción se muestra en la Figura 73.

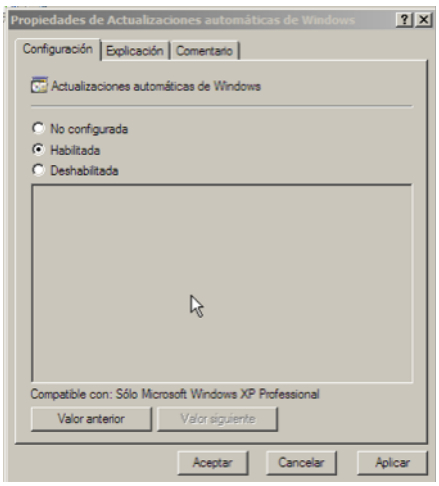


Figura 73: Habilitación de la propiedad actualizaciones automáticas de Windows.
Fuente: Elaborado por investigador.

10. El usuario no debe realizar cambios en la barra de tareas.

    a) Esta configuración se encuentra en **Directivas > Plantillas administrativas > Menú Inicio y barra de tareas > Bloquear barra de tareas**, en el cual solo se debe habilitar, esta acción se muestra en la Figura 74.

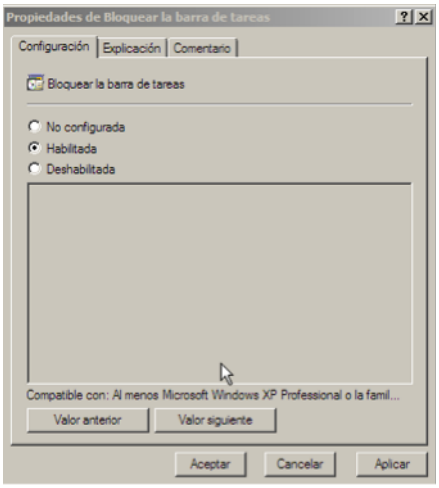


Figura 74: Habilitación de la propiedad de bloqueo de la barra de tareas.
Fuente: Elaborado por investigador.

    b) A continuación, en la Figura 75, se muestra el resultado de la configuración realizada, como se puede observar la barra de tareas está bloqueada y no se pueden hacer cambio alguno.

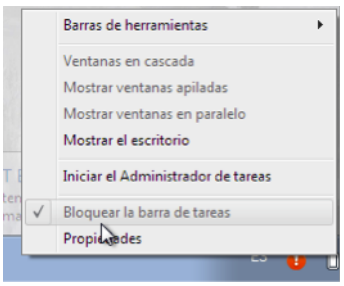


Figura 75: Resultado del bloqueo de la barra de tarea.
Fuente: Elaborado por investigador.

11. El usuario no debe cambiar el tamaño de la barra de tareas.

    a) Esta configuración se encuentra en **Directivas > Plantillas administrativas > Menú Inicio y barra de tareas > Impedir que los usuarios cambien el tamaño de la barra de tareas**, en el cual solo se debe habilitar, esta acción se muestra en la Figura 76.

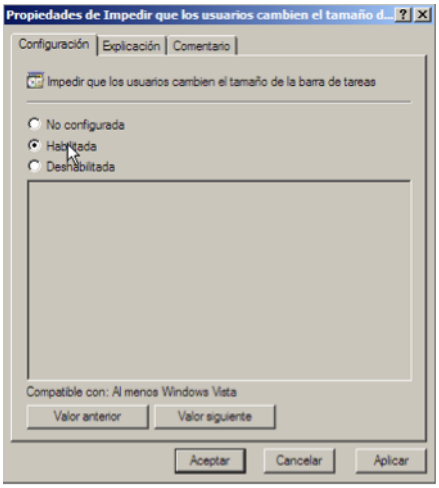


Figura 76: Habilitación de la propiedad de impedir el cambio de tamaño de la barra de tarea.
Fuente: Elaborado por investigador.

12. El usuario no tiene el privilegio de mover la barra de tareas a otro sitio.

    a) Esta configuración se encuentra en **Directivas > Plantillas administrativas > Menú Inicio y barra de tareas > Impedir que los usuarios muevan la barra de tareas a otra ubicación**, en el cual solo se debe habilitar, esta acción se muestra en la Figura 77.

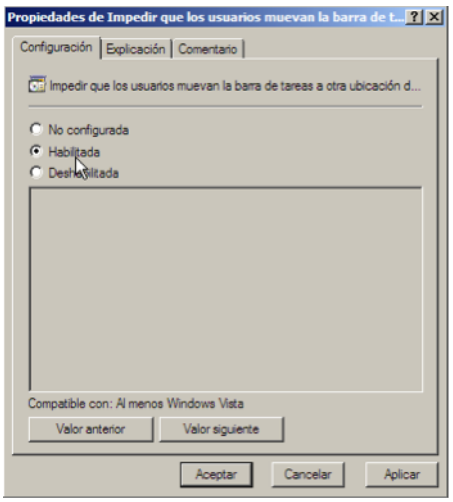


Figura 77: Habilitación de la propiedad de impedir que el usuario mueva la barra de tarea.
Fuente: Elaborado por investigador.

13. El usuario no tiene la autorización para cambiar la hora del equipo.

    a) Esta configuración ya viene por defecto al momento de unir al dominio el equipo, además esta acción ya no tiene función ya que en la política anterior se restringió las aplicaciones a ejecutar. A continuación, en la Figura 78, se muestra la prueba del cambio de fecha y hora.

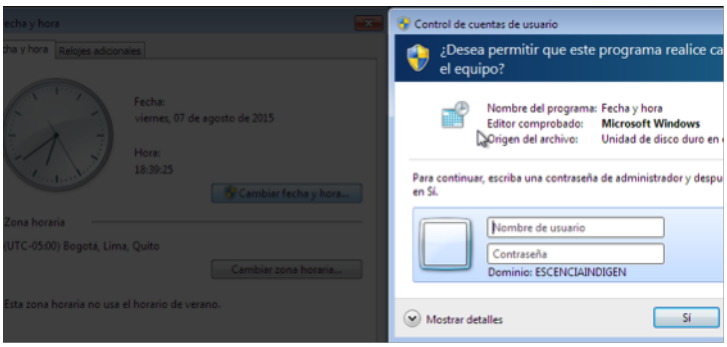


Figura 78: Prueba de cambio de fecha y hora del equipo.
Fuente: Elaborado por investigador.

14. El usuario no debe tener acceso a páginas no autorizadas por el administrador.

    a) Para aplicar esta política se procede a activar o instalar el servicio de **proxy HTTP** en Zentyal 4.0 desde la opción **módulos**, así como se muestra en la Figura 79.

Figura 79: Activación de modulo Proxy HTTP.
Fuente: Elaborado por investigador.

b) Para que se aplique las políticas de restricciones de páginas web se debe configurar el servidor proxy en los clientes Windows, para esto, se debe ir a **Herramientas en el navegador explorer > Opciones de internet > Configuración de LAN** y, a continuación, seleccionar **servidor proxy** e ingresar seguidamente la dirección IP y el puerto 3128 del servidor Zentyal, ya que el proxy no debe ser transparente por seguridad, con esto los equipos que este configurado con el proxy pueden navegar caso contrario no navega, así como se muestra en la Figura 80.

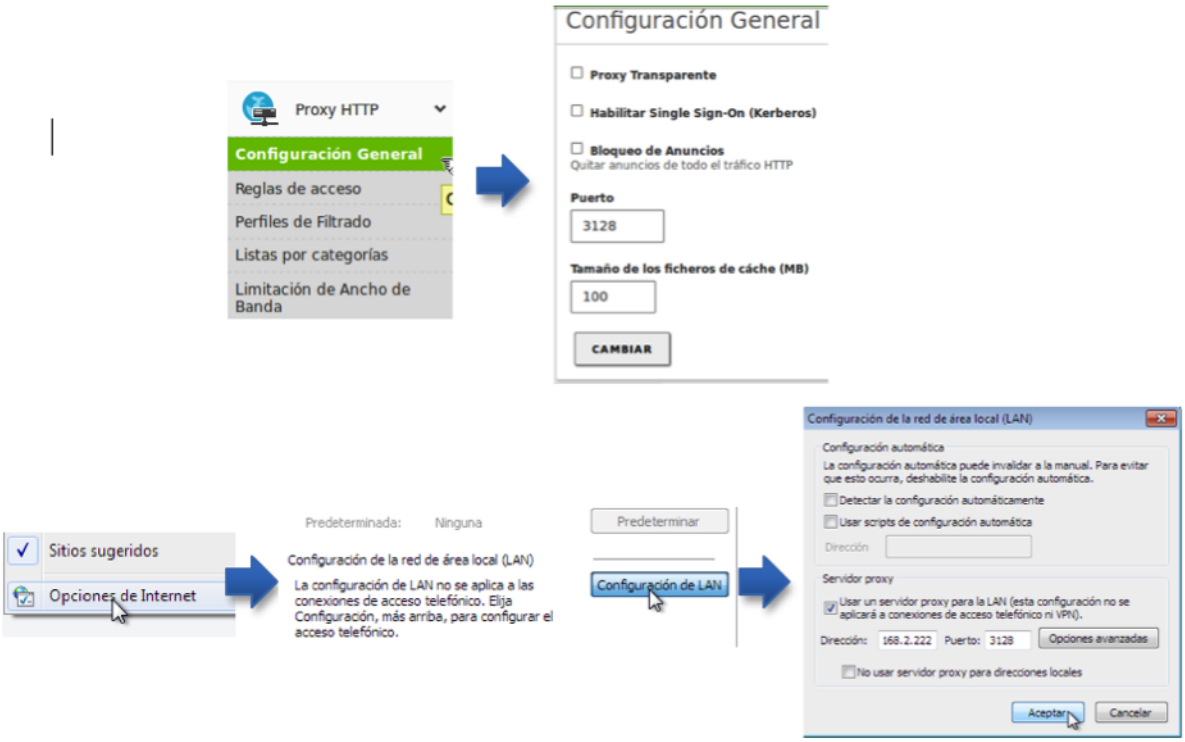


Figura 80: Configuración proxy en clientes Windows.
Fuente: Elaborado por investigador.

c) Las políticas de las páginas permitidas se las debe ingresar desde Perfiles de Filtrado que se encuentra en el módulo instalado, para

esto, se debe hacer clic en añadir **Perfiles de Filtrado > digitar el nombre del perfil >** proceder a cliquear en el icono de **configuración>**dirigirse a la pestaña **Reglas de dominios y URLs**, seleccionar **Bloquear dominios y URLs no listados > guardar cambios > agregar reglas de dominios y URLs >** ingresar los dominios que son permitidos el acceso según los grupos mencionados en el apartado **4.7.1 > guardar cambios**, este proceso se muestra a continuación en la Figura 81.

Figura 81: Proceso de creación de perfiles de filtrado.
Fuente: Elaborado por investigador.

Nota: Este proceso se debe realizar para cada uno de las áreas como: cajas, créditos, inversiones, secretaria y administración, ya que cada una tiene diferentes restricciones.

d) En la opción **Reglas de acceso > añadir nueva regla de acceso >** el ingreso del periodo de tiempo es opcional **> seleccionar el objeto de red > seleccionar el perfil de filtrado junto a la política de restricción >** grabar los cambios realizados, en la Figura 82, se muestra el proceso de la creación de las reglas de acceso.

Figura 82: Proceso de creación de reglas de acceso.
Fuente: Elaborado por investigador.

e) En caso de no haber el objeto de red, se debe proceder a crear de la siguiente manera, clic en **Añadir nuevo > digitar el nombre del nuevo objeto > clic en añadir nuevos miembros >** digitar el nombre del miembro e ingresar el rango de IPs que pertenece al área de inversiones, esto según las tablas del **Anexo A.1** y **A.2**. A continuación, en la Figura 83, se muestra el proceso de creación de objetos de red.

Figura 83: Proceso de creación de objetos de red.
Fuente: Elaborado por investigador.

f) En la siguiente Figura 84, se muestra los resultados de las políticas aplicadas.

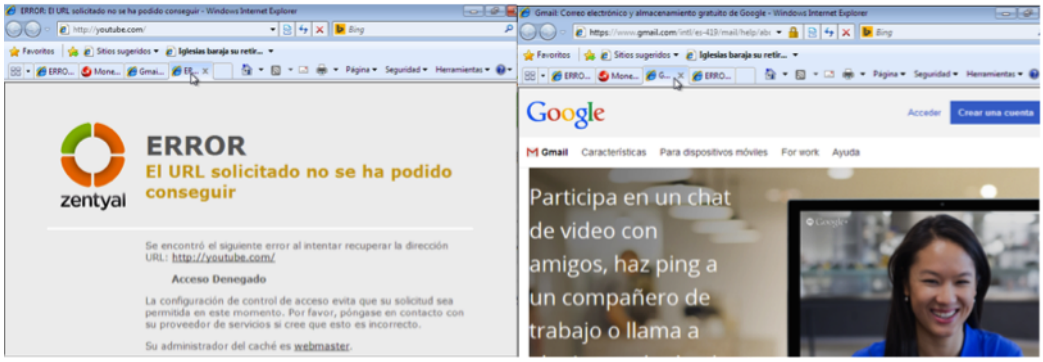


Figura 84: Prueba de políticas configuradas.
Fuente: Elaborado por investigador.

g) De igual manera se procede al bloqueo de las páginas seguras como el Facebook, para esto, se debe dirigir al menú **Cortafuegos > Filtrado de Paquetes > Reglas de filtrado para las redes internas > Añadir nueva regla > Seleccionar la decisión, Destino y servicios,** así como se muestra en la Figura 85.

Figura 85: Creación de reglas de filtrado para las redes internas.
Fuente: Elaborado por investigador.

h) Si no se ha creado el servicio y el objeto destino se lo debe crear de la siguiente manera: opción **Añadir nuevo >** ingresamos el nombre del servicio **> seleccionar protocolo TCP/UDP >** se debe ingresar el puerto destino como único el **443**, esta acción se muestra en la Figura 86.

Figura 86: Creación de servicios.
Fuente: Elaborado por investigador.

i) Para crear el objeto destino es casi similar, seleccionar en **Objeto de Destino** > **Añadir nuevo** > ingresar el nombre del objeto "Facebook" > ingresar un nombre y la dirección CIDR con su respectiva mascara de la página de Facebook, las direcciones se los puede obtener realizando un **Ping** desde el comando de sistemas (CMD) a facebook.com, www.facebook.com, login.facebook.com, etc., este proceso se muestra en la Figura 87.

Figura 87: Creación de objetos de destino.
Fuente: Elaborado por investigador.

j) En la Figura 88, se muestra el resultado de la configuración realizada.

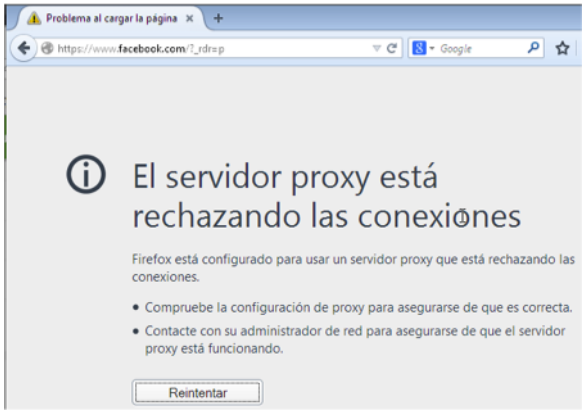


Figura 88: Prueba de restricción a Facebook.
Fuente: Elaborado por investigador.

4.10. Pruebas de funcionalidad del servidor

4.10.1. Configuración e instalación de MikroTik

1. En el primer lugar se procede a descargar MikroTik, esto se lo puede hacer de la página oficial del sistema que se describe a continuación. http://www.mikrotik.com/download

2. Los requerimientos mínimos de MikroTik son: 128 MB, 10 G de Disco Duro y las interfaces de red necesarias para las pruebas, ya que MikroTik se va ha utilizar como router para establecer las conexiones entre las dos agencias virtualizadas. En la Figura 89, se muestra la creación de la máquina virtual con los requerimientos mínimos de MikroTik.

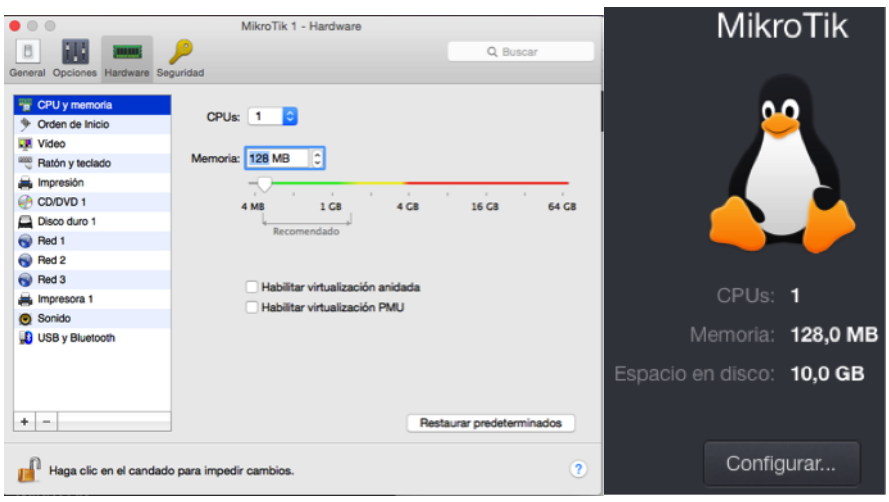


Figura 89: Creación de máquinas virtuales para el sistema MikroTik.
Fuente: Elaborado por investigador.

3. Una vez creada las dos máquinas virtuales para el sistema MikroTik se procede a iniciar la instalación iniciando del disco de arranque virtual.

4. En este paso se debe seleccionar los paquetes necesarios para posteriormente instalarlos, los paquetes se seleccionan con una x. Los paquetes seleccionados para la configuración son los siguientes:

   - system: es el paquete principal que posee los servicios básicos.
   - DHCP: servidor y cliente DHCP.
   - hotspot: es la que ofrece internet por medios de enrutador.
   - ppp: conexión directa entre dos nodos de red.
   - ntp: sincroniza los relojes a través de enrutamiento.
   - routing: este paquete es la que cumple la función de router.
   - Security: conectividad segura con el software WinBox.
     - A continuación, el la Figura 90, se muestra los paquetes seleccionados para ser instalados posteriormente.

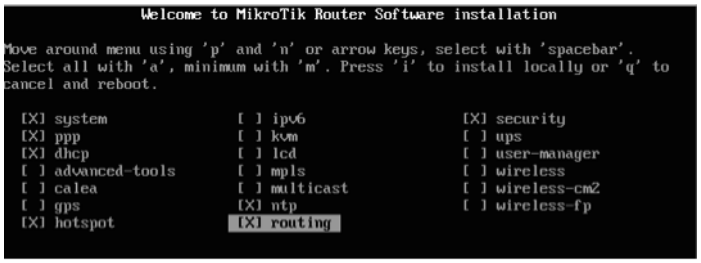


Figura 90: Selección de paquetes a ser instalados en cada sistema MikroTik.
Fuente: Elaborado por investigador.

5. Una vez que se haya seleccionado los paquetes necesarios, se procede a la instalación de las mismas, para esto, se presiona la tecla "i", en este proceso aparece una pregunta si desea quedar con la configuración anterior, al cual se debe contestar que no presionando la tecla **N**; seguidamente, se debe responder **si** presionando la tecla **Y** a la siguiente pregunta, si quiere perder todos los datos que se encuentran en el disco duro, Así como se muestra en la Figura 91.

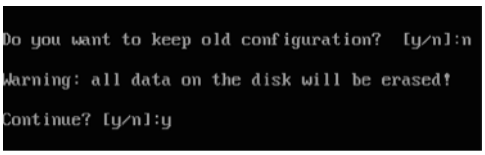


Figura 91: Preguntas de configuración.
Fuente: Elaborado por investigador.

6. En la siguiente Figura 92, se muestra el proceso de instalación de los paquetes seleccionados y finalmente se presiona la tecla "Enter" para reiniciar en sistema.

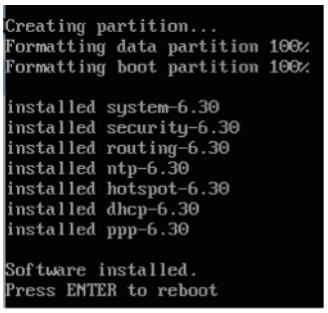


Figura 92: Proceso de instalación de los paquetes seleccionados.
Fuente: Elaborado por investigador.

7. Una vez que se haya reiniciado el sistema pide que se ingrese el usuarios y contraseña, generalmente por defecto el usuarios es: admin y la contraseña se deja en blanco, así como se muestra e la Figura 93.

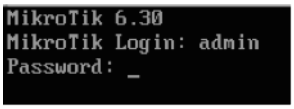


Figura 93: Inicio de sesión del sistema MikroTik.
Fuente: Elaborado por investigador.

8. Finalmente se muestra la ventana de bienvenida, en el cual pide presionar la tecla "Enter" para iniciar.

4.10.2. Acceso a MikroTik

Existen varias maneras de acceder a MikroTik sin haber configurado nada en un principio.

1. Es directamente desde la consola finalizada la instalación.

2. Es utilizando una consola Telnet a través del puerto serie o Ethernet por MAC o IP.

3. Mediante un software Winbox, el cual se lo puede descargar desde la página oficial de MikroTik.

Para este proyecto se considera más óptimo acceder al sistema MikroTik mediante el **Software Winbox**, para lo cual se debe descargar desde la página oficial de MikroTik. Una vez descargada se procede a instalar con unos sencillos pasos que se debe seguir al momento de la instalación. Una vez que se haya finalizado la instalación, se procede a iniciar el software e ingresar la dirección MAC del sistema MikroTik, además solicita el ingreso del usuario y contraseña el mismo que ya se menciona anteriormente al momento de instalar el sistema MikroTik. Finalmente se muestra una ventana con los paquetes ya instalados y con una interfaz muy amigable para que sea más fácil la configuración de la misma.
En la Figura 94, se muestra los campos necesarios para ingresar al sistema MikroTik.

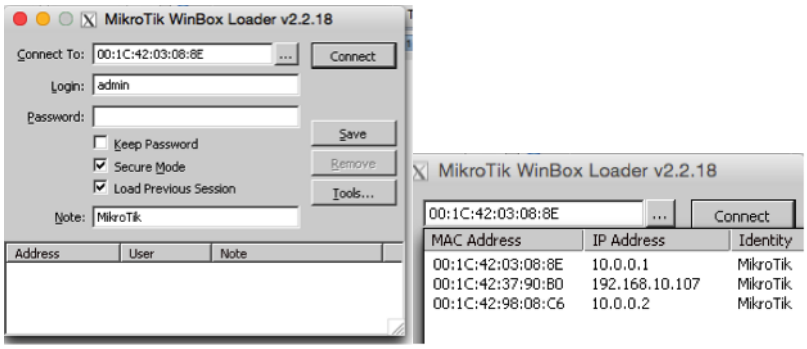


Figura 94: Ventana de inicio de sesión del Winbox hacia MikroTik.
Fuente: Elaborado por investigador.

En la Figura 95, se muestra la ventana principal del software Winbox una vez conectada al sistema MikroTik.

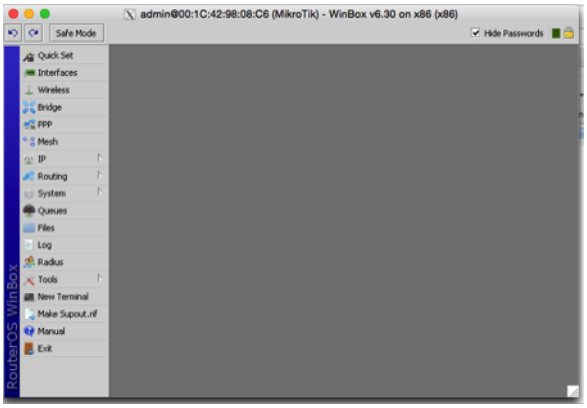


Figura 95: Ventana principal de Winbox.
Fuente: Elaborado por investigador.

4.10.3. Declaración y asignación de interfaces

En este caso las interfaces deben estar en diferentes redes, para este proyecto la red se distribuye de la siguiente manera:
En la Tabla 2, se detalla la asignación y distribución de las interfaces de red de MikroTik 1 Matriz Ambato.

Interfaz	Red virtual	Nombre	IP	Detalle
Red1	Wifi	ENTREMIKROTIK	10.0.0.1/30	Comunicación entre routers
Red2	awdl0	LAN 1	192.168.2.0/24	Red local
Red3	Wifi	WAN	DHCP	Proveedor de internet

Tabla 2: Asignación y distribución de las interfaces de red de MikroTik 1 Matriz Ambato.

Fuente: Elaborado por investigador.

En la Tabla 3, se detalla la asignación y distribución de las interfaces de red de MikroTik 2 Agencia Ibarra.

Interfaz	Red virtual	Nombre	IP	Detalle
Red1	Wifi	ENTREMIKROTIK	10.0.0.2/30	Comunicación entre routers
Red2	Ethernet	LAN2	192.168.0.0/24	Red local
Red3	Wifi	WAN	DHCP	Proveedor de internet

Tabla 3: Distribución de asignación y distribución de las interfaces de red de MikroTik 2 Agencia Ibarra.

Fuente: Elaborado por investigador.

Para realizar el proceso de asignación de nombres a las interfaces, se debe conectar desde el software Winbox hacia el sistema MikroTik para la debida

configuración. Una vez conectada con el software Winbox se debe hacer clic en la opción interfaces, en dicha opción muestra las tres interfaces sin nombres, para proceder al cambio de los nombres se debe hacer doble clic en la interfaz que quiera cambiar para posteriormente digitar el nombre que desee según la tabla distribución anterior. A continuación, en la Figura 96, se muestra el proceso de cambio de nombre a las interfaces de red existentes.

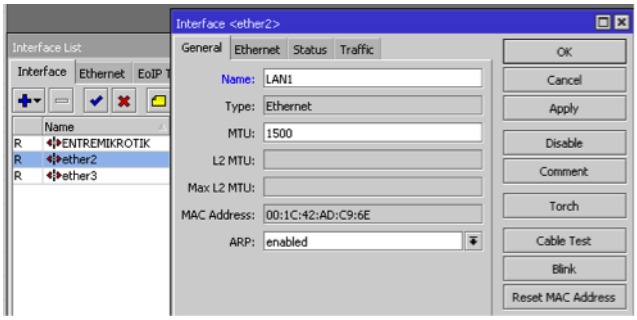


Figura 96: Cambio de nombre a las interfaces de red existentes.
Fuente: Elaborado por investigador.

El siguiente paso permite asignar una dirección IP para las interfaces de red, esto se realiza con los siguientes pasos:

1. En el router MikroTik1, la interfaz WAN debe tener una dirección IP dinámica por DHCP que generalmente el proveedor de internet lo asigna. Para esto, se debe ir al **Menú > IP > DHCP Client**; seguidamente, hacer clic en agregar un nuevo **DHCP Client**, el siguiente paso es elegir la interfaz de internet que es WAN, finalmente se debe hacer clic en ok para aceptar las configuraciones. En la siguiente Figura 97, se muestra el proceso de asignación IP por DHCP, esto para simular la IP que el proveedor lo asigna para la salida a internet.

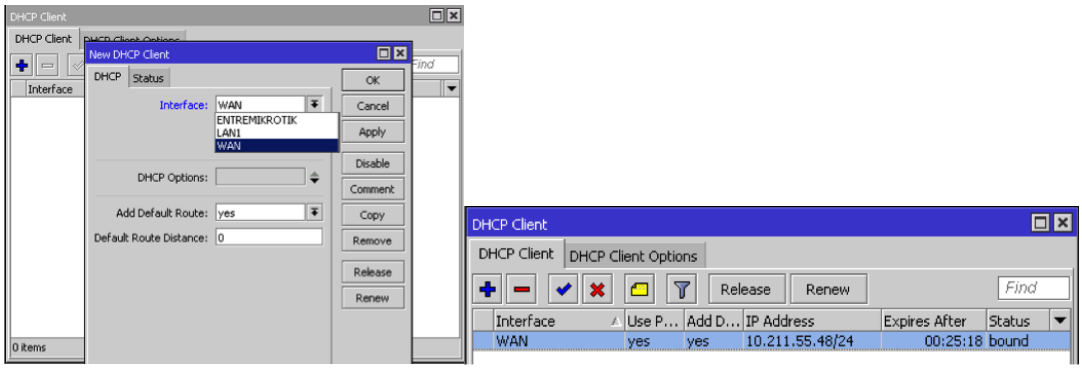


Figura 97: Proceso de asignación IP por DHCP
Fuente: Elaborado por investigador.

Nota: este proceso se lo debe realizar para cada MikroTik.

2. Ahora para configurar las dos interfaces restantes se debe dirigir al **Menú > IP > Addresses**. Se abre una ventana con la interfaz que ya se asignó la dirección IP anteriormente mediante DHCP, para asignar la dirección IP en su interfaz respectivo se procede a hacer clic Agregar lista, en el cual aparece otra ventana donde se deben ingresar las direcciones IPs según la Tabla 2 y 3 independientemente, el mismo proceso se lo realiza en el router MikroTik2 según la tabla mencionada. En la Figura 98, se muestra la asignación de dirección IP a las interfaces LAN y ENTREMIKROTIK.

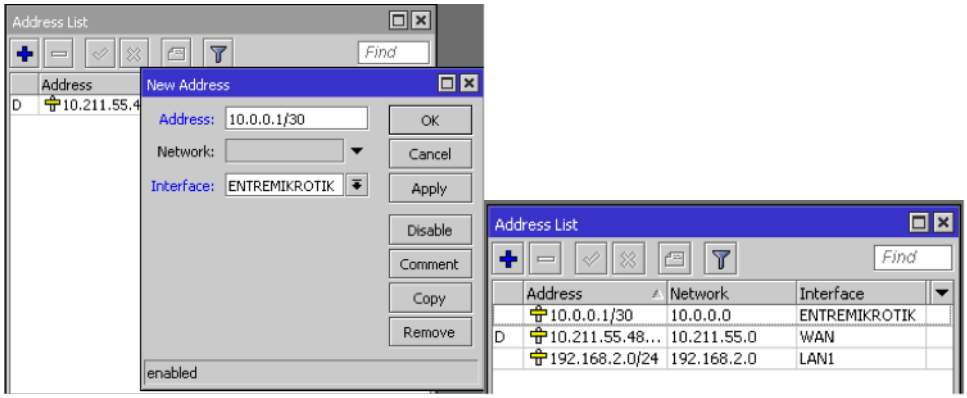


Figura 98: Asignación de dirección IP a las interfaces LAN y ENTREMIKROTIK.
Fuente: Elaborado por investigador.

3. El siguiente paso es verificar la conectividad entre los dos routers, para esto, se debe dirigir al **Menú > New Terminal**, como se muestra en la Figura 99.

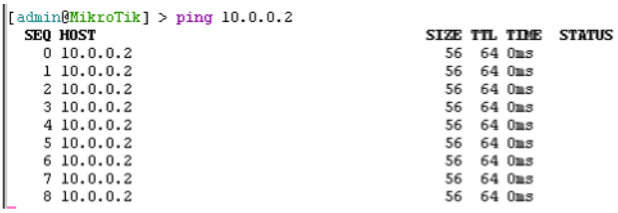


Figura 99: Verificación de conectividad entre los routers.
Fuente: Elaborado por investigador.

4. Ahora se debe configurar el DHCP Server para la interfaz, para esto, se debe ir al **Menú > IP > DHCP Server**, posteriormente hacer clic en el botón **DHCP Setup** para proceder a agregar el servidor DHCP Server con un asistente de configuración.

5. A continuación se muestra una ventana donde se debe seleccionar la interfaz LAN1; seguidamente, hacer clic en **siguiente** y posteriormente solicita el ingreso de la dirección IP de la red LAN1, la misma que se obtiene automáticamente, como se muestra en la Figura 100.

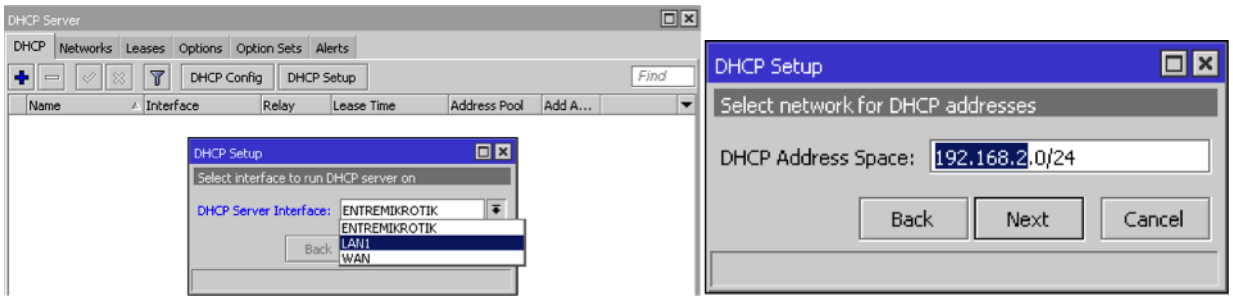


Figura 100: Selección e ingreso de dirección IP de la red LAN1.
Fuente: Elaborado por investigador.

6. Seguidamente solicita el ingreso de la puerta de enlace o Gateway, esto se ingresa de forma automática y también manualmente, en este proceso se debe ingresar manualmente la puerta de enlace de la red LAN1 que es 192.168.2.254 y para la red LAN2 que pertenece a otro router se debe asignar la puerta de enlace 192.168.0.253. A continuación, en la Figura 101, se muestra el ingreso de la puerta de enlace de la red LAN1.

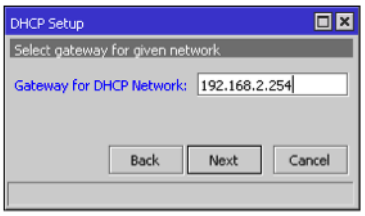


Figura 101: Ingreso de puerta de enlace de la red LAN1.
Fuente: Elaborado por investigador.

7. En este punto se debe hacer clic en **Next** y posteriormente debe solicitar el ingreso del rango de direcciones para el DHCP, esto se ingresa automáticamente y manualmente, como se muestra en la Figura 102.

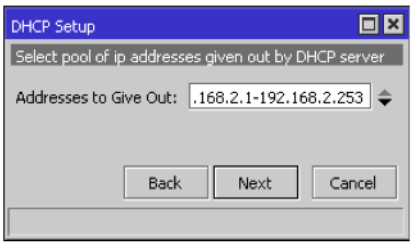


Figura 102: Ingreso del rango de direcciones para el DHCP.
Fuente: Elaborado por investigador.

8. Posteriormente solicita el ingreso del servidor DNS que para el presente proyecto se utiliza el de google 8.8.8.8. A continuación, en la Figura 103, se muestra el ingreso de la dirección DNS.

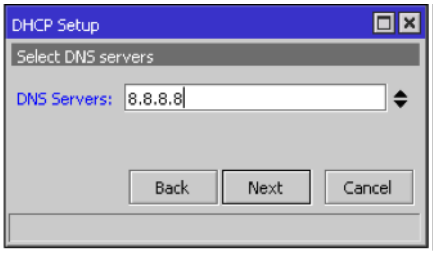


Figura 103: Ingreso de DNS de google.
Fuente: Elaborado por investigador.

9. A continuación hacer clic en **Next**, así mismo lo siguiente que solicita es el tiempo de vida del uso de las IP, en este caso 10 min, así como se muestra en la Figura 104.

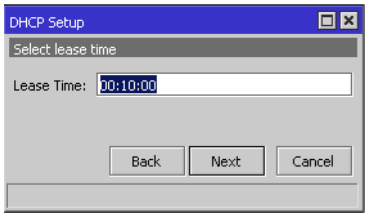


Figura 104: Ingreso de tiempo de vida de las direcciones IP.
Fuente: Elaborado por investigador.

10. Finalmente al hacer clic **Next** y debe mostrar un aviso de configuración exitosa y se debe haber creado el servidor DHCP para los usuarios de la red LAN1 y LAN2 configurando respectivamente, ya que son los mismo pasos a seguir.

4.10.4. Comprobación de funcionalidad del DHCP

Para esto, se debe poner los equipos Windows en la misma red del servidor en este caso la red **awdl0** y automáticamente se debe asignar una dirección IP en el rango que se lo asigno el servidor DHCP, así como se muestra en la Figura 105. Los mismo pasos se los puede realizar para el otro router.

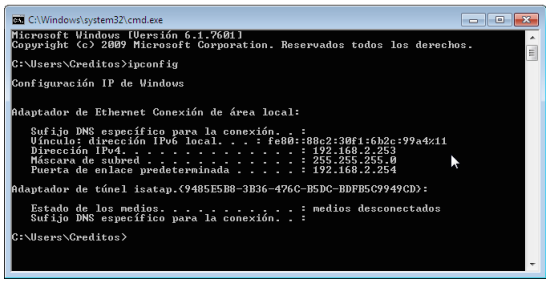


Figura 105: Comprobación del servicio DHCP.
Fuente: Elaborado por investigador.

4.10.5. Enrutamiento estático entre routers

Para el enrutamiento entre los routers MikroTik1 y MikroTik2 se debe realizar los siguientes pasos:

1. Dirigirse a **Menú>IP>Routers** y posteriormente agregar la red LAN2 que es 192.168.0.0/24 y como puerta de enlace 10.0.0.2, así como se muestra en la Figura 106.

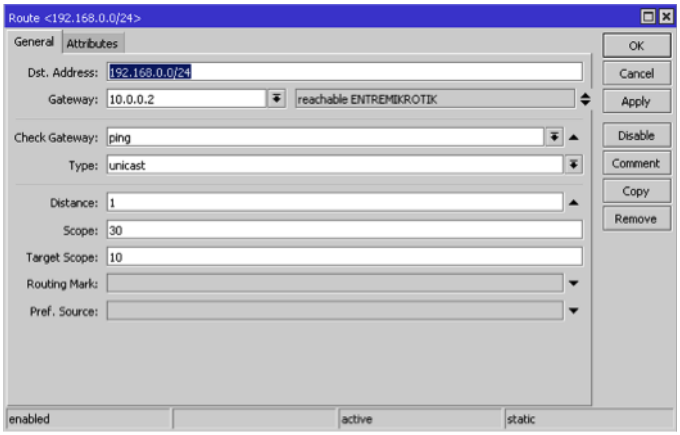


Figura 106: Ingreso de la ruta de LAN1 hacia la red LAN2.
Fuente: Elaborado por investigador.

2. Se da clic en ok y se agrega a la lista de rutas como se muestra en la Figura 107.

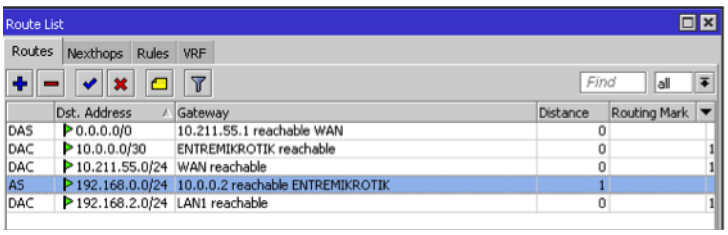


Figura 107: Prueba de funcionamiento correcto de la ruta ingresada.
Fuente: Elaborado por investigador.

3. En el segundo router se agrega de la misma manera con la dirección IP 192.168.2.0/24 y puerta de enlace 10.0.0.1, o a su vez con la IP 0.0.0.0/0 y puerta de enlace 10.0.0.1, como se muestra en la Figura 108.

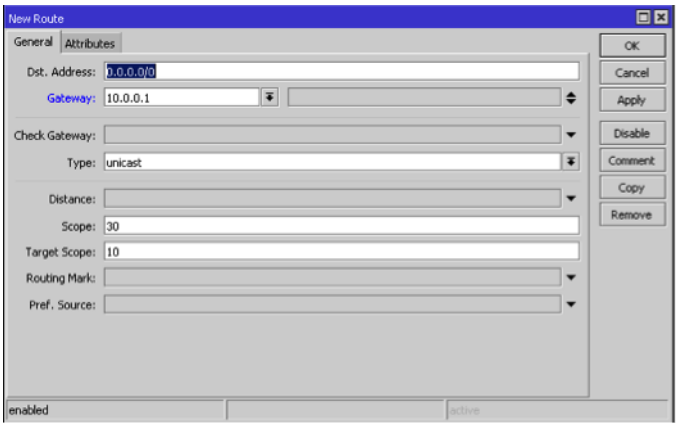


Figura 108: Ingreso de ruta de LAN2 hacia la red LAN1.
Fuente: Elaborado por investigador.

4. Ahora se procede a hacer la comprobación respectiva de conectividad con el comando Ping desde los usuarios Windows desde el sistema de comandos CMD.

   a) En la Figura 109, se muestra la ejecución del comando Ping desde la red LAN1 hacia la red LAN2.

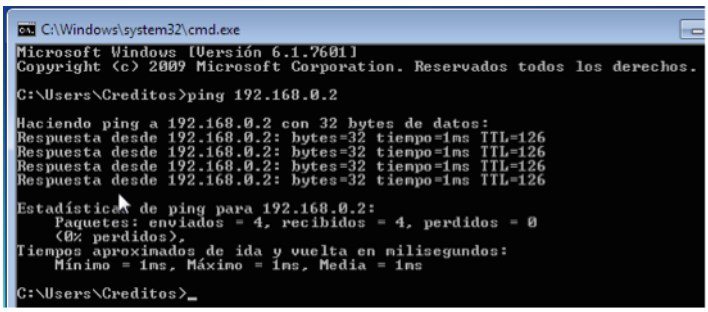


Figura 109: Comando Ping de LAN1 a LAN2.
Fuente: Elaborado por investigador.

b) En la Figura 110, se muestra la ejecución del comando Ping desde la red LAN2 hacia la red LAN1.

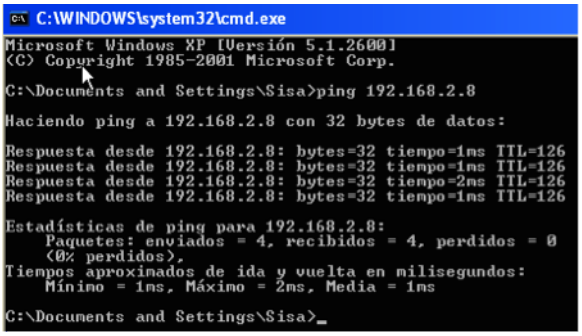


Figura 110: Comando Ping de LAN1 a LAN2.
Fuente: Elaborado por investigador.

4.10.6. Compartir internet por medio de Routers

Este proceso se lo realiza para que los servidores puedan filtrar las páginas web con el servidor Proxy HTTP, para esto, se debe ir al menú **IP** > **Firewall** > Clic en pestaña **NAT** > Seleccionar **srcnat y WAN** > Clic en pestaña **Action** > Seleccionar **masquerade**, este proceso se muestra en la Figura 111.

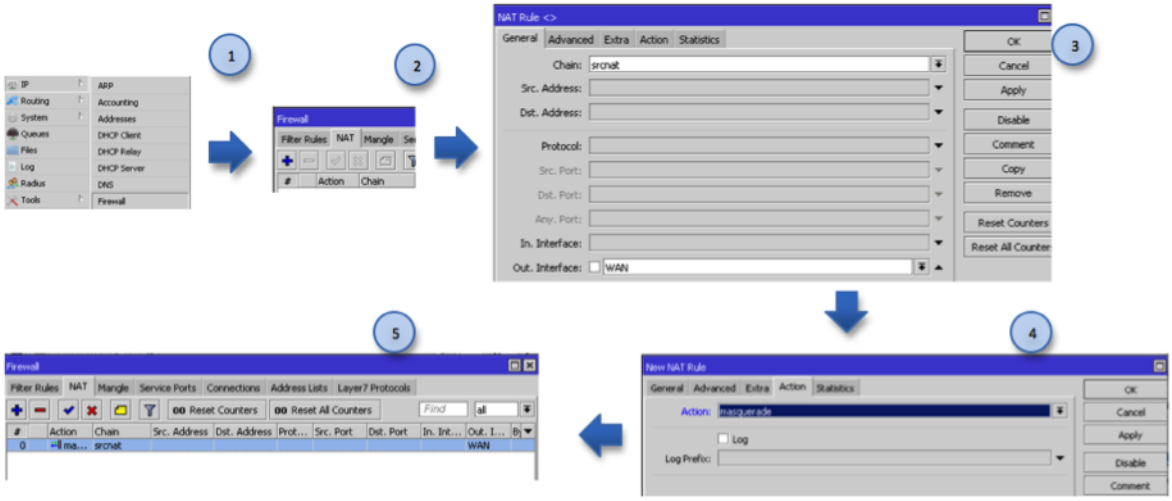


Figura 111: Compartir internet por medio de MikroTik.
Fuente: Elaborado por investigador.

4.10.7. Prueba de sincronización de servidores

Una vez realizadas las configuraciones anteriores, se procede a verificar las sincronizaciones entre los servidores tanto servidor de dominio adicional como también del servidor Windows Server 2008 que tiene la función de controlador de dominio, en la Figura 112, muestra la sincronización de los servidores instalados.

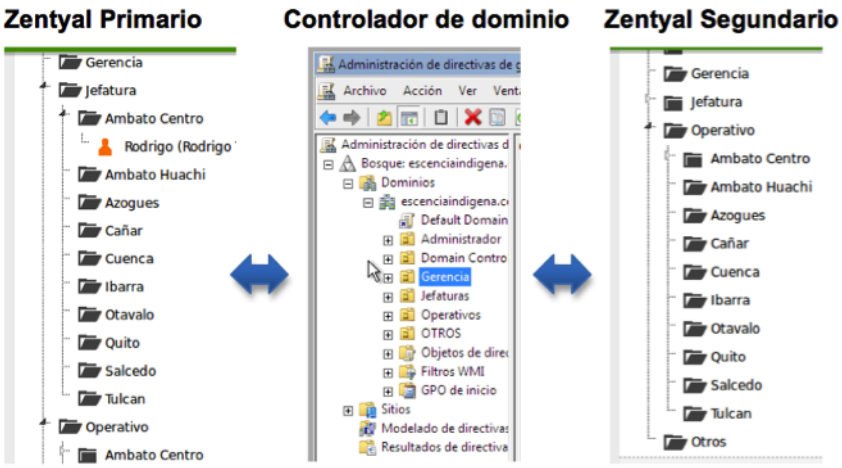


Figura 112: Sincronización de los servidores instalados.
Fuente: Elaborado por investigador.

4.10.7.1. Análisis comparativo económico

Con la implementación de este proyecto de investigación se ahorrará un valor significante en lo que se refiere a licenciamiento ya que el sistema que se instala

es Zentya 4.0 Edición Comunidad, además, se acopla a los requerimientos de la institución y no tiene ningún costo porque varias comunidades Zentyal aportan para el mejoramiento del sistema en lo que a seguridad y funcionamiento se refiere, esto en comparación con Active Directory de Windows que es un software comercial, que se debe pagar o contratar la licencia por el número de usuarios que la empresa posee, en la siguiente tabla se muestra un ejemplo claro de lo que se mencionó anteriormente.

Características	**Precio Windows Server**	**Pago**	**Precio Zentyal Edición Comunidad**	**Pago**
Licencia Servidor	$230**	anual	$0**	-
Servicio de correo	$71**	usuario/mes	$0**	-
Antivirus	$59**	anual	$0**	-
Usuarios ACLs	$2004**	100 usuarios	$0**	-
Total	2364**		$0**	

Tabla 4: Costos de licenciamiento.

Fuente: Elaborado por investigador.

Nota: Los costos que se deben tomar en cuenta adicionalmente para la implementación de esta solución son la configuración, soporte y equipos hardware.

4.10.7.2. Ventajas de la propuesta

- Reducción de los costos de licenciamientos en comparación a sistemas Windows.
- Control en la autenticación de usuarios internos y externos a la Cooperativa.
- Repotenciación de la seguridad de los recursos internos de la Cooperativa.
- Repotenciación de las políticas de seguridad.
- Reestructuración de las unidades organizativas.
- Mejoramiento en la administración de usuarios.
- Creación sencilla de políticas de seguridad con la ayuda de un controlador de dominio Windows.
- Integración de Windows Server como controlador de dominio.
- Restricción de páginas seguras.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- Luego del análisis de las distribuciones GNU/Linux Small Business Server, se pudo observar que la distribución Zentyal versión 4.0 es la que más cubre los requerimientos de la Cooperativa.
- Se podría decir que la presente solución reduciría el costo de licenciamiento de software, consecuentemente existe un costo adicional del hardware que se utilice, la configuración y soporte de la misma.
- La propuesta planteada facilita a los administradores de red gestionar adecuadamente las políticas de seguridad conjuntamente con los usuarios, ya que los servidores de las agencias se sincronizan con el servidor principal de manera inmediata, permitiendo así realizar los cambios en diferentes servidores.

5.2. Recomendaciones

- Para una mejor estructuración de las políticas de seguridad, se recomienda que se las realice conjuntamente con el Departamento de Sistemas y Talento Humano o el Departamento encargado de crear políticas internas para los empleados de la Cooperativa, ya que se debe analizar minuciosamente las diferentes políticas que se debe aplicar a los diferentes departamentos o unidades organizativas.
- Se recomienda que las políticas de seguridad sean revisadas de manera que no haya ninguna redundancia entre las mismas, esto para una mejor administración de las políticas.
- Para un buen rendimiento del sistema, se recomienda actualizar solo los módulos necesarios del servidor Zentyal más no el sistema completo, ya que esto podría acarrear complicaciones.

- Se recomienda formalizar el documento de políticas de seguridad y la difusión de las mismas a todos los funcionarios de la Cooperativa, de modo que se cree conciencia sobre la importancia de la información que se maneja.
- Se recomienda que exista un procedimiento formal de altas y bajas de usuarios con el objetivo de garantizar la cancelación de los accesos a todos los sistemas de información.

Bibliografia

[1] A. G. Ariel, V. L. Luis, G. Cindy, and G. Gustavo, "Sistema de gestión en seguridad informática como soporte a la toma de decisiones en respuesta a incidentes, basados en monitoreo de redes," 2011. [Online]. Available: https://www.dspace.espol.edu.ec/handle/123456789/14922

[2] G. C. C. David, "Implementación de una red segura para los laboratorios del deee utilizando un dispositivo utm." 2011. [Online]. Available: http://repositorio.espe.edu.ec/handle/21000/4741

[3] E. M. J. Pablo, "Implementación de un firewall sobre plataforma linux en la empresa de contabilidad armas & asociados," 2013. [Online]. Available: http://bibdigital.epn.edu.ec/bitstream/15000/6056/1/CD-4785.pdf

[4] P. B. L. Carlos, "Servidor aaa para validación y control de acceso de usuarios hacia la infraestructura de networking de un ente del ministerio de defensa nacional," 2012. [Online]. Available: http://repositorio.utn.edu.ec/handle/123456789/994

[5] S. J. Gavilanes Vásquez, "Seguridad de acceso al servicio de internet y los ataques cibernéticos en el hotel casino emperador de la ciudad de ambato," 2011. [Online]. Available: http://repo.uta.edu.ec/handle/123456789/49

[6] A. C. Salinas Pérez and F. DT-Terán, "Sistema de autenticación unificada para la correcta transmisión de información en el centro de educación"sagrada familia"de la ciudad de ambato," 2012. [Online]. Available: http://repo.uta.edu.ec/handle/123456789/2477

[7] I. Glossary, "National information systems security (infosec) glossary," 2000. [Online]. Available: http://www.dtic.mil/get-tr-doc/pdf?AD=ADA433929

[8] D. Spano, "El open source como facilitador del open access," in *II Encuentro Iberoamericano de editores científicos*, 2010. [Online]. Available: http://eprints.rclis.org/16462/1/ponencia_spano_elis.pdf

[9] F. Andreu, I. Pellejero, and A. Lesta, *Fundamentos y aplicaciones de seguridad en redes WLAN*. Marcombo, 2006.

[10] J. Nño, *Servicios de directorio (Sistemas operativos en red):*, ser. Ciclos Formativos. Editorial Editex, 2011.

[11] J. García Chico, "Estudio de viabilidad de directorio activo en linux," 2011.

[12] T. Drilling, *Linux Small Business Server Distros.* [Online]. Available: http://www.linux-magazine.com/Online/Features/Linux-Small-Business-Server-Distros

[13] K. J. M. Molina, J. P. Meneses, and I. Z. Silgado, "Firewall-linux: Una solución de seguridad informática para pymes (pequeñas y medianas empresas)," *REVISTA UIS INGENIERÍAS*, vol. 8, no. 2, 2010. [Online]. Available: http://revistas.uis.edu.co/index.php/revistauisingenierias/article/view/506/830

[14] W. Flórez, C. A. Arboleda, and J. F. Cadavid, "Solución integral de seguridad para las pymes mediante un utm," *Revista Ingenierías USBMed*, vol. 3, no. 1, pp. 35–42, 2012. [Online]. Available: http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a4.pdf

[15] P. Aguilera, *Redes seguras (Seguridad informática):*, ser. Ciclos Formativos. Editorial Editex, 2011.

[16] D. G. Mier González and S. D. Velásquez Duran, "Análisis y diseño de un modelo de implementación de una red mesh con calidad de servicio, ruteo y seguridades, mediante el uso de equipos mikrotik, tomando como referencia la red inalámbrica de la universidad politécnica salesiana, sede quito, campus sur," 2013. [Online]. Available: dspace.ups.edu.ec/bitstream/123456789/4923/1/UPS-ST000993.pdf

[17] Zentyal.org. Las pymes y las tics. Zentyal. [Online]. Available: https://wiki.zentyal.org/wiki/Es/3.5/Presentacion

[18] A. F. Vanegas Calle, "Zentyal como herramienta de seguridad y gestión frente a clearos, en entornos de red linux," 2013. [Online]. Available: http://dspace.uazuay.edu.ec/handle/datos/3133

[19] O. L. Peral and Y. O. Leyva, "Zentyal como servidor libre para empresas cubanas." [Online]. Available: http://www.researchgate.net/publication/233426531_Zentyal_como_servidor_libre_para_empresas_cubanas

Anexos y Apéndices

Anexo A

Anexo

A.1. Distribución de direcciones IP

Los siguientes dos siguientes cuadros se obtuvo del Departamento de Sistemas de la Cooperativa, donde se pudo evidenciar la distribución de las direcciones IPs que están actualmente en funcionamiento.

DE	A	ÁREA
2	3	Secretaría
4	7	Cajas
8	15	Créditos
16	17	Inversiones
18	39	Administrativo

Tabla 5: Distribución de direcciones IPs por área.

AGENCIA	IPS
Ibarra	41
Otavalo	42
Ambato-Huachi	43
Cañar	44
Ambato-Centro	45
Quito	46
Salcedo	47
Tulcán	48
Azogues	49
Cuenca	50

Tabla 6: Distribución direcciones IP para Jefaturas por agencias.

A.2. Distribución de red de la Cooperativa

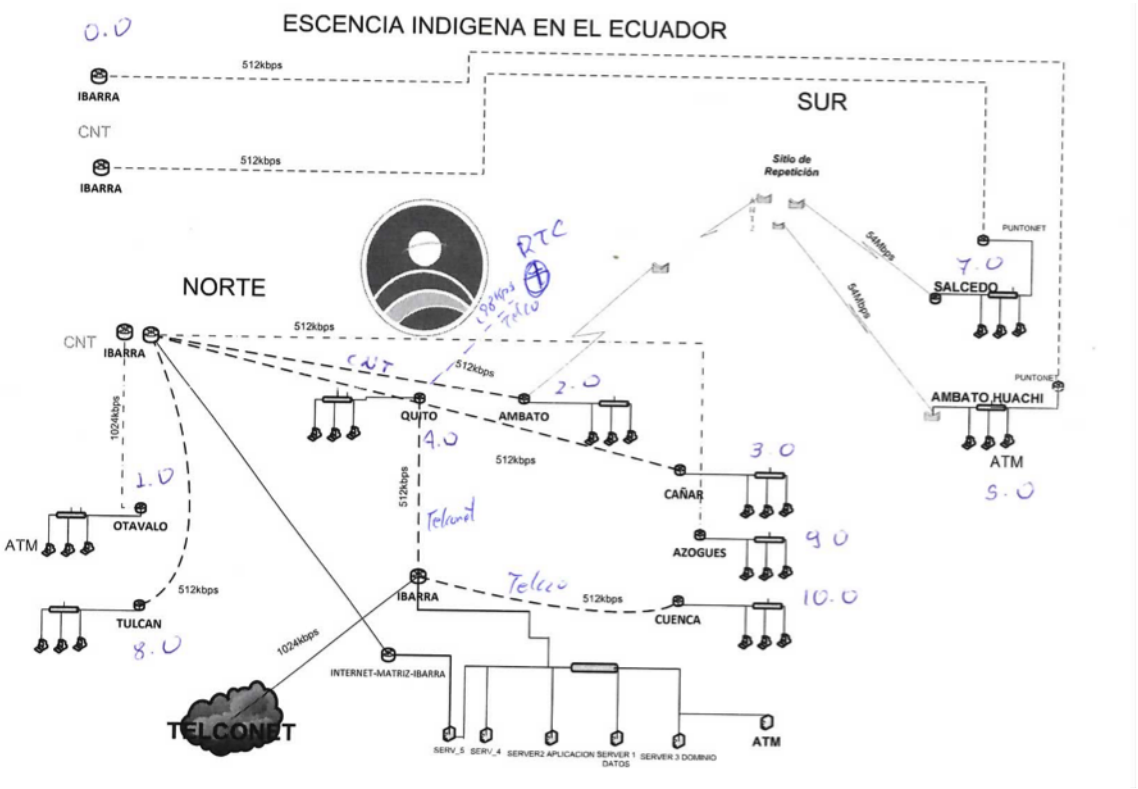


Figura 113: Esquema actual de la red de la Cooperativa.

Anexo B

Anexo

B.1. Árbol de problema

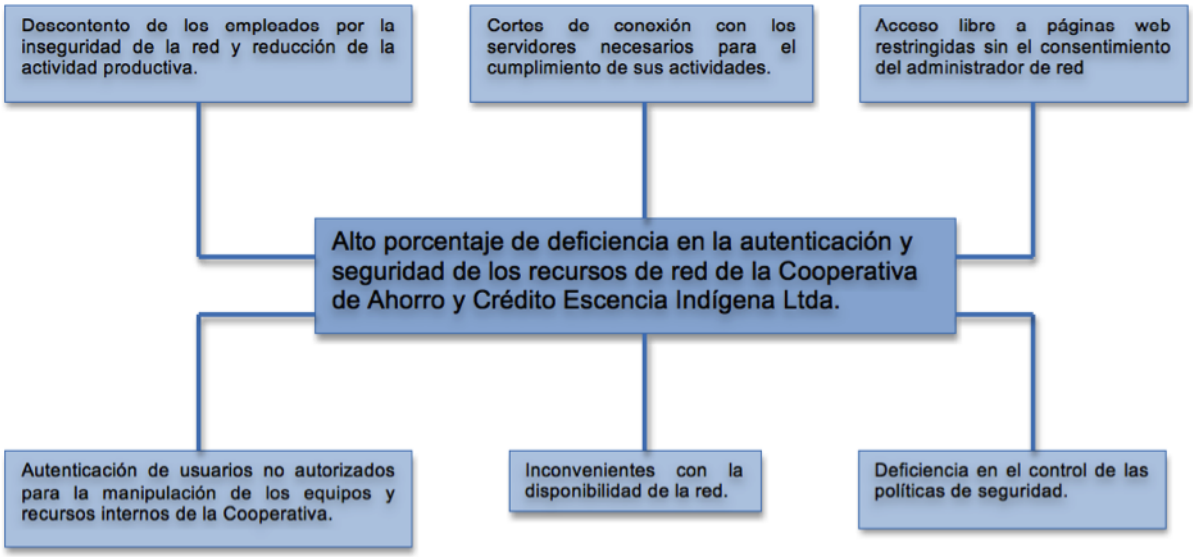


Figura 114: Árbol de problema.

Anexo C

Anexo

C.1. Reglas de acceso proxy impresas actualmente en el servidor ClearOS.

1. ADMINISTRADOR
   - *a*) Configuración General
     - Escaneo de virus activado
   - *b*) Listado de frases
     - Badwords
     - Chat
     - Drugadvocacy
     - Gambling
     - Games
     - Goodphrases
     - Illegaldrugs
     - Intolerance
     - Legaldrugs
     - Malware
     - Nudism
     - peer2peer
     - pornography
     - proxies
     - selflabeling
     - warezhacking
   - *c*) Sitios de Excepción
     - 190.152.22.157:20000

- 192.168.0.205:8386//FIT-COOP/TEST/EscenciaIndigenaTest
- 213.0.40.235/ctibsecurity/CTIBSecurity.application
- google.com
- teller.coonecta.com.ec
- www.bancoguayaquil.com/responsive/index.asp
- www.iess.gob.ec/empleador-web/

2. GERENCIAL

a) Lista de frases

- Badwords
- Chat
- Drugadvocacy
- Gambling
- Games
- Goodphrases
- Illegaldrugs
- Intolerance
- Legaldrugs
- Malware
- Nudism
- peer2peer
- pornography
- proxies
- selflabeling
- warezhacking

b) Sitios de Excepción

- 190.152.22.157:20000
- machdeportes.com/es/inicio
- teller.coonecta.com.ec

3. JEFATURA

   a) Configuración General

      - Modo de filtro normal.
      - Escaneo de virus activado.
      - Bloque de descargas activado.

   b) Lista de Frases

      - Badwords
      - Chat
      - Drugadvocacy
      - Gambling
      - Games
      - Goodphrases
      - Illegaldrugs
      - Intolerance
      - Legaldrugs
      - Malware
      - Nudism
      - peer2peer
      - pornography
      - proxies
      - selflabeling
      - violence
      - warezhacking

   c) Extensiones de Archivos

      - exe Program
      - wav Audio file

   d) Sitios Prohibidos

      - facebook.com
      - https.facebook.com

- twitter.com
- www.ebuddy.com
- www.facebook.com/
- www.xxx.com
- youtube.com

e) Sitios de Excepción

- 192.168.0.1
- 192.168.0.203
- 192.168.0.203:8386/FIT-COOP/EscenciaIndigena/FBSVS
- 192.168.0.245
- 213.0.40.235/ctibsecurity/CTIBSecurity.application
- 213.0.40.237/ctibsecurity/CTIBSecurity.application
- cajas.rapipago.ec/VentanillaWeb/Contenido/Login.aspx
- cashbg.bankguay.com/cashm/
- ecuatransfer
- servicios.seps.gob.ec/sca/login/login.jsf
- switchorm
- switchorm.com/es/index.php/es/home/descargas/category
- teller.coonecta.com.ec
- www.bancoguayaquil.com
- www.bancoguayaquil.com/responsive/index.asp
- www.escenciaindigena.com/webaccess/
- www.funcionjudicial-tungurahua.gob.ec
- www.iess.gob.ec/
- www.iess.gob.ec/empleador-web/

4. OPERATIVO

a) Configuración General

- Modo de filtro normal.
- Escaneo de virus activado.

- Bloque de descargas activado.

b) Lista de Frases

- Badwords
- Chat
- Drugadvocacy
- Gambling
- Games
- Goodphrases
- Illegaldrugs
- Intolerance
- Legaldrugs
- Malware
- Nudism
- peer2peer
- pornography
- proxies
- selflabeling
- warezhacking

c) Extensiones de Archivos

- ade Microsoft Access project extension
- adp Microsoft Access project
- bas Microsoft Visual Basic class module
- bat Batch file
- cab Windows compressed setup file
- cmd Microsoft Windows NT command script
- exe Program url Internet shortcut
- rar RAR compressed file
- zip Zip compressed file
- asx Windows Media Audio and Video

- avi Movie file midi Audio file
- mov Quicktime file
- mp3 Music file
- mp4 Music file
- mpeg Movie file
- mpg Movie file
- ogg Music file
- pcd Photo CD image
- qt Quicktime file
- wav Audio file
- wma Windows Media Audio file
- wmf Movie file
- wmv Windows Media File

d) Sitios Prohibidos

- 173.252.110.27
- ebuddy.com
- facebook.com
- outlook.com
- s.yimg.com
- socioempleo.gob.ec
- www.facebook.com
- youtube.com

e) Sitios de Excepción

- .org
- 186.3.35.156
- 186.42.112.66:8080/cobroenlinea/mis/pg_mis_principal_fs.asp
- 186.42.112.68
- 190.11.14.244
- 190.152.220.29

- 190.99.72.142
- 192.168.0.203:8386/FIT-COOP/EscenciaIndigena/
- 192.168.0.203:8386/FIT-COOP/EscenciaIndigena/FBSVS
- 192.168.0.244
- 192.168.0.244:8080/SWITCH_ENTURA/index.jsf
- 192.168.0.245
- 192.168.0.245/intranet/
- 192.168.0.246
- 192.168.0.81
- 200.25.206.91
- 207.67.74.163
- 213.0.40.235/ctibsecurity/CTIBSecurity.application
- 213.0.40.237
- 213.0.40.237/ctibsecurity/CTIBSecurity.application
- 63.91.129.163
- 65.55.39.103
- bancavirtual.bankguay.com
- bancoguayaquil.com
- bce.fin.ec
- cajas.rapipago.ec/VentanillaWeb/Contenido/Login.aspx
- cajas.rapipago.ec/VentanillaWeb/Contenido/Ventanilla/
- com.ec
- coonecta.com.ec
- corporacionregistrocivil.gov.ec
- creditreport.ec
- easypagos.com
- ecuadorlegalonline.com
- ecuatransfer
- ecuatransfer.com
- es.wikipedia.org/wiki/Certificado

- escencia.com
- escenciaindigena.com
- espe.edu.ec
- gob.ec
- google.com
- iniglobe.com.pe
- intranet
- maps.yahoo.com
- microsoft.com
- moneygram.com
- motorlink.ec
- pctools.com
- perspeak.avira-update.com
- pichincha.com
- radioambato.com
- registrosocial.gob.ec
- services.com
- servientrega.com.ec
- skype.com
- slicomp
- switchorm.com
- teamviwer
- teamviwer.com
- teller.coonecta.com.ec
- teller.coonecta.com.ec:2272/extremewebfx/home.html
- verisign.com
- webaccess
- wlxrs.com
- www.coonecta.com.ec/coonecta/index.php
- www.registrosocial.gob.ec/

- www.uta.edu.ec

f) Excepción Direcciones IP

- 192.168.0.14
- 192.168.0.26
- 192.168.0.6

g) Direcciones IP Prohibidas

- 173.252.110.27

C.2. Reglas de filtrado de paquetes.

Nombre	Servicio	Protocolo
CONSEP	-	TCP
FTPS	FTPS	TCP
FTPS	FTPS	TCP
Fit_Test	-	TCP
HTTP	HTTP	TCP
HTTPS	HTTPS	TCP
IMAP	IMAP	TCP
IMAPS	IMAPS	TCP
MOney_G	-	TCP
Money_Gram	-	TCP
OpenVPN	OpenVPN	UDP
POP3	POP3	TCP
POP3S	POP3S	TCP
PPTP	PPTP	GRE+TCP
SMTP	SMTP	TCP
Webmail	-	TCP
smtps	-	TCP
sshnuevo	-	TCP
webconfig	webconfig	TCP

Tabla 7: Conexiones permitidas al servidor.

C.3. Organigrama Estructural de la Cooperativa de Ahorro y Crédito Escencia Indígena Ltda.

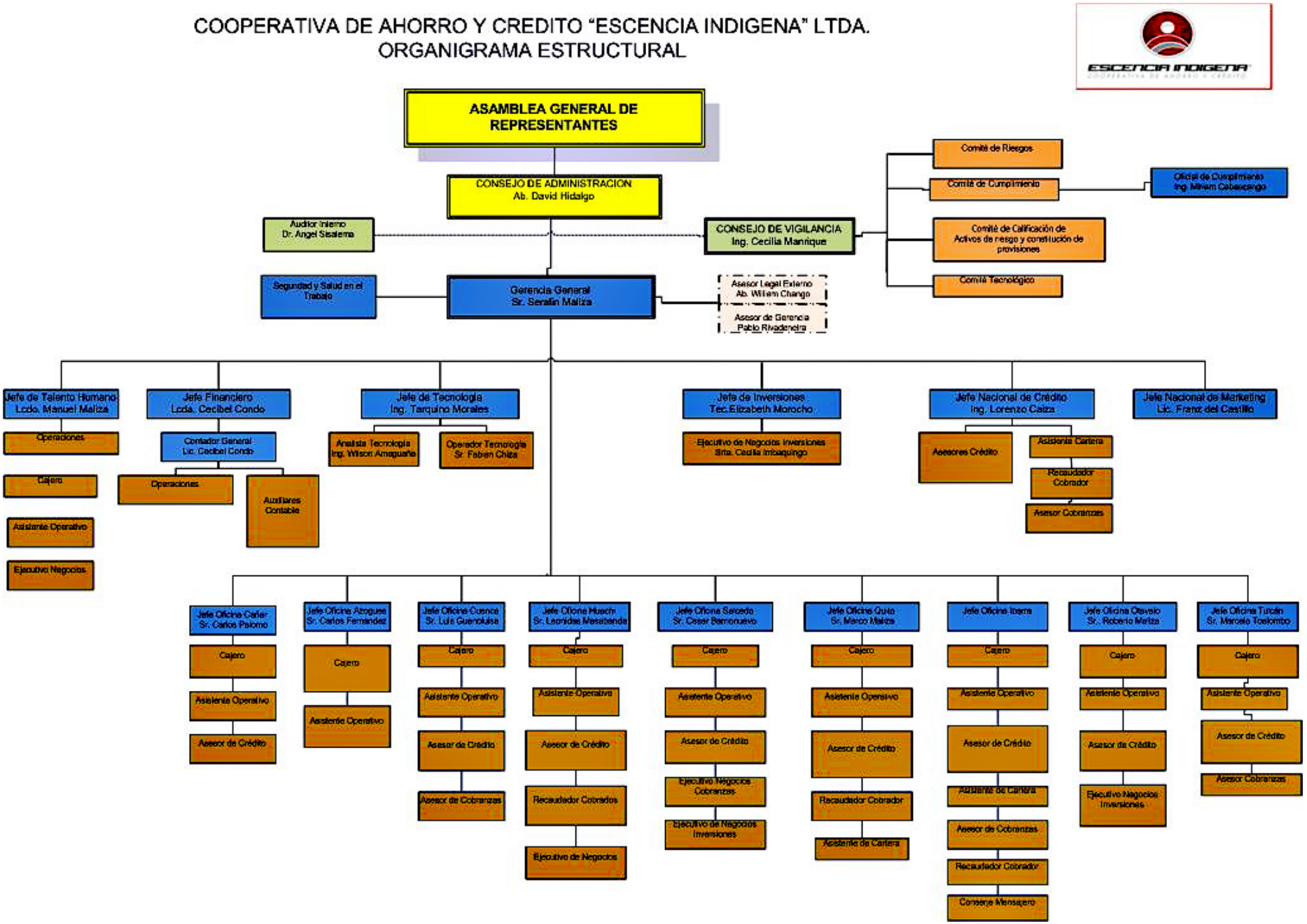
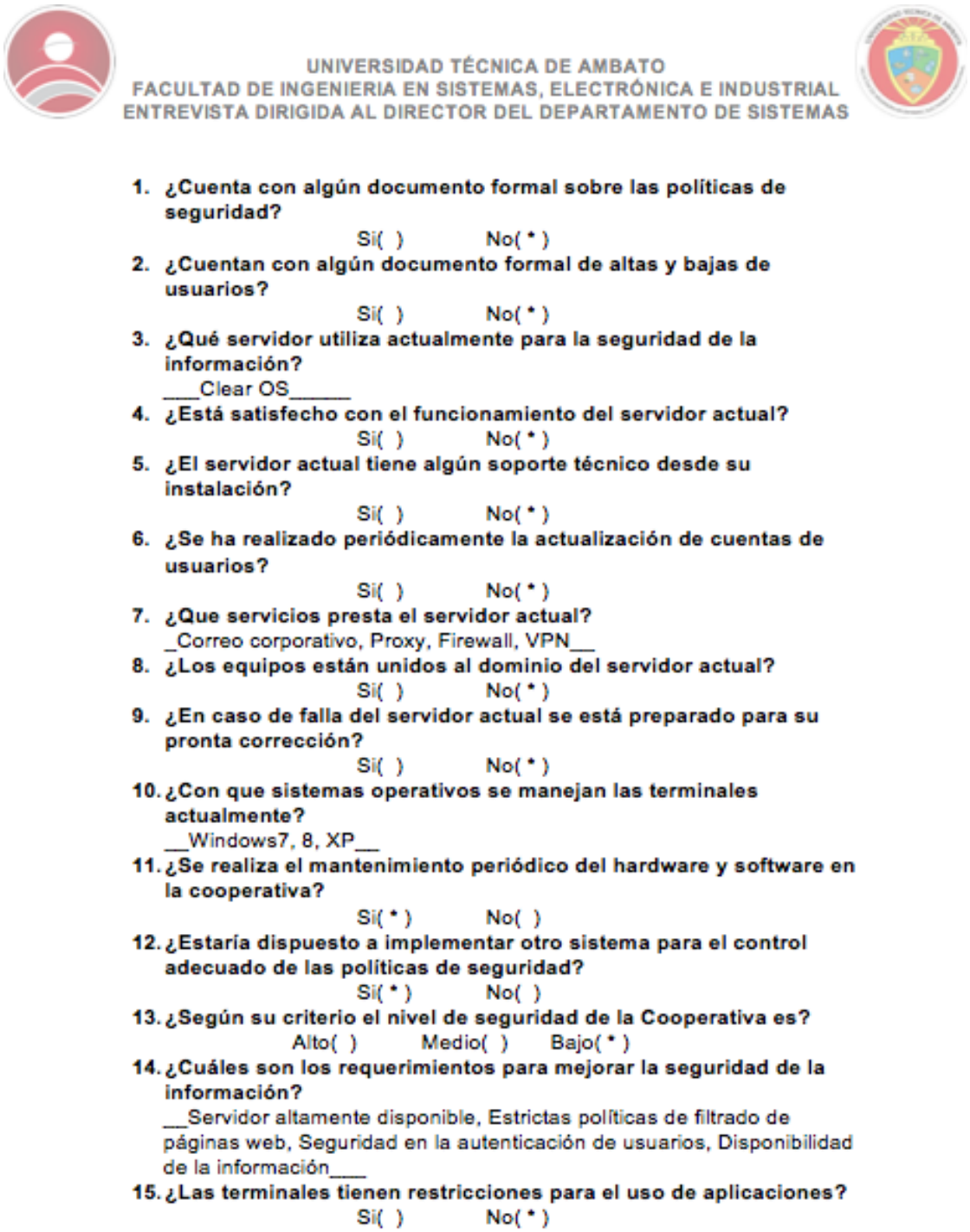


Figura 115: Organigrama estructural de la Cooperativa de Ahorro y Crédito Escencia Indígena Ltda.

Anexo D

Anexo

D.1. Entrevista al director departamental de sistemas.



UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERIA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL
ENTREVISTA DIRIGIDA AL DIRECTOR DEL DEPARTAMENTO DE SISTEMAS

1. **¿Cuenta con algún documento formal sobre las políticas de seguridad?**
   Si( ) No(*)
2. **¿Cuentan con algún documento formal de altas y bajas de usuarios?**
   Si( ) No(*)
3. **¿Qué servidor utiliza actualmente para la seguridad de la información?**
   ___Clear OS_____
4. **¿Está satisfecho con el funcionamiento del servidor actual?**
   Si( ) No(*)
5. **¿El servidor actual tiene algún soporte técnico desde su instalación?**
   Si( ) No(*)
6. **¿Se ha realizado periódicamente la actualización de cuentas de usuarios?**
   Si( ) No(*)
7. **¿Que servicios presta el servidor actual?**
   _Correo corporativo, Proxy, Firewall, VPN__
8. **¿Los equipos están unidos al dominio del servidor actual?**
   Si( ) No(*)
9. **¿En caso de falla del servidor actual se está preparado para su pronta corrección?**
   Si( ) No(*)
10. **¿Con que sistemas operativos se manejan las terminales actualmente?**
    __Windows7, 8, XP__
11. **¿Se realiza el mantenimiento periódico del hardware y software en la cooperativa?**
    Si(*) No( )
12. **¿Estaría dispuesto a implementar otro sistema para el control adecuado de las políticas de seguridad?**
    Si(*) No( )
13. **¿Según su criterio el nivel de seguridad de la Cooperativa es?**
    Alto( ) Medio( ) Bajo(*)
14. **¿Cuáles son los requerimientos para mejorar la seguridad de la información?**
    __Servidor altamente disponible, Estrictas políticas de filtrado de páginas web, Seguridad en la autenticación de usuarios, Disponibilidad de la información___
15. **¿Las terminales tienen restricciones para el uso de aplicaciones?**
    Si( ) No(*)

Figura 116: Entrevista al director departamental de sistemas.